Archived NIST Technical Series Publication

The attached publication has been archived (withdrawn), and is provided solely for historical purposes. It may have been superseded by another publication (indicated below).

Archived Publication

Series/Number:	NIST Special Publication 800-101
Title:	Guidelines on Cell Phone Forensics
Publication Date(s):	May 2007
Withdrawal Date:	May 2014
Withdrawal Note:	SP 800-101 is superseded in its entirety by the publication of SP 800-101 Revision 1 (May 2014).

Superseding Publication(s)

The attached publication has been **superseded by** the following publication(s):

Series/Number:	NIST Special Publication 800-101 Revision 1
Title:	Guidelines on Mobile Device Forensics
Author(s):	Rick Ayers, Sam Brothers, Wayne Jansen
Publication Date(s):	May 2014
URL/DOI:	http://dx.doi.org/10.6028/NIST.SP.800-101r1

Additional Information (if applicable)

Contact:	Computer Security Division (Information Technology Lab)
Latest revision of the attached publication:	SP 800-101 Revision 1 (as of August 11, 2015)
Related information:	http://csrc.nist.gov/groups/SNS/mobile_security/index.html
Withdrawal announcement (link):	N/A

Date updated: August 11, 2015

NIST
National Institute of Standards and Technology
U.S. Department of Commerce

AUTHENTICATED U.S. GOVERNMENT INFORMATION GPO

National Institute of Standards and Technology
Technology Administration
U.S. Department of Commerce

Special Publication 800-101

Sponsored by the Department of Homeland Security

Guidelines on Cell Phone Forensics

Recommendations of the National Institute of Standards and Technology

Wayne Jansen
Rick Ayers

NIST Special Publication 800-101

Guidelines on Cell Phone Forensics

Recommendations of the National Institute of Standards and Technology

Wayne Jansen
Rick Ayers

C O M P U T E R S E C U R I T Y

Computer Security Division
Information Technology Laboratory
National Institute of Standards and Technology
Gaithersburg, MD 20899-8930

May 2007

U.S. Department of Commerce
Carlos Gutierrez, Secretary

Technology Administration
Robert C. Cresanti, Under Secretary for Technology

National Institute of Standards and Technology
William Jeffrey, Director

Reports on Computer Systems Technology

The Information Technology Laboratory (ITL) at the National Institute of Standards and Technology (NIST) promotes the U.S. economy and public welfare by providing technical leadership for the Nation's measurement and standards infrastructure. ITL develops tests, test methods, reference data, proof of concept implementations, and technical analysis to advance the development and productive use of information technology. ITL's responsibilities include the development of technical, physical, administrative, and management standards and guidelines for the cost-effective security and privacy of sensitive unclassified information in Federal computer systems. This Special Publication 800-series reports on ITL's research, guidance, and outreach efforts in computer security and its collaborative activities with industry, government, and academic organizations.

National Institute of Standards and Technology Special Publication 800-101
Natl. Inst. Stand. Technol. Spec. Publ. 800-101, 104 pages (2007)

Certain commercial entities, equipment, or materials may be identified in this document in order to describe an experimental procedure or concept adequately. Such identification is not intended to imply recommendation or endorsement by the National Institute of Standards and Technology, nor is it intended to imply that the entities, materials, or equipment are necessarily the best available for the purpose.

Acknowledgements

The authors, Wayne Jansen and Rick Ayers from NIST, wish to thank colleagues who reviewed drafts of this document. In particular, our appreciation goes to Tim Grance from NIST for his research, technical support, and written contributions to this document. Our appreciation also goes out to Ronald van der Knijff and his colleagues at the Netherlands Forensic Institute and Svein Willassen at the Norwegian University of Science and Technology for their assistance on technical issues that arose in our work. The authors would also like to thank Rick Mislan from Purdue University, Chris Sanft from the SEARCH Group, and all others who assisted with our review process.

This work was sponsored by the Department of Homeland Security (DHS), whose support and guidance in this effort are greatly appreciated.

Table of Contents

TABLE OF CONTENTS V

LIST OF FIGURES VII

LIST OF TABLES VIII

EXECUTIVE SUMMARY 1

1. INTRODUCTION 3
   - 1.1 AUTHORITY 3
   - 1.2 PURPOSE AND SCOPE 3
   - 1.3 AUDIENCE AND ASSUMPTIONS 4
   - 1.4 DOCUMENT STRUCTURE 4

2. BACKGROUND 6
   - 2.1 CELL NETWORK CHARACTERISTICS 6
   - 2.2 MOBILE PHONE CHARACTERISTICS 8
   - 2.3 IDENTITY MODULE CHARACTERISTICS 11

3. FORENSIC TOOLS 13
   - 3.1 (U)SIM TOOLS 17
   - 3.2 HANDSET TOOLS 18
   - 3.3 INTEGRATED TOOLKITS 20
   - 3.4 CAPABILITIES 22

4. PROCEDURES AND PRINCIPLES 24
   - 4.1 ROLES AND RESPONSIBILITIES 24
   - 4.2 EVIDENTIAL PRINCIPLES 25
   - 4.3 PROCEDURAL MODELS 26

5. PRESERVATION 29
   - 5.1 SECURING AND EVALUATING THE SCENE 31
   - 5.2 DOCUMENTING THE SCENE 32
   - 5.3 COLLECTING THE EVIDENCE 33
   - 5.4 PACKAGING, TRANSPORTING, AND STORING EVIDENCE 36

6. ACQUISITION 38
   - 6.1 DEVICE IDENTIFICATION 39
   - 6.2 TOOL SELECTION AND EXPECTATIONS 41
   - 6.3 MEMORY CONSIDERATIONS 42
   - 6.4 UNOBSTRUCTED DEVICES 44
   - 6.5 OBSTRUCTED DEVICES 48
   - 6.6 TANGENTIAL EQUIPMENT 53

7. EXAMINATION AND ANALYSIS 56
7.1 POTENTIAL EVIDENCE 56
7.2 APPLYING TOOLS 59
7.3 CALL AND SUBSCRIBER RECORDS 61
8. REPORTING 65
9. REFERENCES 68
APPENDIX A. ACRONYMS 74
APPENDIX B. GLOSSARY 77
APPENDIX C. GENERIC ACQUISITION OVERVIEW 82
C.1 CONNECTION IDENTIFICATION 82
C.2 DEVICE IDENTIFICATION 82
C.3 DATA SELECTION 83
C.4 ACQUISITION 84
C.5 PHONEBOOK ENTRIES 85
C.6 CALL LOG ENTRIES 86
C.7 MESSAGE ENTRIES 87
C.8 CALENDAR ENTRIES 88
C.9 (U)SIM DATA 89
C.10 PICTURE ENTRIES 90
C.11 SEARCHING 91
C.12 REPORTING 92
APPENDIX D. STANDARDIZED CALL RECORDS 93
APPENDIX E. ONLINE RESOURCES FOR MOBILE DEVICE FORENSICS 95

List of Figures

Figure 1: Cellular Network Organization 8

Figure 2: (U)SIM Format 12

Figure 3: Data Acquisition, Decoding, and Translation .. 13

Figure 4: Storage Assignments 43

Figure 5: Alternative Storage Assignments..... 43

Figure 6: SIM File System 44

Figure 7: Connection Identification 82

Figure 8: Device Acquisition 83

Figure 9: Data Selection 84

Figure 10: Acquisition 85

Figure 11: Phonebook Entries 86

Figure 12: Call Log Entries 86

Figure 13: SMS Text Messages 87

Figure 14: Multimedia Message 88

Figure 15: Calendar Entries 89

Figure 16: (U)SIM Data 90

Figure 17: Picture Entries 91

Figure 18: Search Facility 91

Figure 19: Report Facility 92

List of Tables

Table 1: Hardware Characterization 9

Table 2: Software Characterization 10

Table 3: Example IMEI Acquisition..... 14

Table 4: Forensic Tools 16

Table 5: Memory Cards..... 54

Table 6: Cross Reference of Sources and Objectives 59

Table 7: Example Record Structure..... 93

Table 8: Technical Resource Sites..... 95

Table 9: Databases for Identification Queries 95

Table 10: Forensic Tools 95

Table 11: Other Related Tools 96

Executive Summary

Mobile phone forensics is the science of recovering digital evidence from a mobile phone under forensically sound conditions using accepted methods. Mobile phones, especially those with advanced capabilities, are a relatively recent phenomenon, not usually covered in classical computer forensics. This guide attempts to bridge that gap by providing an in-depth look into mobile phones and explaining the technologies involved and their relationship to forensic procedures. It covers phones with features beyond simple voice communication and text messaging and their technical and operating characteristics. This guide also discusses procedures for the preservation, acquisition, examination, analysis, and reporting of digital information present on cell phones, as well as available forensic software tools that support those activities.

The objective of the guide is twofold: to help organizations evolve appropriate policies and procedures for dealing with cell phones, and to prepare forensic specialists to contend with new circumstances involving cell phones, when they arise. The guide is not all-inclusive nor is it prescribing how law enforcement and incident response communities handle mobile devices during investigations or incidents. However, from the principles outlined and other information provided, organizations should nevertheless find the guide helpful in setting policies and procedures. This publication should not be construed as legal advice. Organizations should use this guide as a starting point for developing a forensic capability in conjunction with extensive guidance provided by legal advisors, officials, and management.

The information in this guide is best applied in the context of current technology and practices. Every situation is unique, as are the experiences of the forensic specialists and the tools and facilities at their disposal. The judgment of the forensic specialists should be given deference in the implementation of the procedures suggested in this guide. Circumstances of individual cases; international, federal, state, local laws and rules; and organization-specific policies may also require actions other than those described in this guide. As always, close and continuing consultation with legal counsel is advised.

Implementing the following recommendations should facilitate efficient and effective digital forensic activities involving cell phones and cellular devices.

Organizations should ensure that their policies contain clear statements about forensic considerations involving cell phones.

At a high level, policy should allow authorized personnel to perform investigations of organizationally issued cell phones for legitimate reasons, under the appropriate circumstances. The forensic policy should clearly define the roles and responsibilities of the workforce and of any external organizations performing or assisting with the organization's forensic activities. The policy should also indicate internal teams and external organizations to be contacted under various circumstances.

Organizations should create and maintain procedures and guidelines for performing forensic tasks on cell phones.

Guidelines should focus on general methodologies for investigating incidents using forensic techniques. While developing comprehensive procedures tailored to every possible situation is

not generally feasible, organizations should consider developing step-by-step procedures for performing all routine activities in the preservation, acquisition, examination and analysis, and reporting of digital evidence found on cell phones and associated media. The guidelines and procedures should facilitate consistent, effective, accurate, and repeatable actions carried out in a forensically sound manner, suitable for legal prosecution or disciplinary actions. The guidelines and procedures should support the admissibility of evidence into legal proceedings, including seizing and handling evidence properly, maintaining the chain of custody, storing evidence appropriately, establishing and maintaining the integrity of forensic tools and equipment, and demonstrating the integrity of any electronic logs, records, and case files. The guidelines and procedures should be reviewed periodically, and also whenever significant changes in cell phone technology appear that affect them.

Organizations should ensure that their policies and procedures support the reasonable and appropriate use of forensic tools for cell phones.

Policies and procedures should clearly explain what actions are to be taken by a forensic unit under various circumstances commonly encountered with cell phones. They should also describe the quality measures to apply in verifying the proper functioning of any forensic tools used in examining cell phones and associated media. Procedures for handling sensitive information that might be recorded by forensic tools should also be addressed. Legal counsel should carefully review all forensic policy and high-level procedures for compliance with international, federal, state, and local laws and regulations, as appropriate.

Organizations should ensure that their forensic professionals are prepared to conduct activities in cell phone forensics.

Forensic professionals, especially first responders to incidents, should understand their roles and responsibilities for cell phone forensics and receive training and education on related forensic tools, policies, guidelines, and procedures. Forensic professionals should also consult closely with legal counsel both in general preparation for forensics activities, such as determining which actions should and should not be taken under various circumstances. In addition, management should be responsible for supporting forensic capabilities, reviewing and approving forensic policy, and examining and endorsing unusual forensic actions that may be needed in a particular situation.

1. Introduction

1.1 Authority

The National Institute of Standards and Technology (NIST) developed this guide in furtherance of its statutory responsibilities under the Federal Information Security Management Act (FISMA) of 2002, Public Law 107-347.

NIST is responsible for developing standards and guidelines, including minimum requirements, for providing adequate information security for all Federal agency operations and assets; but such standards and guidelines shall not apply to national security systems. This guideline is consistent with the requirements of the Office of Management and Budget (OMB) Circular A-130, Section 8b(3), "Securing Agency Information Systems," as analyzed in A-130, Appendix IV: Analysis of Key Sections. Supplemental information is provided in A-130, Appendix III.

This guide has been prepared for use by Federal agencies. It may be used by non-governmental organizations on a voluntary basis and is not subject to copyright, though attribution is desired.

Nothing in this guide should be taken to contradict standards and guidelines made mandatory and binding on Federal agencies by the Secretary of Commerce under statutory authority, nor should these guidelines be interpreted as altering or superseding the existing authorities of the Secretary of Commerce, Director of the OMB, or any other Federal official.

1.2 Purpose and Scope

This guide provides basic information on the preservation, acquisition, examination, analysis, and reporting of digital evidence on cell phones, relevant to law enforcement, incident response, and other types of investigations. The guide focuses mainly on the characteristics of cell phones, including smart phones having advanced capabilities. It also covers provisions to be taken into consideration during the course of an incident investigation.

The guide is intended to address common circumstances that may be encountered by organizational security staff and law enforcement investigators, involving digital electronic data residing on cell phones and associated electronic media. It is also intended to complement existing guidelines and delve more deeply into issues related to cell phones and their examination and analysis.

Procedures and techniques presented in this document are a compilation of the authors' opinions and references taken from existing forensic guidelines. The publication is not to be used as a step-by-step guide for executing a proper forensic investigation when dealing with mobile phones or construed as legal advice. Its purpose is to inform readers of the various technologies involved and potential ways to approach them from a forensic point of view. Readers are advised to apply the recommended practices only after consultation with management and legal officials for compliance with laws and regulations (i.e., local, state, federal, and international) that pertain to their situation.

1.3 Audience and Assumptions

The intended audience is varied and ranges from response team members handling a computer security incident to organizational security officials investigating an employee-related situation to forensic examiners involved in criminal investigations. The practices recommended in this guide are designed to highlight key technical principles associated with the handling and examination of electronic evidence, in general, and cell phones in particular. Readers are assumed to have a basic grounding in classical computer forensics involving individual computer systems (e.g., personal computers) and network servers. Because of the constantly changing nature of handheld devices and related forensic procedures and tools, readers are expected to take advantage of other resources, including those listed in this guide, for more current and detailed information.

1.4 Document Structure

The guide is divided into the following chapters and appendices:

- Chapter 1 (this chapter) explains the authority, purpose and scope, audience and assumptions of the document, and outlines its structure.
- Chapter 2 is an overview on cell phones, including an overview of common hardware and software capabilities.
- Chapter 3 discusses present-day cell phone forensic tools and the types of devices with which they work.
- Chapter 4 provides general information on procedures and principles that apply to cell phone forensics.
- Chapter 5 discusses considerations for preserving digital evidence associated with cell phones.
- Chapter 6 examines the process of acquisition of digital evidence from cell phones, as well as from common types of peripheral equipment.
- Chapter 7 outlines common sources of evidence on cell phones and the features and capabilities of tools for examination.
- Chapter 8 discusses the reporting of findings.
- Chapter 9 contains a list of references used in this guide.
- Appendix A contains a list of acronyms used in this guide.
- Appendix B contains a glossary defining terms used in this guide.
- Appendix C gives a summary of the steps involved in an acquisition.
- Appendix D provides an example of the structure of call records maintained by cell phone carriers.

- Appendix E provides links to online resources.

2. Background

The digital forensic community faces a constant challenge to stay abreast of the latest technologies that may be used to expose relevant clues in an investigation. Mobile phones are commonplace in today's society, used by many individuals for both personal and professional purposes. Mobile phone forensics is the science of recovering digital evidence from a mobile phone under forensically sound conditions using accepted methods. Cell phones vary in design and are continually undergoing change as existing technologies improve and new technologies are introduced. When a cell phone is encountered during an investigation, many questions arise: What should be done about maintaining power? How should the phone be handled? How should valuable or potentially relevant data contained on the device be examined? The key to answering these questions is an understanding of the hardware and software characteristics of cell phones.

This chapter gives an overview of the hardware and software capabilities of cell phones and their associated cellular networks. The overview provides a summary of general characteristics and, where useful, focuses on key features. Developing an understanding of the components and organization of cell phones (e.g., memory organization and use) is a prerequisite to understanding the criticalities involved when dealing with them forensically. For example, cell phone memory that contains user data may be volatile (i.e., RAM) and require continuous power to maintain content, unlike a personal computer's hard disk. Similarly, features of cellular networks are an important aspect of cell phone forensics, since logs of usage and other data are maintained therein. Handheld device technologies and cellular networks are rapidly changing, with new technologies, products, and features being introduced regularly. Because of the fast pace with which cellular device technologies are evolving, this discussion captures a snapshot of the cell phone area at the present time.

2.1 Cell Network Characteristics

Within the U.S., different types of digital cellular networks abound that follow distinct incompatible sets of standards. The two most dominant types of digital cellular networks are known as Code Division Multiple Access (CDMA) and Global System for Mobile Communications (GSM) networks. Other common cellular networks include Time Division Multiple Access (TDMA) and Integrated Digital Enhanced Network (iDEN). IDEN networks use a proprietary protocol designed by Motorola, while the others follow standardized open protocols. A digital version of the original analog standard for cellular telephone phone service, called Digital Advanced Mobile Phone Service (D-AMPS), also exist.

CDMA refers to a technology designed by Qualcomm in the U.S., which employs spread spectrum communications for the radio link. Rather than sharing a channel as many other network air interfaces do, CDMA spreads the digitized data over the entire bandwidth available, distinguishing multiple calls through a unique sequence code assigned. Successive versions of the IS-95 standard define CDMA conventions in the U.S., which is the reason why the term CDMA is often used to refer to IS-95 compliant cellular networks. IS-95 CDMA systems are sometimes referred to as cdmaOne. The next evolutionary step for CDMA to 3G

services is cdma2000, TIA/EIA/IS-2000 Series[1], Release A, based on the ITU IMT-2000 standard. Both Verizon and Sprint operate nationwide CDMA networks in the U.S.

GSM is a cellular system used worldwide that was designed in Europe, primarily by Ericsson and Nokia. Cingular and T-Mobile operate nationwide networks in the U.S. GSM uses a TDMA air interface. TDMA refers to a digital link technology whereby multiple phones share a single carrier, radio frequency channel by taking turns – using the channel exclusively for an allocated time slice, then releasing it and waiting briefly while other phones use it. A packet switching enhancement to GSM wireless networks called General Packet Radio Service (GPRS) was standardized to improve the transmission of data. The next generation of GSM, commonly referred to as the third generation or 3G, is known as Universal Mobile Telecommunications System (UMTS) and involves enhancing GSM networks with a Wideband CDMA (W-CDMA) air interface.

TDMA is also used to refer specifically to the standard covered by IS-136, which defines a specific type of cellular network. Using the term TDMA to refer to a general technique or a specific type of cellular network can be a source of confusion. For example, although GSM uses a TDMA air interface (i.e., the general technique), as does iDEN, neither of those systems is compatible with so-called TDMA cellular networks that follow IS-136.

Mobile phones work with certain subsets of the network types mentioned, typically those associated with the service provider providing the phone and from whom a service agreement was arranged. For example, a service provider or network operator for a GSM network that has some older TDMA network segments in operation might supply a phone that has GSM voice and data capabilities, and TDMA capabilities. Such a phone would not be compatible with CDMA networks. Mobile phones can also be acquired without service from a manufacturer, vendor, or other source, and have their service set up separately with a service provider or network operator, provided that the phone is compatible with the network. When in operation, mobile phones may contact compatible networks operated for or by another service provider, and gain service. To administer the cellular network system, provide subscribed services, and accurately bill or debit subscriber accounts, data about the service contract and associated service activities are captured and maintained by the network system.

As the name implies, cellular networks provide coverage based on dividing up a large geographical service area into smaller areas of coverage called cells. Cells play an important role in reuse of radio frequencies in the limited radio spectrum available to allow more calls to occur than otherwise would be possible. As a mobile phone moves from one cell to another, however, a cellular arrangement requires active connections to be monitored and effectively passed along between cells to maintain the connection

Despite their differences in technology, cellular networks are organized similarly to one another, in a manner illustrated in Figure 1. The main components are the radio transceiver equipment that communicates with mobile phones, the controller that manages the transceiver equipment and performs channel assignment, and the switching system for the cellular network. The technical names for these components are respectively the Base Transceiver Station (BTS), the Base Station Controller (BSC), and the Mobile Switching Center (MSC). The BSC and the BTS units it controls are sometimes collectively referred to as a Base Station

[1] Available at the following site: http://www.tiaonline.org/standards/technology/cdma2000/cdma2000table.cfm

Subsystem. The transceivers at the BTS can be configured in a variety of ways. A typical configuration involves three distinct sectors of 120 degree coverage: 0 degrees North to 120 degrees Southeast, 120 degrees Southeast to 240 degrees Southwest, and 240 degrees Southwest to 360 degrees North. A cell identifier uniquely identifies the BTS and sector involved in servicing a call.

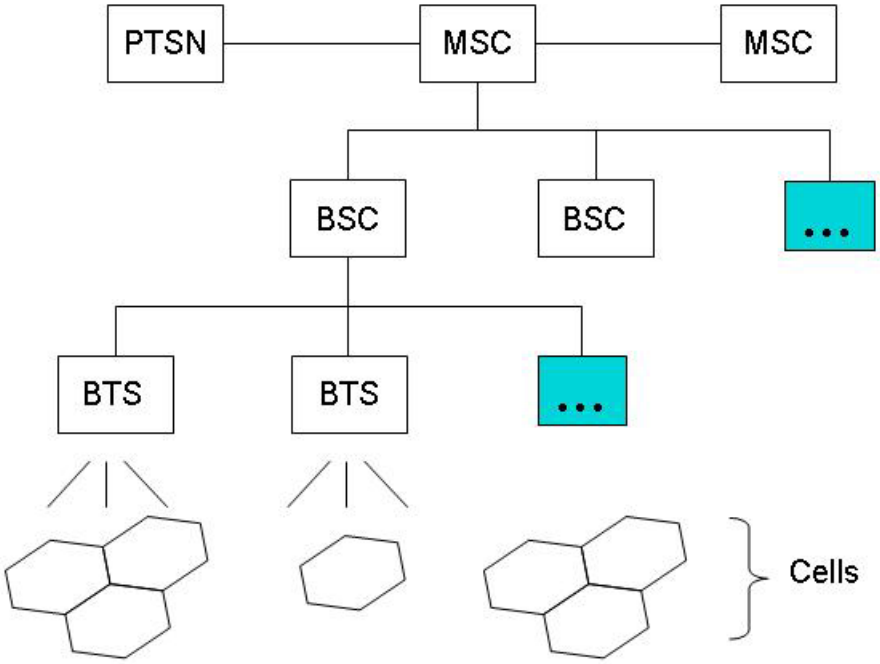

Figure 1: Cellular Network Organization

The MSC controls a set of BSCs and manages overall communications throughout the cellular network, including interfacing to the public switch telephone network. To perform its tasks, the MSC uses several databases. A key database is the central repository system for subscriber data and service information, called the Home Location Register (HLR). Another database used in conjunction with the HLR for mobile phones roaming outside of their service area is the Visitor Location Register. Account information, such as data about the subscriber (e.g., a billing address), the subscribed services, and the location update last registered with the network are maintained at the HLR and used by the MSC to route calls and messages and to generate usage records called call detail records. The subscriber account data and call detail records are often a valuable source of evidence in an investigation.

2.2 Mobile Phone Characteristics

Mobile phones are highly mobile communications devices that perform an array of functions ranging from that of a simple digital organizer to that of a low-end personal computer. Designed for mobility, they are compact in size, battery powered, and lightweight. Most cell phones have a basic set of comparable features and capabilities. They house a microprocessor, read only memory (ROM), random access memory (RAM), a radio module, a digital signal processor, a microphone and speaker, a variety of hardware keys and interfaces, and a liquid crystal display (LCD). The operating system (OS) of the device is held in ROM, which with the proper tools typically can be erased and reprogrammed electronically. RAM, which for

certain models may be used to store user data, is kept active by batteries, whose failure or exhaustion causes that information to be lost.

The latest cell phones come equipped with system-level microprocessors that reduce the number of supporting chips required and include considerable memory capacity. Built-in Mini Secure Digital (MiniSD)[2], MultiMedia Card Mobile (MMCmobile)[3], or other types of card slots support removable memory cards or specialized peripherals, such as an SDIO WiFi card. Wireless communications such as infrared (i.e., IrDA) or Bluetooth may also be built into the device.

Different devices have different technical and physical characteristics (e.g., size, weight, processor speed, memory capacity). Devices may also use different types of expansion capabilities to provide additional functionality. Furthermore, cell phone capabilities sometimes include those of other devices such as PDAs, global positioning systems, and cameras. Overall, they can be classified as basic phones that are primarily simple voice and messaging communication devices; advanced phones that offer additional capabilities and services for multimedia; and smart phones or high-end phones that merge the capabilities of an advanced phone with those of a PDA. Table 1 highlights the general hardware characteristics of basic, advanced, and smart phone models, which underscore this diversity.

Table 1: Hardware Characterization

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

Note that the characteristics used in this classification scheme are illustrative. The features of actual devices do vary and can span more than one category identified. Over time, advanced

[2] The Secure Digital home page can be found at: http://www.Sdcard.org

[3] The MultiMediaCard home page can be found at: http://www.mmca.org

features also tend to appear in more basic phones as new ones are added to the high end. Though the lines among this classification scheme are somewhat fuzzy and dynamic, it nevertheless serves as a general guide.

Despite the type of cell phone, nearly all devices support voice and text messaging, a set of basic Personal Information Management (PIM) applications that includes phonebook and date book facilities, and a means to synchronize PIM data with a desktop computer. More advanced devices also provide the ability to perform multimedia messaging, connect to the Internet and surf the Web, exchange electronic mail, or chat using instant messaging. They may also provide enhanced PIM applications that work with specialized built-in hardware, such as a camera.

Finally, very high-end devices called smart phones add PDA-like capability for reviewing electronic documents (e.g., reports, briefing slides, and spreadsheets) and running a wide variety of general and special-purpose applications. Smart phones are typically larger than other phones, support a bigger-size display (e.g., ¼ VGA and higher), and may have an integrated QWERTY keyboard or touch sensitive screen. They also offer more extended expansion capabilities through peripheral card slots, other built-in wireless communications such as Bluetooth and WiFi, and synchronization protocols to exchange other kinds of data beyond basic PIM data (e.g., graphics, audio, and archive file formats). Table 2 lists the differences in software capabilities found on these device classes.

Table 2: Software Characterization

	Basic	Advanced	Smart
OS	Proprietary	Proprietary	Linux, Windows Mobile, RIM OS, Palm OS, Symbian
PIM	Simple Phonebook	Phonebook and Calendar	Reminder List, Enhanced Phonebook and Calendar
Applications	None	MP3 Player	MP3 Player, Office Document Viewing
Messaging	Text Messaging	Text with Simple Embedded Images and Sounds (Enhanced Text)	Text, Enhanced Text, Full Multimedia Messaging
Chat	None	SMS Chat	Instant Messaging
Email	None	Via Network Operator's Service Gateway	Via POP or IMAP Server
Web	None	Via WAP Gateway	Direct HTTP
Wireless	IrDA	IrDA, Bluetooth	IrDA, Bluetooth, WiFi

The basic and advanced cell phones typically use a company proprietary operating system. A number of companies specializing in embedded software also offer real-time operating system solutions for manufacturers of portable devices, including cell phones. Nearly all cell phones claiming to be smart phones use one of the following operating systems: Palm OS, Windows Mobile (phone edition), RIM OS, Symbian OS, or Linux. Unlike the more limited, real-time kernels in basic and advanced phones, these operating systems are multi-tasking and full-featured, designed specifically to match the capabilities of high-end mobile devices. Besides a wide array of applications, they often come complete with a Java Virtual Machine and native

application support using a Software Development Kit (SDK) for C++ or another language. Characteristics of a wide range of past, current, and future cell phones can be found on manufacturer and vendor Web sites, as well as product review sites.[4]

2.3 Identity Module Characteristics

Subscriber Identity Modules are synonymous with mobile phones and devices that interoperate with GSM cellular networks. Under the GSM framework, a cellular phone is referred to as a Mobile Station and is partitioned into two distinct components: the Subscriber Identity Module (SIM) and the Mobile Equipment (ME). As the name implies, a SIM is a removable component that contains essential information about the subscriber. The ME, the remaining radio handset portion, cannot function fully without one. The SIM's main function entails authenticating the user of the cell phone to the network to gain access to subscribed services. The SIM also provides storage for personal information, such as phone book entries and text messages, as well as service-related information.

The SIM-ME partitioning of a cell phone stipulated in the GSM standards has brought about a form of portability. Moving a SIM between compatible cell phones automatically transfers with it the subscriber's identity and the associated information and capabilities. In contrast, present-day CDMA phones do not employ a SIM. Analogous SIM functionality is instead directly incorporated within the device. While SIMs are most widely used in GSM systems, comparable modules are also used in iDEN phones and UMTS user equipment (i.e., a USIM). Because of the flexibility a SIM offers GSM phone users to port their identity, personal information, and service between devices, eventually all cellular phones are expected to include (U)SIM-like capability. For example, requirements for a Removable User Identity Module (R-UIM), as an extension of SIM capabilities, have been specified for cellular environments conforming to TIA/EIA/IS-95-A and -B specifications, which include Wideband Spread Spectrum based CDMA [3GP02].

At its core, a (U)SIM is a special type of smart card that typically contains a processor and between 16 to 128 KB of persistent electronically erasable, programmable read only memory (EEPROM). It also includes RAM for program execution and ROM for the operating system, user authentication and data encryption algorithms, and other applications. The (U)SIM's hierarchically organized file system resides in persistent memory and stores such things as names and phone number entries, text messages, and network service settings. Depending on the phone used, some information on the (U)SIM may coexist in the memory of the phone. Information may also reside entirely in the memory of the phone instead of available memory reserved for it in the file system of the (U)SIM [Wil05, Jan06].

The (U)SIM operating system controls access to elements of the file system [3GP05a]. Actions such are reading or updating can be permitted or denied unconditionally, or allowed conditionally with certain access rights. Rights are assigned to a subscriber through 4-8 digit Personal Identification Number (PIN) codes. PINs protect core (U)SIM subscriber-related data and certain optional data. PIN codes can be modified by the subscriber, and their function disabled or enabled. A preset number of attempts, usually three, are allowed for providing the correct PIN code to the (U)SIM before further attempts are blocked completely, rendering communications inoperative. Only by providing a correct PIN Unblocking Key (PUK) can the

[4] For example, specifications and product reviews for many current cell phones can be found at http://www.cnet.com.

value of a PIN and its attempt counter be reset on the (U)SIM. If the number of attempts to enter the correct PUK value exceeds a set limit, normally ten attempts, the card becomes blocked permanently. The PUK for a PIN can be obtained from the service provider or network operator by providing the identifier of the SIM (i.e., its Integrated Circuit Chip Identifier or ICCID). The ICCID is normally imprinted on the (U)SIM, but can also be read from an element of the file system.

(U)SIMs have a width of 25 mm, a height of 15 mm, and a thickness of .76 mm, which is roughly the footprint of a postage stamp. Though similar in dimension to a MiniSD or an MMCmobile removable memory card supported by some cell phones, (U)SIMs follow a different set of specifications with vastly different characteristics. For example, their pin connectors are not aligned along a bottom edge as with removable media cards, but instead form a circular contact pad integral to the smart card chip, which is embedded in a plastic frame, as shown in Figure 2. (U)SIMs also employ a broad range of tamper resistance techniques to protect the information they contain.

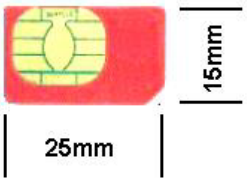

Figure 2: (U)SIM Format

The slot for the (U)SIM card is normally not accessible from the exterior of the phone to facilitate frequent insertion and removal as with a memory card. Instead, it typically is found in the battery compartment under the battery. When a (U)SIM is inserted into a phone handset and pin contact is made, a serial interface is used for communicating between them. A (U)SIM can be removed from a phone and read using a specialized (U)SIM reader and software through the same interface. Standard-size smart card adapters are also available for (U)SIMs, which allows them to be inserted into and read with a conventional smart card reader.

Authenticating a device to a network securely is a vital function performed via the SIM. Cryptographic key information and algorithms within the tamper resistant module provide the means for the device to participate in a challenge-response dialogue with the network and respond correctly, without exposing key material and other information that could be used to clone the SIM and gain access to a subscriber's services. Cryptographic key information in the SIM also supports stream cipher encryption to protect against eavesdropping on the air interface [Ved93, Wil03].

3. Forensic Tools

The situation with forensic software tools for cell phones is considerably different from personal computers. While personal computers are designed as general-purpose systems, cell phones are designed more as special-purpose appliances that perform a set of predefined tasks. Cellular phone manufacturers also tend to rely on assorted proprietary operating systems rather than the more standardized approach found in personal computers. Because of this, the variety of toolkits for mobile devices is diverse and the range of devices over which they operate is typically narrowed to distinct platforms for a manufacturer's product line, an operating system family, or a type of hardware architecture. Short product release cycles are the norm for cellular phones, requiring tool manufacturers to update their tools continually to keep coverage current. The task is formidable and tool manufacturers' support for newer models often lags significantly. Some have argued that the current state is likely to continue, keeping the cost of examination significantly higher than if a few standard operating systems prevailed [Moo06].

Forensic tools acquire data from a device in one of two ways: physical acquisition or logical acquisition. Physical acquisition implies a bit-by-bit copy of an entire physical store (e.g., a memory chip), while logical acquisition implies a bit-by-bit copy of logical storage objects (e.g., directories and files) that reside on a logical store (e.g., a file system partition). The difference lies in the distinction between memory as seen by a process through the operating system facilities (i.e., a logical view), versus memory as seen in raw form by the processor and other related hardware components (i.e., a physical view).

Physical acquisition has advantages over logical acquisition, since it allows deleted files and any data remnants present (e.g., in unallocated memory or file system space) to be examined, which otherwise would go unaccounted. Extracted device images need to be parsed, decoded, and translated to uncover the data present. The work is tedious and time consuming to perform manually. Physical device images can be imported into a tool to automate examination and reporting, however, only a few tools tailored for obtaining cell phone images are currently available. A logical acquisition, though more limited than a physical acquisition, has the advantage that the system data structures are normally easier for a tool to extract and provide a more natural organization to understand and use during examination. If possible, doing both types of acquisition is preferable – a physical acquisition before a logical acquisition.

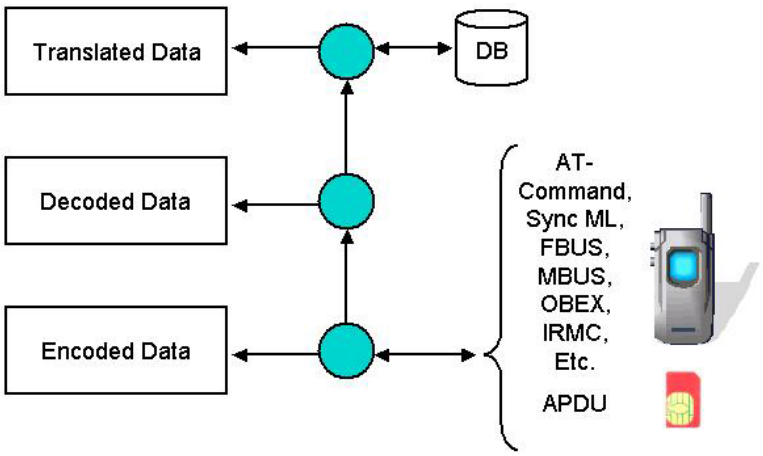

Figure 3: Data Acquisition, Decoding, and Translation

Most forensic software tools for cell phones and (U)SIMs acquire data logically, using common device protocols for synchronization, communications, and debugging, as shown in Figure 3 [Gra02, Mcc05]. Some tools may also be capable of acquiring data physically for certain classes of phones. AT commands, Sync ML, and the other protocols listed are commonly used in the logical acquisition of cell phones. Because handsets can support multiple protocols, a tool may employ several of them in succession to acquire the broadest range of available data. Even if a tool uses multiple protocols for a particular handset, all of the data available may not be able to be retrieved.

Different tools can use a different protocol to acquire the same data. Table 3 illustrates the protocol exchanges used by several tools to acquire the IMEI (i.e., ASCII value of 356661005704092) from a Nokia 6101 cell phone. The first tool listed uses a standardized AT Command exchange [Nok05], while the other two tools use the FBUS protocol [Pea05]. While many of the protocols are standardized and publicly available, some such as MBUS and FBUS are proprietary. Even standardized protocols often include manufacturer extensions or variants. (U)SIMs follow stricter standards than handsets and the application protocol data unit (APDU) interface protocol listed in Figure 3 is normally used exclusively with them.

Table 3: Example IMEI Acquisition

	Request/Response (Hex)	Request/Response (ASCII)
GSM .XRY	41 54 2B 43 47 53 4E 0D	A T + C G S N .
	0D 0A **33 35 36 36 36 31 30 30 35 37 30 34 30 39 32** 0D 0A 0D 0A 4F 4B 0D 0A	**. . 3 5 6 6 6 1 0 0 5 7 0 4 0 9 2** . . . . O K . .
PhoneBase	1E 00 0C 7F 00 02 D2 01 C0 7C 1E 00 10 1B 00 07 00 01 00 00 41 01 41 00 0E 1C	. . . . . Ò . À | . . . . . A . A **. . .**
	1E 10 00 7F 00 02 1B 01 05 6C 1E 10 00 1B 00 1C 01 39 00 01 00 01 41 14 00 10 **33 35 36 36 36 31 30 30 35 37 30 34 30 39 32** 00 01 42 5B 50	. . . . . l . . . . . 9 . . . . A . . . **3 5 6 6 6 1 0 0 5 7 0 4 0 9 2** . . B [P
Secure View	55 55 55

a handset and any removable identity modules such as SIMs found in GSM and other types of phones. Both forensic and non-forensic software tools often use the same protocols to communicate with the device. However, non-forensic tools allow a two-way flow of information to enhance or customize one's cellular device (e.g., to add customized phone rings, wallpaper, themes, etc.), while forensic tools are designed specifically to acquire data from the device without altering device content and to calculate integrity hashes over the acquired data. Most practitioners use a collection of both forensic and non-forensic tools along with other accessories to form their "toolbox."[5] Tools not designed specifically for forensic purposes are questionable, however [New07]. Before considering their use, they should be thoroughly evaluated and the implications of any associated forensic issues should be fully understood. In some situations, non-forensic tools might be the only means to retrieve data that could be relevant as evidence and may be appropriate to use when the proper precautions are taken.

Port Monitoring: On occasion one might be faced with having to use a non-forensic tool, such as a phone manager, to recover data. Besides using test phones in thoroughly evaluating and understanding the tool, some additional steps can be considered. One of the easiest things to do, not only during the tool evaluation, but also during an actual acquisition once the evaluation has been completed, is to capture the protocol exchanges that occur over the serial connection between the phone and forensic workstation. Port monitors with such logging capabilities for cabled devices include Portmon[6] and Serial Monitor.[7] Infrared and Bluetooth monitoring is also possible using a separate workstation to eavesdrop on the wireless communications.

During evaluation, the protocol exchanges can be analyzed for specific actions taken at the user interface and benign actions identified. During an actual acquisition, capturing the protocol exchanges serves as a record of the events that occurred, which can be kept for reference to refute any concerns that may be raised at a later time.

Port monitoring can also be carried out with a forensic tool to gain insight on its operation or simply to capture a complete log of an acquisition. For example, the entries shown in Table 3 were captured this way. Monitoring of (U)SIM tool exchanges can be done similarly. Built-in logging of protocol exchanges is a useful feature that some forensic tools provide, and precludes the need for a separate tool.

While most forensic tools support a full range of acquisition, examination, and reporting functions, some tools focus only on a subset. Different tools may also support different interfaces (e.g., IrDA, Bluetooth, or serial cable) to acquire device contents. Acquisition through a cable interface generally yields superior results than other interfaces. However, under certain conditions, a wireless interface such as infrared or Bluetooth can serve as a reasonable alternative (e.g., when the correct cable is not readily available and the forensic issues of using another interface are understood). Regardless of the interface used, vigilance of the potential forensic issues associated is paramount. For example, Bluetooth typically involves an exchange of information with the forensic workstation to setup a connection,

---

[5] For an example of recommended tools to include in an investigator's toolkit, see http://www.search.org/files/pdf/CellphoneInvestToolkit-0806.pdf.

[6] For more information, see http://www.sysinternals.com/Utilities/Portmon.html.

[7] For more information, see http://www.hhdsoftware.com/sermon.html.

which is then retained on the device. Enabling the connection and pairing the device to the workstation also requires key entries on the handset.

Most forensic software tools address a wide range of applicable devices, handle the most common investigative situations, and require a modest level of skill to operate. Table 4 gives an overview of available tools used in cell phone investigations, and identifies the facilities they provide: acquisition, examination, or reporting. Additional tools do exist, but only those familiar to the authors are discussed. The tools are grouped into tools that target SIMs exclusively, tools that target handsets exclusively, and toolkits that target both handsets and SIMs. The range of devices a tool addresses is often narrowed to those from certain manufacturers, with specific operating systems, or with distinct hardware architectures. To cover the broadest range of mobile phones and (U)SIMs, a set of several tools is required. More detailed information about the performance forensic tools can be found in two companion reports [Aye05, Aye07]. The remaining sections of this chapter give a synopsis for each category of tool and an overview of their capabilities. Note that the capabilities of the tools listed are constantly improving and may differ slightly from the description given.

Table 4: Forensic Tools

	Function	Target Devices
Forensic Card Reader	Acquisition, Reporting	▪ SIMs
ForensicSIM	Acquisition, Examination, Reporting	▪ SIMs and USIMs
SIMCon[8]	Acquisition, Examination, Reporting	▪ SIMs and USIMs
SIMIS	Acquisition, Examination, Reporting	▪ SIMs and USIMs
USIMdetective	Acquisition, Examination, Reporting	▪ SIMs and USIMs
BitPIM	Acquisition, Examination	▪ Certain CDMA phones using Qualcomm chipsets
Oxygen PM (forensic version)	Acquisition, Examination, Reporting	▪ Nokia phones
Oxygen PM for Symbian (forensic version)	Acquisition, Examination, Reporting	▪ Symbian phones
PDA Seizure[9]	Acquisition, Examination, Reporting	▪ Palm OS, Windows Mobile/Pocket PC, and Blackberry devices
Pilot-Link	Acquisition	▪ Palm OS devices

[8] During the preparation of this guide, SIMCon was acquired by Paraben and incorporated into its product line.

[9] During the preparation of this guide, PDA Seizure was incorporated into Device Seizure, a forensic application for mobile devices. For more information, see www.paraben-forensics.com.

	Function	Target Devices
Cell Seizure[10]	Acquisition, Examination, Reporting	▪ TDMA, CDMA, and GSM phones ▪ SIMs and USIMs
CellDEK	Acquisition, Examination, Reporting	▪ GSM and CDMA phones ▪ SIMs and USIMs
GSM .XRY	Acquisition, Examination, Reporting	▪ GSM and CDMA phones ▪ SIMs and USIMs
MobilEdit!	Acquisition, Examination, Reporting	▪ GSM phones ▪ SIMs
PhoneBase	Acquisition, Examination, Reporting	▪ GSM phones ▪ SIMs and USIMs
Secure View	Acquisition Examination Reporting	▪ TDMA, CDMA, and GSM phones ▪ SIMs
TULP 2G	Acquisition, Reporting	▪ GSM phones ▪ SIMs

3.1 (U)SIM Tools

A few forensics tools deal exclusively with (U)SIMs. These tools perform a direct read of a module's contents via a (U)SIM reader, as opposed to an indirect read via the phone handset. The richness and scope of data acquired varies with the capabilities and features of the tool. The majority of (U)SIM exclusive tools acquire the following data: International Mobile Subscriber Identity (IMSI), Integrated Circuit Card ID (ICCID), Abbreviated Dialling Numbers (ADN), Last Numbers Dialled (LND), SMS messages, and Location Information (LOCI) [Aye05, Aye07].

More capable tools provide additional information such as deleted SMS messages, properly rendered foreign language SMS messages, and EMS messages with simple graphics and sounds embedded [Jan06]. They also attempt to translate certain data such as country and network operator codes into meaningful names, and provide other facilities such as PIN administration. Below is a brief overview of some tools that are designed to acquire data specifically from SIMs.

- Forensic Card Reader (FCR) is a forensic tool from Becker & Partner that provides the means to extract data from SIMs. FCR does not generate a case file, but outputs the acquired data in an XML-format that can be viewed with the appropriate editor. FCR consists of the software and a proprietary USB smart card reader necessary for acquisition. Neither integrity hash protection nor customizable report facilities are provided.

[10] During the preparation of this guide, Cell Seizure was incorporated into Device Seizure, a forensic application for mobile devices. For more information, see www.paraben-forensics.com.

- The Forensic SIM Toolkit (FST) is a forensic tool from Radio Tactic that provides the means to extract and duplicate data from SIMs/USIMs. The case file is stored in a proprietary FST format and can be output in either an HTML or RTF/Word file-format. A USB dongle is needed to operate the software on a desktop computer. The FST acquisition terminal, a standalone unit, duplicates the contents of the target (U)SIM to a set of FST data storage cards (i.e., the Master Data Storage Card, Defense Data Storage Card, and Prosecution Data Storage Card). Data analysis can be carried out using the appropriate FST data storage card with the ForensicSIM card reader (i.e., PC/SC-compatible card reader) attached to a PC running the ForensicSIM analysis application. An MD5 checksum provides integrity protection for the generated case data. FST allows the import of archived case files and basic searches of the acquired data file.

- SIMCon is a forensic tool from InsideOut Forensics that provides the means to extract data from SIMs and USIMs. The case file has a proprietary format but can be exported to a standard ASCII text format. Additional hardware (e.g., USB dongle, proprietary card readers) are not necessary for acquisition. SIMCon acquires data from a (U)SIM via a PC/SC-compatible card reader and uses a SHA1 hash to protect the integrity of the generated case data. SIMCon provides the ability to import archived case files and export specific data out into a final report.

- SIMIS is a forensic tool from Crownhill USA that provides means to extract data from SIMs and USIMs. The case file is generated in an HTML file-format. An additional "SIM dump" feature provides a more detailed case file in a standard ASCII text format. A USB dongle is needed to operate the software on a desktop computer. SIMIS acquires information from a (U)SIM via a PC/SC-compatible card reader and generates MD5 and SHA2 hashes of the acquired data. SIMIS provides the ability to create report notes, import archived case files, search acquired data, and administer PINs. The search function can range over any archived SIMs present in the program folder.

- Quantaq Solutions' USIMdetective SIM acquisition tool provides examiners with the ability to acquire, examine, and produce reports from any SIM or USIM card using a PC/SC compatible reader. Acquired elements can be displayed in a textual or hexadecimal format. USIMdetective uses an internal hashing facility to ensure the integrity of case. Image Integrity Check (.iic) files are created with each acquisition to protect against data tampering. SHA1 and MD5 hashes ensure that the original acquired file is consistent with the reopened case file. USIMdetective provides multiple report output types ranging from a "Standard Report" to a more detailed "File Content Report."

3.2 Handset Tools

A few forensic tools deal with handsets exclusively, designed strictly for the acquisition of their internal memory. These tools sometimes stem from tools aimed at pure PDA devices and thus are useful with smart phones that incorporate operating systems with a PDA heritage, such as Palm OS and Windows Mobile devices. Others have arisen from phone management software modified to disable writing to the device. They generally exclude the capability to acquire data from SIMs using a direct read. Below is a brief overview of some tools designed for memory acquisition from mobile devices with cellular capabilities.

- PDA Seizure is a forensic software toolkit from Paraben that provides the means to extract data from mobile devices running Palm OS, Windows CE, and RIM OS. The case file has a proprietary format and can be output in an HTML file format. Acquisition occurs via a cable, IrDA, or Bluetooth interface; no additional hardware is necessary. Although the tool can be used with smart phones, the toolkit is oriented toward non-cellular devices. PDA Seizure's features include the ability to perform a logical acquisition and, for certain devices, a physical acquisition, providing views of internal memory as well as individual files and databases. An MD5 message digest is created for individual data objects and the overall case file. Additionally, the case files are encrypted to prevent tampering and data modification. PDA Seizure provides examiners with the ability to create customized reports and report notes, import archived case files, bookmark significant findings, and search the acquired data.

- Pilot-link is a non-forensic open source software suite originally developed for the Linux community as a means to transfer data between Linux hosts and Palm OS devices. Pilot-link provides the ability to extract RAM, ROM and individual files present on Palm OS devices. Two programs of interest to forensic examiners are pi-getram and pi-getrom, which respectively retrieve the physical contents of RAM and ROM from a device. Another useful program is pilot-xfer, which provides a means to acquire the contents of a device logically. Neither an overall case file, integrity hash computation, nor customizable report facility are provided.

- The forensic version of Oxygen Phone Manager (OPM) from Oxygen Software is a variant of the phone management product of the same name, which works mainly on Nokia phones. The forensic version differs from the non-forensic version by prohibiting modification to the target device. OPM provides examiners with the ability to extract data from cellular devices operating over the GSM network. OPM does not allow examiners to export an overall case file; however, acquired data is stored in multiple files (e.g., Phonebook, SMS, and Gallery) that correlate with the related function. OPM does not protect acquired data via hashing functions. Acquired data can be exported out into various supported format types.

- A forensic version of Oxygen Phone Manager for Symbian devices, from Oxygen Software, also exists. The tool targets mobile phones and smart phones that use the Symbian OS. The above-mentioned characteristics of OPM apply equally to OPM for Symbian devices.

- BitPIM is open source software available under the GNU General Public License. It is a phone management program that allows the viewing and manipulation of data primarily from CDMA cell phones by various manufacturers. A read-only check box is provided to disable writing to the phone when used for acquisition. BitPIM does not allow examiners to export or save an overall case file; however, acquired data is stored in multiple files (e.g., Phonebook, SMS, and Filesystem) and can be exported in common formats for reporting purposes. BitPIM does not protect acquired data via hashing functions.

- Phone flashing tools are available for different families of cell phones from a variety of sources. These tools are intended to load new versions of software into the memory of a phone as a means of repair and upgrade. While they do provide the means to acquire handset memory physically, they are strictly non-forensic in nature,

have little documentation and support, and do not compute an integrity hash over acquired data. Phone flashers should be used with extreme caution only after sufficient testing and study is done. Mapping the layout of recovered memory, identifying objects, and decoding data is time-consuming to perform manually. However, the process can recover such things as phone locks, deleted data, and other useful information normally not recoverable through a logical acquisition, such as historical information (e.g., the IMSI of previous (U)SIMs used with the phone).

3.3 Integrated Toolkits

Several toolkits incorporate the capabilities of both (U)SIM and handset tools under a unified framework. One advantage for those devices that involve (U)SIMs is that the results of handset and (U)SIM examinations can appear within the same generated report. This advantage disappears if another tool is used for either device, such as in the case where a particular handset might not be supported by the tool.

- Cell Seizure from Paraben is a forensic software toolkit that provides the means to extract data from GSM and non-GSM (i.e., CDMA, TDMA) cellular devices and (U)SIMs. The case file is in a proprietary format and case data can be output in either an ASCII or HTML format. Acquisition occurs via a cable, IrDA, or Bluetooth interface. Cell Seizure also allows direct acquisition of (U)SIM cards with the included RS-232 SIM card reader. The package comes complete with cables and drivers for supported phones, as well as the application software. Cell Seizure's features include the ability to perform a logical and physical acquisition, providing views of internal memory as well as individual files and databases. MD5 and SHA1 hash values are created for individual data objects and an overall message digest of the acquired case data is calculated. The case file is also encrypted, preventing tampering and data modification. Cell Seizure provides examiners with the ability to create customized reports and report notes, import archived case files, bookmark significant findings, and search the acquired data.

- CellDEK from Logicube Inc. is designed to acquire data from cell phones operating over GSM and non-GSM networks, PDAs, SIM cards and flash-based media. The CellDEK terminal contains an embedded touch-screen PC, data cables for various devices, a PC/SC SIM card reader, and a write-protected memory card reader, packaged in a rugged, watertight carrying case. The unit provides the ability to connect to cell phones and PDAs via a cable, Bluetooth or IrDA connection. Acquisitions are stored on the CellDEK's hard disk and can be moved or backed up to a USB thumb drive. All data is individually hashed using the MD5 algorithm to ensure that the integrity of the data can be verified. CellDEK generates report files in an HTML format, containing all of the data recovered. Reports can be customized with company logos and case details when entered by the examiner before acquiring the device.

- GSM .XRY is a forensic software toolkit from Micro Systemation that provides the means to extract data from GSM and non-GSM (i.e., CDMA) cellular devices and SIM/USIM cards. A USB dongle is needed to operate the software. The GSM .XRY hub provides an interface for the dongle and device cables, and interfaces for Bluetooth and IrDA. The package comes complete with cables and drivers for supported phones, as well as the application software. Data acquired from cell phone

devices are stored in the proprietary .XRY format and cannot be altered, but can be exported into external formats and viewed with third-party applications. GSM .XRY encrypts case data and compares digital signatures for consistency when previously stored case data is re-opened for examination. Additionally, case files can be locked and password protected, providing an extra layer of security against alteration. GSM .XRY provides the ability to create customized reports, import archived case files, and perform searches on the acquired data.

- MOBILedit! Forensic from Compelson Labs is an application that provides the means to acquire data logically from GSM or non-GSM (i.e., CDMA) devices and SIM cards. The tool is based on the non-forensic phone management software of the same name. Phone data can be acquired via cable, Bluetooth, or IrDA, and via a PC/SC compatible card reader for SIMs. Acquired data is stored in a proprietary case file format and can be exported to XML. Mobiledit! provides the ability to create customized reports, import archived case files and perform search queries on specific folders. Mobiledit! does not protect acquired data via hash value computations.

- PhoneBase 2 from Envisage Systems Ltd. provides the means to acquire data from GSM and non-GSM cellular devices and data contained on (U)SIMs. PhoneBase 2 uses the MOBILedit! acquisition engine for its handset support, but complements that with its own facility for (U)SIM acquisition. A USB dongle is needed to operate the software. Data can be acquired via cable, Bluetooth, IrDA or a PC/SC compatible card reader for SIMs. Acquired data is stored in a common database format and protected from tampering via a PhoneBase security (pbs) file. PhoneBase 2 provides examiners with the ability to create customized reports, import archived case files and perform search queries over multiple cases.

- Secure View is a commercial forensic tool from Susteen, derived from the company's Datapilot phone management software, which provides examiners with the ability to extract data from cellular devices operating over GSM and non-GSM (i.e., CDMA, TDMA) networks. Recent versions of Secure View also can acquire SIM card data using a PC/SC-compatible reader. Secure View does not allow examiners to export an overall case file; however, acquired data is stored in multiple files (e.g., Address book, SMS, Graphics, and Audio) that correlate with the related function. The package comes complete with cables and drivers for supported phones, and the application software. Secure View does not protect acquired data via hashing functions. However, data can be password protected, allowing only authorized access. Secure View provides a search engine that allows a subset of the acquired data to be analyzed and the ability to import pre-existing case data.

- TULP2G (2nd generation) is an open source forensic software tool from the Netherlands Forensic Institute that provides the means to acquire data from cellular GSM and non-GSM (i.e., CDMA) devices and SIMs [Bos05]. Data can be acquired via a cable, Bluetooth or IrDA interface. Reading SIMs requires a PC/SC-compatible smart card reader. TULP2G generates a set of raw data in XML format, which can be converted to a readable format using embedded XSL stylesheets. SHA1 and MD5 hashes are created over the entire case file, ensuring the integrity of acquired data. TULP2G provides the ability to create a report over selected data elements or the entire case file and import archived case files.

Tool Segregation: With the use of multiple forensic tools, the possibility exists for conflicts to occur among certain ones. Resolving such conflicts can sometimes be onerous and time consuming, and may need to be repeated across a number of forensic workstations. One method to avoid these problems is to use a product such as VMware to create a virtual machine environment on each forensic workstation for the tool to execute.

Each software tool and its operating system can be installed in a distinct virtual machine environment, independently from other tools, effectively segregating each tool from the others. Compatible collections of tools could also be isolated from incompatible tools this way. Cloning the virtual machine with the installed tool or tool collection can be done to baseline a configuration for distribution and execution at other workstations' virtual machines, establishing a common computational environment throughout an organization while simplifying the configuration process. Since multiple independent virtual machines can run simultaneously on a single workstation, several tools or tool collections that otherwise would be incompatible are readily supported.

3.4 Capabilities

Forensic software tools strive to address a wide range of applicable devices to handle the most common investigative situations with modest skill level requirements and keep the device intact. More difficult situations, such as the recovery of deleted data, require more specialized tools and expertise, and often disassembly of the device [Wil05]. The range of support provided, including phone cables and drivers, product documentation, (U)SIM readers, and updates, can vary significantly among products. The features offered such as searching, bookmarking, and reporting capabilities can also vary considerably.

Quality measures should be applied when first choosing a tool to ensure its acceptability and reapplied when updates or new versions of the tool become available to uphold consistency. Validating a tool entails defining a comprehensive test data set, loading it onto the device using the same methods a user would, and following procedures to acquire and recover the test data [Goo03, Aye05, Aye07]. While tool validation can be time consuming to perform, it is a necessary standard quality practice to follow. Forensic specialists should also receive adequate up-to-date training in the tools and procedures to employ, as a quality measure.

Mobile phone forensic tools are in their early stages of maturity. They typically have limitations in both the breadth of the devices supported and the depth of evidence recovered. Subtle errors may also be encountered in their use. For example, a data item displayed on screen may vary from the same item appearing in a generated report. Practice and experience with a tool can normally compensate for such problems and procedures can be adapted accordingly. Occasionally, new versions of a tool may fail to perform as well as a previous one.

The most important characteristic of a forensic tool is its ability to maintain the integrity of the original data source being acquired and also that of the extracted data. The former is done by blocking or otherwise eliminating write requests to the device containing the data. The latter is done by calculating a cryptographic hash of the contents of the evidence files created and recurrently verifying that this value remains unchanged throughout the lifetime of those files. Preserving integrity not only maintains credibility from a legal perspective, but it also allows any subsequent investigation to use the same baseline for replicating the analysis.

Forensic Hash: A forensic hash is used to maintain the integrity of an acquisition by computing a cryptographically strong, non-reversible value over the acquired data. After acquisition, any changes made to the data can be detected, since a new hash value computed over the data will be inconsistent with the old value. For non-forensic tools, hash values should be created manually using a tool such as sha1sum or md5sum and retained for integrity verification. Even tools labeled as forensic tools may not compute a cryptographic hash, and an integrity hash should be computed manually.

Note that mobile devices are constantly active, updating information (e.g., the device clock) continuously. Some devices, stemming mainly from a PDA heritage, are active even when turned off [Bur02]. Therefore, back-to-back acquisitions of a device will be slightly different and produce different hash values when computed over all the data. However, hash values computed over selected portions of the data, such as individual files and directories, generally remain constant. Only a few forensic tools offer more granular hash computation of files and directories. Some forensic tools also do not notify the user automatically about hash inconsistencies, placing the onus on the forensic specialist to check the hash values manually.

4. Procedures and Principles

Investigations and incidents are handled in various ways depending upon the circumstances of the incident, the gravity of the incident, and the preparation and experience of the investigation team. Digital investigations are comparable to crime scenes where investigative techniques used by law enforcement have been applied as a foundation for the creation of procedures used when dealing with digital evidence. This chapter provides an overview of various procedural models and principles that have been proposed.

4.1 Roles and Responsibilities

Whatever the type of incident, the various types of roles involved are similar. Planning should address how existing personnel fulfill these roles when responding and participating in an investigation. A set of generic roles and associated responsibilities are given below as an example. They include First Responders, Investigators, Technicians, Forensic Examiners, Forensic Analysts, and Evidence Custodians. Organizations may need to blend together these roles to match their method of operation and level of staffing. In given situations, a single individual may also be expected to perform more than one role. Nevertheless, distinguishing distinct roles is a useful way to identify associated responsibilities and ensure that the overall scope of activities is complete and sufficient.

First Responders are trained personnel who arrive first on the scene of an incident, provide an initial assessment, and begin the appropriate level of response. The responsibilities of First Responders are to secure the incident scene, call for the appropriate support needed, and assist with evidence collection.

Investigators plan and manage preservation, acquisition, examination, analysis, and reporting of electronic evidence. The Lead Investigator is in charge of making sure that activities at the scene of an incident are executed in the right order and at the right time. The Lead Investigator may be responsible for developing the evidence, preparing a case report, and briefing any findings and determinations to senior officials.

Technicians carry out actions at the direction of the Lead Investigator. Technicians are responsible for identifying and collecting evidence and documenting the incident scene. They are specially trained personnel who seize electronic equipment and acquire digital images resident within memory. More than one technician is typically involved in an incident, because different skills and knowledge are needed. Sufficient expertise should be available at the scene to address all distinct digital apparatus involved in the incident.

Evidence Custodians protect all evidence gathered that is stored in a central location. They accept evidence collected by Technicians, ensure it is properly tagged, check it into and out of protective custody, and maintain a strict chain of custody.

Forensic Examiners are specially trained personnel who reproduce images acquired from seized equipment and recover digital data. Examiners make visible evidential information on the device. Examiners may also acquire more elusive data using highly specialized equipment, intensive reverse engineering, or other appropriate means unavailable to Forensic Technicians. Having individuals serve as both an Investigator and a Forensic Examiner in an investigation should generally be avoided.

Forensic Analysts evaluate the product of the Forensic Examiner for its significance and probative value to the case.

4.2 Evidential Principles

As a backdrop to any investigation, basic principles have been proposed for dealing with digital evidence. Digital evidence by its very nature is extremely fragile, especially that found on cell phones. A phone's contents and the evidence it contains can be affected or even lost any time it is on. Digital evidence has two aspects: the physical components, peripherals, and media, that may contain data, and the data extracted from those sources. Each has associated chain of custody issues. The Association of Chief Police Officers (ACPO) Good Practice Guide for Computer based Electronic Evidence [ACPO] suggests four principles when dealing with digital evidence, summarized here:

- No actions performed by investigators should change data contained on digital devices or storage media that may subsequently be relied upon in court.
- Individuals accessing original data must be competent to do so and have the ability to explain their actions.
- An audit trail or other record of applied processes, suitable for replication of the results by an independent third-party, must be created and preserved, accurately documenting each investigative step.
- The person in charge of the investigation has overall responsibility for ensuring the above-mentioned procedures are followed and in compliance with governing laws.

The Proposed Standards for the Exchange of Digital Evidence [IOCE] suggest a similar set of principals for the standardized recovery of computer-based evidence:

- Upon seizing digital evidence, actions taken should not change that evidence.
- When it is necessary for a person to access original digital evidence, that person must be forensically competent.
- All activity relating to the seizure, access, storage, or transfer of digital evidence must be fully documented, preserved, and available for review.
- An individual is responsible for all actions taken with respect to digital evidence while the digital evidence is in their possession.
- Any agency that is responsible for seizing, accessing, storing, or transferring digital evidence is responsible for compliance with these principles.

The above sets of principles aim to ensure the integrity and accountability of digital evidence through its entire life cycle. Proper handling of evidence is always vital for it to be admissible in judicial proceedings. However, different standards may apply to different types of investigations. The degree of training and expertise required to execute a forensic task largely depends on the level of evidence required in the case [Pur]. For example, using a forensic software tool requires modest skill levels to acquire active data, compared with those required

to remove a memory chip and recover data contents, which includes both active and deleted data.

The Daubert method, a set of standards that serve as a guide when dealing with evidence in a court of law, proposes several reliability factors, which should be kept in mind when applying and reporting on a scientific technique that is being used in a forensic examination [Oco04]:

- **Testability** – Has the scientific theory or technique been empirically tested? According to K. Popper (1989) in The Growth of Scientific Knowledge, "the criterion on the scientific status of a theory is its falsifiability, refutability, and testability."

- **Acceptance** – Has the scientific theory or technique been subjected to peer review and publication? This ensures that flaws in the methodology would have been detected and that the technique is finding its way into use via the literature.

- **Error Rate** – What is the known or potential error rate? Scientific measures generally have associated error rates, which can be estimated with a fair amount of precision. Known threats exist against the validity and reliability in any test (experimental and quasi-experimental) of a theory.

- **Credibility** – What is the expert's qualifications and stature in the scientific community? Does the technique rely upon the special skills and equipment of one expert, or can it be replicated by other experts elsewhere?

- **Clarity** – Can the technique and its results be explained with sufficient clarity and simplicity so that the court and the jury can understand its plain meaning? This criterion is implicitly assumed to be incorporated in Daubert.

The procedures used to acquire evidence affect its admissibility. This applies as well to evidence acquired from mobile phones using forensic software tools [Mcc06]. Even outside of law enforcement investigations, evidence should be collected in a manner that is suitable for admissibility in court. It may not be obvious when an investigation is initiated, for example, when a computer security incident is first detected, that court action may ensue. Important evidence might be overlooked, improperly handled, or accidentally destroyed before the seriousness of the incident is realized.

4.3 Procedural Models

The Electronic Crime Scene Investigation – A Guide for First Responders, produced by the U.S. Department of Justice [DOJ01], offers the following suggestions when approaching a digital crime scene.

- **Securing and Evaluating the Scene** – Steps should be taken to ensure the safety of individuals and to identify and protect the integrity of potential evidence.

- **Documenting the Scene** – Create a permanent record of the scene, accurately recording both digital-related and conventional evidence.

- **Evidence Collection** – Collect traditional and digital evidence in a manner that preserves their evidentiary value.

- **Packaging, Transportation, and Storage** – Take adequate precautions when packaging, transporting, and storing evidence, maintaining chain of custody.

Incident Response [Man01], an "Incident Response Methodology" proposes the following phases when encountering an incident or performing a digital investigation.

- **Pre-incident preparation** – Through training and education, gain an understanding on how to respond to an incident.
- **Detection of incidents** – Develop techniques on how to detect suspect activities.
- **Initial Response** – Confirm that an incident has occurred and obtain volatile evidence.
- **Response strategy formulation** – Respond to incident based upon knowledge of all known facts collected from the Initial Response phase.
- **Duplication (forensic backups)** – Based upon the scenario, either create a physical forensic image or do a live retrieval of evidence.
- **Investigation** – Determine what happened, who did it and how the incident can be prevented in the future.
- **Security measure implementation** – Apply security measures to isolate and contain infected systems.
- **Network monitoring** – Monitor network traffic for ongoing or additional attacks.
- **Recovery** – Restore the affected system to a secure, operational state.
- **Reporting** – Document all of the details and investigative steps taken throughout the incident.
- **Follow-up** – Learn from the incident by reviewing how and why it happened and make necessary adjustments.

Research conducted at the U.S. Air Force proposes the following steps when dealing with a forensic investigation [Rei02].

- **Identification** – Recognize and determine the type of incident.
- **Preparation** – Prepare tools, techniques, search warrants, authorizations, and management approval.
- **Approach Strategy** – Maximize untainted evidence collection while minimizing the impact upon the victim.
- **Preservation** – Isolate, secure, and preserve the state of physical and digital evidence.
- **Collection** – Record the physical scene and duplicate digital evidence.

- **Examination** – Search for evidence relating to the suspected crime.
- **Analysis** – Determine significance, reconstruct fragments of data, and draw conclusions based on the evidence found. The Analysis phase may go through numerous iterations until a theory has been supported.
- **Presentation** – Summarize and provide an explanation of conclusions.
- **Return Evidence** – Ensure physical and digital property is returned to the proper owner.

Although developed primarily for computer systems, each of the above procedural models and the evidential principles discussed contain important points that should be considered when dealing with digital evidence on cell phones. Because every investigation is distinct with its own unique set of circumstances, a single definitive procedural approach is difficult to prescribe. Nevertheless, most models touch on the same key areas, though stressing different aspects. The remaining chapters of this guide follow a simple framework of four topical areas: obtaining an exhibit, making a forensic copy of its contents, obtaining evidence from the forensic copy, and reporting on the evidence obtained and process used. They are respectively referred to within this document as *preservation*, *acquisition*, *examination and analysis*, and *reporting*.

5. Preservation

Evidence preservation is the process of seizing suspect property without altering or changing the contents of data that reside on devices and removable media. It is the first step in digital evidence recovery. The chapter begins with a generic introduction to preservation, and then provides more specific guidance about cell phones.

Preservation involves the search, recognition, documentation, and collection of electronic-based evidence. In order to use evidence successfully, whether in a court of law or a less formal proceeding, it must be preserved. Failure to preserve evidence in its original state could jeopardize an entire investigation, potentially losing valuable case-related information.

The DOJ's Electronic Crime Scene Investigation report covers this subject in detail [DOJ01]. The guide offers principles, policies, and procedures to follow when encountering a digital evidence scene. The reader is directed to that report for additional information. The following is a summary of the key points to observe.

- **Securing and Evaluating the Scene**
  - Ensure the safety of all individuals at the scene.
  - Protect the integrity of traditional and electronic evidence.
  - Evaluate the scene and formulate a search plan.
  - Identify potential evidence.
  - All potential evidence should be secured, documented, and/or photographed.
  - Conduct interviews.
- **Documenting the Scene**
  - Create a permanent historical record of the scene.
  - Accurately record the location and condition of computers, storage media, other digital devices, and conventional evidence.
  - Document the condition and location of the computer system, including power status of the computer (on, off, or in sleep mode).
  - Identify and document related electronic components that will not be collected.
  - Photograph the entire scene to create a visual record as noted by the first responder.

- **Collecting Evidence**
  - Handle computer evidence, whether physical or digital, in a manner that preserves its evidentiary value.
  - Recover non-electronic evidence (e.g., written passwords, handwritten notes, blank pads of paper with indented writing, hardware and software manuals, calendars, literature, text or graphical computer printouts, and photographs).
- **Packaging, Transporting, and Storing Evidence**
  - Take no actions to add, modify, or destroy data stored on a computer or other media.
  - Avoid high temperatures and humidity, physical shock, static electricity, and magnetic sources.
  - Maintain chain of custody of electronic evidence, documenting its packaging, transportation and storage.
    - ***Packaging Procedure***
      - Properly document, label, and inventory evidence before packaging.
      - Pack magnetic media in antistatic packaging (paper or antistatic plastic bags).
      - Avoid folding, bending, or scratching computer media such as diskettes, CD-ROMs, removable media, etc.
      - Properly label evidence containers.
    - ***Transportation Procedure***
      - Avoid magnetic sources (e.g., radio transmitters, speaker magnets).
      - Avoid conditions of excessive heat, cold, or humidity while in transit.
      - Avoid shock and excessive vibrations.
    - ***Storage Procedures***
      - Ensure evidence is inventoried in accordance with authoritative policies.
      - Store evidence material in a secure area away from temperature and humidity extremes.
      - Protect evidence material from magnetic sources, moisture, dust, and other harmful particles or contaminants.

The Good Practice Guide for Computer Based Electronic Evidence [ACPO] suggests the following procedures when handling cell phones:

- Before handling, consider what other types of evidence, such as DNA or fingerprints, are needed from the phone and follow the appropriate handling procedures.
- Switching the phone off is advisable, because of the potential for loss of data if either the battery expires or network activity occurs, causing call logs or other recoverable data to be overwritten.
- If the phone remains on for some purpose, it should be kept charged and not tampered with, then switched off before transport.
- To prevent accidental operation in transit, the phone should be packaged in a rigid container, secured with support ties.
- The container should be placed into an evidence bag, sealed to restrict access, and the labeling procedures completed for the exhibit.

The remaining sections of this chapter provide supplemental information related to cell phones, following the paradigm of Securing and Evaluating the Scene, Documenting the Scene, Collecting Evidence, and Packaging, Transporting, and Storing Evidence.

5.1 Securing and Evaluating the Scene

Ensuring that the proper authorizations (e.g., a search warrant or consent from the owner) are in place is paramount for beginning an investigation. When searching a site, the team should proceed cautiously. Incorrect procedures or improper handling of a mobile phone during seizure can cause loss of digital evidence. Moreover, traditional forensic measures, such as fingerprints or DNA testing, may need to be applied to establish a link between a mobile phone and its owner or user, or for other reasons. If the device is not handled properly, physical evidence can be easily contaminated and rendered useless.

Alertness to device characteristics and issues (e.g., memory volatility) and familiarity with associated accessories (e.g., media, cables, cradles, and power adapters) are essential. For cell phones, sources of evidence include the device, (U)SIM, and media. Associated peripherals, cables, cradles, power adapters, and other accessories are also of interest. The surrounding area and rooms, other than where a device is found, should be searched to ensure related evidence is not overlooked. To avoid unwanted interaction with devices found on the scene, consideration should be given to turning off wireless interfaces, such as Bluetooth and WiFi radios, on equipment brought into the search area.

Equipment associated with the cell phone, such as removable media, (U)SIMs, or even personal computers possibly synched with it, may prove more valuable than the phone itself. Removable media varies from the size of a fingernail to that of a postage stamp, and can be easily hidden and difficult to find. Most often, removable memory cards are identifiable by their distinctive shape and the presence of pins, pin receptacles, or contacts located on their body, used to establish an electrical interface with the device.

When interviewing the owner or user of a mobile device, consider requesting any security codes or passwords needed to gain access to its contents. For example, a PIN can be set on GSM phones and some of them also have lock codes that can be set in conjunction with or in lieu of the PIN. Suspects should never be allowed to handle mobile phones or other mobile devices. Many phones have master reset codes that clear the contents of the phone to the original factory conditions. Removing the battery can also cause the contents of some devices to be lost, such as certain smart phones.

Phones may be found in a compromised state that can complicate seizure, such as immersed in a liquid. In the case of liquids, the battery should be removed to prevent electrical shorting. The remainder of the phone should be sealed in an appropriate container filled with the same liquid for transport to the lab, provided the liquid is not caustic. Some compromised states, such as blood contamination or use with explosives (i.e., as a bomb component) can pose a danger to the technician collecting evidence. In such situations, a specialist should be consulted for specific instructions or assistance, if doubt exists on how to proceed.[11]

Mobile phones and associated media may be found in a damaged state, caused by accident or deliberate action. Devices or media with visible external damage do not necessarily prevent the extraction of data from them. Damaged equipment should be taken back to the lab for closer inspection. Repairing damaged components on a mobile phone and restoring the device to working order for examination and analysis may be possible. Undamaged memory components may also be removed from a damage device and their contents recovered independently.

Legal advisors should be contacted for assistance, if needed, with the following two critical legal considerations [DOJ04]:

- Determining the extent of the authority to search and what additional legal process may be necessary to continue the search (e.g., warrant, amended consent form), if evidence is located that was not authorized in the original search authority.

- Identifying possible concerns related to applicable local policies and laws, and International, Federal, or State statutes, such as the Electronic Communications Privacy Act of 1986 (ECPA) and the Cable Communications Policy Act (CCPA).

5.2 Documenting the Scene

Evidence must be accurately accounted for and identified. Non-electronic evidence such as invoices, manuals, and packaging material may provide useful information about the capabilities of the device, the network used, account information, and unlocking codes for the PIN. The labeling process should document the case number, a brief description, signature, and the date and time the evidence was collected. Photographing the crime scene in conjunction with documenting a report of the state of each digital device and computer encountered (personal computers may contain useful data that has not been synchronized with the owner's mobile phone) can be helpful, particularly if questioned about the environment later [Kru01].

---

[11] The Netherlands Forensic Institute's procedures for preservation can be found at http://www.holmes.nl/MPF/FlowChartForensicMobilePhoneExamination.htm.

A record of all visible data should be created. All digital devices, including mobile phones, which may store data, should be photographed along with all peripherals cables, cradles, power connectors, removable media, and connections. Avoid touching or contaminating the phone when photographing it and the environment where found. If the device's display is in a viewable state, the screen's contents should be photographed and, if necessary, recorded manually, capturing the time, service status, battery level, and other displayed icons. Other characteristics such as LED activity (e.g., blinking), physical condition, physical connectivity, or visible identifiers should also be noted. Having an individual in charge to perform evidence custodian duties at the scene, alongside a partner responsible for documentation of evidence, is desirable during the collection phase [Kru01].

Actions taken on the system to view and record other volatile data not under display at the time can affect the state of the device. For example, launching an application on a smart phone can overwrite parts of memory. Furthermore, it risks activating Trojan horse code hidden within the application or accidentally hitting an incorrect key sequence, and causing unintended effects.

The chain of custody procedure is a simple yet effective process of documenting the complete journey of evidence through the lifecycle of the case. Carefully maintaining the chain of custody not only protects the integrity of evidence, but also makes if difficult for someone to argue that the evidence was tampered with [Kru01]. The documentation should answer the following questions:

- Who collected it? (i.e., devices, media, associated peripherals, etc.)
- How and where? (i.e., how was the evidence collected and where was it located)
- Who took possession of it? (i.e., individual in charge of seizing evidence)
- How was it stored and protected in storage? (i.e., evidence-custodian procedures)
- Who took it out of storage and why? (i.e., on-going documentation of individual's name and purpose for checking-out evidence)

Documentation to all of the above questions must be maintained and filed in a secure location for current and future reference.

5.3 Collecting the Evidence

The Mobile Phone Forensics Sub-Group of the Interpol European Working Party on IT Crime has identified how the ACPO Principles of Evidence apply to seizure of mobile phones [INT06]. Some key implications for proper collection are summarized below.

Isolating the phone from other devices used for data synchronization is important to keep new data from contaminating existing data. If the device is found in a cradle or connected with a computer via a cable, pulling the plug from the back of the computer eliminates data transfer or synchronization overwrites. The phone should be seized along with the cradles and cables found. Media cards, (U)SIMs, and other hardware residing in the phone should not be removed. Also, seizing the computer that was connected to the phone allows the possibility to acquire synchronized data from the hard disk that might not be obtained from the phone. Any

associated hardware such as media cards, (U)SIMs, power adapters, device sleeves, or peripherals, should be seized along with related materials such as product manuals, packaging, and software.

Isolating the phone from the radio network is important to keep new traffic, such as SMS messages, from overwriting existing data, if the phone is turned on when found. Besides the risk of overwriting potential evidence, the question may arise whether data received on the phone after seizure is within the scope of the original authority granted. Add-on programs, such as LockMe[12] and OmaiProtect[13], are also available that enable the phone lock to be set remotely upon receipt of a properly formatted message. Moreover, vulnerabilities may exist that can be exploited. For example, a malformed message sent to a Nokia 6210 phone has been shown to disable it completely, much like the a malformed ICMP packet known as the "ping of death" did to older Windows computers [Ley01].

Two basic methods for isolating the phone from radio communication and preventing these problems are to "Turn (the) device off at the point of seizure" or to "Place (the) device in a shielded container/bag" [INT06]. Alternatively, if the device has an "Airplane Mode" function, the setting could be enabled [Bur02]. Each method has certain drawbacks, however.

- Turning off the phone may activate authentication codes (e.g., SIM PIN and/or handset security codes), which are then required to gain access to the device, complicating acquisition and delaying examination.

- Keeping the phone on, but radio isolated, hastens battery life due to increased power consumption as it tries unsuccessfully to connect to a network, raising its signal strength to the maximum. After some period, failure to connect to the network may cause certain phones to reset or clear network data that otherwise would be useful if recovered [Smi05]. Containers attenuate the radio signal, but not necessarily eliminate it completely, allowing the possibility of communications being established with a cell tower, if in its immediate vicinity. The risk of improperly sealing the radio isolation container and unknowingly allowing access to the cell network also exists.

- Enabling "Airplane Mode" requires interaction with the phone via the keypad, which poses some risk – less so, if the technician is familiar with the device in question and documents the actions taken (e.g., on paper or on video).

If user data resides in battery-dependent volatile memory, expiration of the battery would be disastrous. Before collecting such a mobile phone, the power state must be considered. For example, the device may be fully charged, receiving power from a charger or cradle plugged into an outlet, or extremely low on battery power. Steps must be taken to maintain the battery level at an appropriate level until a successful acquisition takes place. This may be especially challenging if the device needs to be radio isolated, requiring it to be placed in the container together with a portable source of supplemental power (e.g., a disposable charger such as

---

[12] Product information is available at http://www.allaboutsymbian.com/software/item/LockMe1.php.

[13] Product information is available at: http://shop.my-symbian.com/PlatformProductDetail.jsp?siteId=695&jid=9XE2C5FBA428B2D242AXA4AB13E866AX&platformId=4&productType=2&catalog=0&sectionId=0&productId=187426.

cellboost[14] or a battery-powered charger[15]), after full charging. If sufficient power cannot be supplied, consideration should be given to switching off the phone to preserve battery life, documenting the current device state and noting the time and date of the shutdown.

Charging may also be required post-examination, if reexamination of the original device is anticipated due to expected challenges to the results of the initial examination. Otherwise, replication of results cannot be achieved once battery depletion causes loss of volatile memory content. Even when the phone is isolated, content changes may occur on an active device that could be undesirable, such as the execution of a scheduled script that purges old data.

To conserve power, some smart phones are normally configured to enter energy savings mode and shut off the display after a short period of inactivity. Some phones also shut themselves off if the battery level drops below a certain threshold to protect data stored in volatile memory, which defeats the original purpose of keeping it turned on. Keeping a device in the active state is troublesome, requiring periodic interaction with the device. Anecdotal evidence suggests that built-in and add-on protections, such as user authentication and content encryption, are not employed for the vast majority of phones seized. If additional power cannot be supplied to a device and it is turned off to conserve power and preserve memory contents, the risk of encountering a protection mechanism when turned on again should overall be low. Moreover, authentication mechanisms, such as passwords, typically cannot be deactivated without first satisfying the mechanism (e.g., supplying the correct password). For these reasons, procedures for some organizations may recommend turning off certain classes of phones, if found powered on.

"A small number of mobile communication devices … use alkaline batteries as a power source. Consideration should be given to replacing the batteries prior to transit to minimize the risk of data loss due to complete battery discharge before the device reaches the examination unit [INT06]." Some smart phones use rechargeable batteries that are replaceable, and a fully charged replacement battery can be substituted, if available. Such phones keep a small charge to the device to maintain volatile data for a short amount of time during battery replacement. To prevent loss of volatile data, batteries must be replaced quickly.

The time maintained on the phone may be set independently of that from the network. Always record the date and time shown on the handset, if it is turned on, and compare them with a reference clock, noting any inconsistencies. If the screen is dim due to power management, it may be necessary to press an insignificant key such as the volume key to light the screen. When preparing the packing labels, be sure to record the manufacturer and model of the seized equipment, and also its condition. The make and model may be branded on the body of the handset and also appear in the interior of the handset under the battery. However, do not remove the battery to read this information, if the phone is on.

Caution should be exercised when handling a phone suspected of being modified, especially if the modifications are presumed to be done by a security-minded individual or organization. Certain types of modifications to the software applications and operating system of the device

---

[14] Product information is available at http://www.cellboost.com/us/.

[15] Product information is available at: http://www.chargetogo.com/specs.htm and http://www.paramountzone.com/mobile_charger.htm.

might affect the way it is handled. The following is a list of examples of some classes of modifications to consider:

- **Security Enhancements** – Organizations and individuals may enhance their handheld devices with add-on security mechanisms. A variety of visual login, biometric, and token-based authentication mechanisms are available for smart phones to use as replacements or supplements to password mechanisms. Improper interaction with a mechanism could cause the device to lock down and even destroy its contents. This is particularly a concern with mechanisms that use security tokens whose presence is constantly monitored and whose disconnection from a card slot or other device interface is immediately acted upon.

- **Malicious Programs** – A phone may contain a virus or other malicious software. Such malware[16] may attempt to spread to other devices over wired or wireless interfaces, including cross platform jumps to completely different platforms such as Windows computers. Common utilities or functions may also be intentionally replaced with versions that contain software designed to alter or damage data present on a phone. Such Trojan-bearing programs could conditionally be activated or suppressed based on conditions such as input parameters or hardware key interrupts. Watchdog applications could also be written to listen for specific events (e.g., key cords or over the air messages) and carry out actions such as wiping the device clean.

- **Key Remapping** – Hardware keys may be remapped to perform a different function than the default. A key press or combination of key presses intended for one purpose could launch an arbitrary program.

5.4 Packaging, Transporting, and Storing Evidence

Once the device is ready to be seized, the forensic specialist should seal the device in a static proof bag and tag it. The individual who seizes the device must sign and date the tag to initiate a chain of custody. The device should be secured properly to prevent keys from being pressed accidentally (e.g., turning the device on) when in the evidence bag. Hard containers are manufactured specifically for this purpose and are recommended for use.[17] Radio frequency isolation bags are also available for attenuating a device's radio signal and should be used with phones left on. An independent external power charger may be connected and placed in the bag with the device to keep the power level full during transit. Phones with volatile memory resident user data, which are left off, turned off, or in "Airplane Mode," may be packaged to allow a power adaptor to be connected to the device through a hole in the evidence bag to keep the power level high. Rechargeable devices can usually be powered through a compatible cigarette-lighter adapter cable to keep charge to the device while in transit. If a power adapter is used in conjunction with a radio frequency isolation bag, the cable must be properly shielded to prevent it from serving as an antenna and nullifying the effect of the isolation bag.

Digital devices are fragile and easily damaged. When a device is transported, it should be handled carefully and adequately protected from shock, breakage, and extreme temperature. Due to the volatile nature of some smart phones, they should immediately be checked into a

[16] For more information, see http://www.eweek.com/article2/0,1895,1750109,00.asp.

[17] For example, see http://www.forensicts.co.uk/fts-packaging.asp.

forensic laboratory to be processed and the evidence custodian should be made aware of the situation regarding power requirements. Battery powered devices held in storage for more than a few days risk power depletion and data loss, unless a process is in place to avoid this outcome.

Storage facilities that hold evidence should provide a cool, dry environment appropriate for valuable electronic equipment. All evidence should be in sealed containers, in a secure area with controlled access.

6. Acquisition

Acquisition is the process of imaging or otherwise obtaining information from a digital device and its peripheral equipment and media. Performing acquisition at the scene has the advantage that loss of information due to battery depletion, damage, etc. during transportation and storage is avoided. However, finding a controlled setting in which to work, having the appropriate equipment, and satisfying other prerequisites may not be possible at the scene, but readily achievable within a laboratory setting. For the purpose of discussion, a laboratory environment is assumed throughout this chapter. Powered on devices should be handled with caution in a radio frequency shielded work area or have their wireless communications disabled by some other means.

Radio Isolation Techniques: A number of techniques exist for isolating a mobile phone from cell tower communications [INT06]. Because communications are blocked, the handset continues increasing its signal strength up to the maximum as it continually attempts to make contact. This activity significantly shortens battery life. The device should be fully charged prior to examination and consideration should be given to having a fixed or portable power source attached.

Use a jamming or spoofing device - Emitting a signal stronger than a cell phone's or interfering with the signal can render a cell phone useless. Another technique involves tricking the phone into thinking a "no service" signal is coming from the nearest cell tower. Because such devices can affect communications in the surrounding public airspace beyond the examination area, they are illegal in many countries. [Wyl00, NIJ05]

Use a shielded work area - Shielding an entire work area can be an expensive but effective way to conduct examinations safely in a fixed location. A "Faraday tent" is a cheaper alternative that also allows portability. Feeding cables into the tent is problematic, however, since without proper isolation they can behave as an antenna, defeating the purpose of the tent. The work space can also be very restrictive.

Use a shielded container - A portable shielded container can allow examinations to be conducted safely once the phone is situated inside. Cables into the box must be fully isolated to prevent network communications from occurring.

Use a substitute (U)SIM - A substitute (U)SIM mimics the identity of the original and prevents network access by the handset. Such cards trick the handset into accepting them as the original (U)SIM. The technique allows examinations to be conducted safely at any location.

Arrange for the network service to be disabled - The cellular carrier providing service to the device might be induced to disable service. The service provider or network operator must be determined and contacted with details identifying the service to be disabled (e.g., the equipment identifier, subscriber identifier, phone number). Such information is not always readily available, however, and the coordination and confirmation process also imposes delay.

Acquisition should occur at a forensics laboratory once the seized equipment has arrived and been checked in. The forensic examination begins with the identification of the device. The type of device, its operating system, and other characteristics determine the route to take in creating a forensic copy of the contents of the device. Only a few forensic software tools currently exist that image certain types of phones, and no single tool presently handles the full

range of phones on the market [Aye05, Aye07]. The type of phone under examination, therefore, generally dictates which tools to use in an investigation.

6.1 Device Identification

To proceed effectively, devices need to be identified by the make, model, and service provider. This information allows examiners to select the appropriate tools for acquisition. Individuals may attempt to thwart specialists by altering the device to conceal its true identity. Device alteration could range from removing manufacturer labels to filing off logos. In addition, the operating system and applications may be modified or in rare situations completely replaced, and appear differently as well as behave differently than expected. For example, removing or replacing splash screens is a widely discussed modification in phone forums.

If the phone is powered on, the information appearing on the display can sometimes help identify the type of phone. For example, the manufacturer's or service provider's name may appear on the display, or the screen layout may indicate the family of operating system used. Information such as the manufacturer's label may be found in the battery cavity (e.g., Make, Model, IMEI, or ESN). Removing the battery from the cavity of a phone, even when powered off, can affect its state, particularly the contents of volatile memory. Most phones keep user data in non-volatile memory, however, with the exception of certain smart phones. If the phone is powered on, battery removal will power it off, possibly causing an authentication mechanism to trigger when again powered on.

Other clues that allow identification of a device include such things as manufacturer logos, serial numbers, the cradle, and power adapter. Overall, knowing the make and model helps to limit the potential service providers, by differentiating the type of network the device operates over (i.e., GSM, non-GSM), and vice versa. Synchronization software discovered on an associated computer also helps to differentiate among operating system families. Further means of identification include the following areas:

- **Device Characteristics** – The make and manufacturer of a phone can sometimes be identified by its observable characteristics (e.g., weight, dimensions, and form factor), particularly if unique design elements exist. Various Web sites contain databases of phones that can be queried based on selected attributes to identify a particular device and obtain its specifications and features.[18] Coverage is considerable, but not extensive or complete, and may require consulting more than one repository before making a match.

- **Device Interface** – The power connector is often specific to a manufacturer and a reliable aid to identification. With familiarization and experience, the manufacturers of certain devices can be readily identified. Similarly, the size, number of contacts, and shape of the data cable interface of a phone used to create a connection to a host computer are often specific to a particular manufacturer and may prove helpful in

[18] Several examples of such Web sites include the following: http://www.phonescoop.com/phones/finder.php, http://www.gsmarena.com/search.php3, and http://mobile.softpedia.com/phoneFinder.

identification.[19] Unfortunately, the available databases for these interfaces lack the broad coverage to be of assistance.

- **Device Label** – For phones powered off, information obtained from within the battery cavity can be revealing, particularly when coupled with an appropriate database. The manufacturer's label often lists the make and model number of the phone and also unique identifiers, such as the Federal Communications Commission Identification Number (FCC ID) and an equipment identifier (IMEI or ESN). The FCC and equipment identifiers can be found on cell phones sold in the U.S. domestic market.

  For GSM or other (U)SIM bearing phones, the (U)SIM is usually located under the battery and is typically imprinted with a unique identifier called the Integrated Circuit Card Identification (ICCID). For powered on GSM and UMTS phones, the International Mobile Equipment Identifier (IMEI) can be obtained by keying in *#06#. Similar codes exist for obtaining the Electronic Serial Number (ESN) from powered on CDMA phones. Various sites on the Internet offer databases for querying the identifier and providing information about the device.

  - The IMEI is a 15-digit number that indicates the manufacturer, model type, and country of approval for GSM devices. The initial 8-digit portion of the IMEI, known as the Type Allocation Code (TAC), gives the model and origin. The remainder of the IMEI is manufacturer specific, with a check digit at the end [GSM04]. A database lookup service is available from the GSM numbering plan Web site.[20]

  - The ESN is a unique 32-bit identifier recorded on a secure chip in a mobile phone by the manufacturer. The first 8-14 bits identify the manufacturer and the remaining bits the assigned serial number. Many phones have codes that can be input into the handset to display the ESN. Hidden menus can also be activated on certain phones by placing them in "test mode" through the input of a code. Besides the ESN, other useful information such as the phone number of the device can be obtained. Manufacturer codes can be checked on-line at the Telecommunications Industry Association Web site.[21]

  - The ICCID of the (U)SIM can be up to 20 digits long. It consists of an industry identifier prefix (89 for telecommunications), followed by a country code, an issuer identifier number, and an individual account identification number [ITU06]. The country and network operator name can be determined by the ICCID. If the ICCID does not appear on the (U)SIM, it can always be obtained with a (U)SIM acquisition tool. The GSM numbering plan Web site supports ICCID queries for this information[22].

---

[19] For example, see http://www.gsm-technology.com/gsm.php/en,unlock,subpage_id,pinout.html.

[20] For more information, see http://www.numberingplans.com/?page=analysis&sub=imeinr.

[21] For more information, see http://www.tiaonline.org/standards/resources/esn/codes.cfm.

[22] For more information, see http://www.numberingplans.com/?page=analysis&sub=simnr.

- The first 3 characters of the FCC ID are the company code; the next 14 are the product code. The FCC provides a database lookup service that can be used to identify a device manufacturer and retrieve information about the phone, including photos, user manual, and radio frequency test results.[23]

- **Reverse Lookup** – If the telephone number of the phone is known, a reverse lookup can be used to identify the network operator (e.g., Cingular) and the originating city and state (e.g., Washington D.C.). For example, FoneFinder is a service to obtain such information by inputting the user's area code, three-digit prefix, and the seventh digit of the phone number.[24] The network operator's Web site typically contains lists of supported phones that can be used to narrow down and possible identify the phone in question. Because phone numbers can be ported among service providers, in many situations more up-to-date information is needed. The Number Portability Administration Center (NPAC) provides an automated phone system for law enforcement agencies to determine the current service provider assigned to a number and obtain contact information.[25] The service covers both U.S. and Canadian phone numbers.

6.2 Tool Selection and Expectations

Once the make and model of the phone are known, available manuals can be retrieved and studied. The manufacturer's Web site is a good place to begin. Typing the model number into Google or another search engine can also reveal a significant amount of information about the device. As mentioned earlier, the device being acquired largely dictates the choice of forensic tools. The following criteria have been suggested as a fundamental set of requirements for forensic tools [Car02], and should be considered when a choice of tools is available:

- **Usability** – the ability to present data in a form that is useful to an investigator

- **Comprehensive** – the ability to present all data to an investigator so that both inculpatory and exculpatory evidence can be identified

- **Accuracy** – the quality that the output of the tool has been verified and a margin of error ascertained

- **Deterministic** – the ability for the tool to produce the same output when given the same set of instructions and input data

- **Verifiable** – the ability to ensure accuracy of the output by having access to intermediate translation and presentation results

---

[23] For more information, see http://www.fcc.gov/oet/fccid/.

[24] For more information, see http://www.fonefinder.net/.

[25] More information about the service, including user registration, can be found at http://www.npac.com by selecting the Law Enforcement/911 tab at the left-hand side of the page.

Other factors in choosing among software tools include the Daubert considerations mentioned earlier in section 4.2 (particularly Acceptance) and the following items:

- **Quality** – technical support, reliability, and upgrade version path
- **Capability** – supported feature set, performance, and richness of features with regard to flexibility and customization
- **Affordability** – cost versus benefits in productivity

Experimenting with various tools on test devices to find out which acquisition tools work efficiently with particular device types is highly recommended. Besides gaining familiarity with the capabilities of the tool, experimentation allows special purpose search filters and custom configurations to be set up before use in an actual case. In addition, any needed software updates from the manufacturer can be installed.

Established procedures should guide the technical process of acquisition, as well as the examination of evidence. New circumstances can arise sporadically that require adjustment to existing procedures, and in some situations require new procedures and methods be devised. Recent examples include (U)SIMs being permanently bonded into the handset of certain phones, handsets that are capable of supporting two (U)SIMS, and phones that block logical acquisition ports until a connection is made with a cell tower. Procedures must be tested to ensure that the results obtained are valid and independently reproducible. The development and validation of the procedures should be documented and include the following steps [DOJ04]:

- Identifying the task or problem
- Proposing possible solutions
- Testing each solution on an identical test device and under known control conditions
- Evaluating the results of the test
- Finalizing the procedure

6.3 Memory Considerations

A mobile phone contains various types of volatile and non-volatile memory over which several general categories of data can reside: storage for the operating system code, including the kernel, device drivers, and system libraries; memory for executing operating system applications and for storing and executing user applications loaded onto the device; and user storage for various kinds of text, image, audio, video, and other data files, including PIM application data. The structure of phone memory may be partitioned into fixed areas for certain data, such as phonebook entries, calendar entries, call logs, and SMS messages, or assigned dynamically from a common shared pool of memory. Memory may also be structured more rigorously as a formatted file system.

The type of memory in which each category of data is stored and the memory structure employed vary among manufacturers and often are based on the characteristics of the

operating system used. Even for a given model of phone, data storage location assignments can vary somewhat between subsidized phones supplied by different network carriers, depending on the adaptations made for the carriers by the manufacturer. Firmware updates sent out by a network carrier can also affect data locations [Vam07].

Figure 4 illustrates the most typical arrangement in which user files reside in non-volatile memory, such as Flash ROM or possibly a micro hard drive, along with the operating system code. Since the storage is persistent, the contents are unaffected by complete power drainage. Volatile memory is used for dynamic storage and its contents are lost when power is drained from the phone.

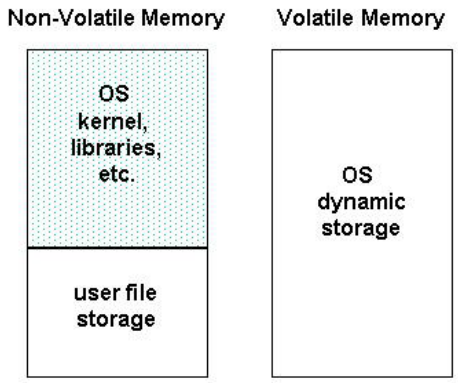

Figure 4: Storage Assignments

A common alternative memory arrangement, used mainly in smart phones that have a PDA heritage, is shown in Figure 5. Volatile memory is used for dynamic storage and user file storage. Non-volatile memory is used mainly to hold the operating system code, and possibly PIM data or files backed up from volatile memory by the user. Completely draining power from the phone clears the contents of volatile memory, while non-volatile memory is unaffected.

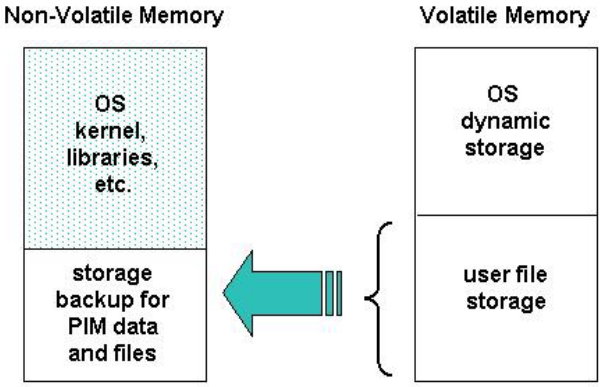

Figure 5: Alternative Storage Assignments

A (U)SIM is similar to a mobile phone insofar as it has both volatile and non-volatile memory that can contain the same general categories of data as found in a mobile phone. It can be thought of as a trusted sub-processor that interfaces to a phone and draws power from it. The file system of a SIM resides in nonvolatile memory and is organized as a hierarchical tree structure, composed of three types of elements: the root of the file system (MF), subordinate

directory files (DF), and files containing elementary data (EF). Figure 6 illustrates the structure of the file system. The EFs under DF_{GSM} and $DF_{DCS1800}$ contain mainly network related information for different frequency bands of operation. The EFs under $DF_{TELECOM}$ contain service related information.

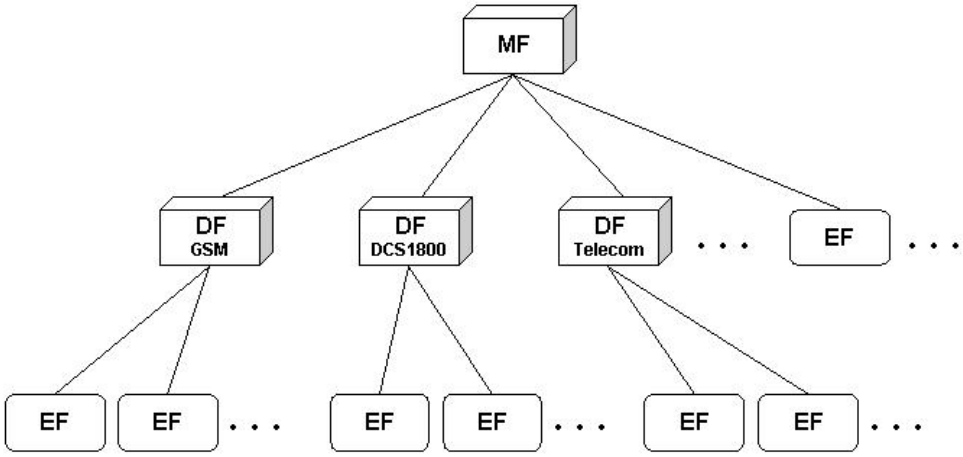

Figure 6: SIM File System

Various types of digital evidence can exist in elementary data files scattered throughout the file system and be recovered from a (U)SIM. Some of the same information held in the (U)SIM may be maintained in the memory of the mobile phone and encountered there as well. Besides the standard files defined in the GSM specifications, a (U)SIM may contain non-standard files established by the network operator [Cas06]. Several general categories of evidence that can be found in standard elementary data files are as follows [Jan06]:

- Service-related Information, including unique identifiers for the (U)SIM, the Integrated Circuit Card Identification (ICCID), and the subscriber, the International Mobile Subscriber Identity (IMSI)
- Phonebook and Call Information, known respectively as the Abbreviated Dialling Numbers (ADN) and Last Numbers Dialled (LND)
- Messaging Information, including both Short Message Service (SMS) textual messages and Enhanced Messaging Service (EMS) simple multimedia messages.
- Location Information, including Location Area Information (LAI) for voice communications and Routing Area Information (RAI) for data communications

6.4 Unobstructed Devices

An unobstructed device refers to a device that does not require a password or other authentication technique to be satisfied to gain access to the device and perform an acquisition. Anecdotally, most devices seized in investigations appear to fall into this category. Unobstructed devices include mainly CDMA phones, freestanding (U)SIMs, and GSM phones containing a (U)SIM. A GSM phone that contains no (U)SIM is considered to be an "Obstructed Device," discussed later in this chapter. Depending on the type of the phone, potential evidence, particularly user data, may reside in either the volatile or non-volatile

memory, and must be handled accordingly. While the recoverable memory of (U)SIMs is non-volatile and in and of itself not a concern when found freestanding, their insertion and removal from a GSM mobile phone has forensic implications on the contents of the phone that must be taken into account.

To preserve the integrity of the data, examiners should handle the original evidence as little as possible. Generally, it is recommended to create a "master" forensic copy of the device case file first, which is kept completely pristine. The master copy is then used to create additional mirror images needed for analysis and examination of evidence [Gas03]. A strong one-way cryptographic hash (e.g., SHA1) should be performed to ensure that the additional images created from the master copy are identical.

6.4.1 Mobile Phone Acquisition

Often phones are submitted for laboratory processing with only specific items requested for recovery, such as phone call logs or images. If any doubt or concerns exist about the requested data, contacting the person who initiated the examination for clarification is recommended. Though it is not always necessary to recover all available data, a complete acquisition avoids having to redo the process later, if other data is needed, and the possibility that technical problems may arise on a later attempt.

To acquire data from a phone, a connection must be established to the device from the forensic workstation. Before performing an acquisition, the version of the tool being used should be documented, along with any applicable patches or errata from the manufacturer applied to the tool. As mentioned earlier, caution should be taken to avoid altering the state of a mobile phone when handling it, for example, by pressing keys that could potentially corrupt or erase evidence. Once the connection has been established, the forensic software suite can proceed to acquire data from the device. Appendix C gives an overview of the steps involved in an acquisition. They entail selecting a connection, identifying the device to be acquired, identifying the data to be recovered, and viewing the recovered data.

Acquiring a device's contents logically, the prevailing technique used by present day forensic tools, requires the device to be switched on. This effectively means that the first evidentiary principle mentioned in section 4.2 – *actions taken should not modify data contained on the device* – cannot be complied with, strictly speaking. Therefore, the goal during acquisition is to affect memory contents as little as possible and then only with the knowledge of what is occurring internally, relying more on adherence to the second and third evidentiary principles that respectively emphasize high competence of the specialist and the capture of a detailed audit trail of the actions taken [ACPO].

The date and time maintained on the mobile phone is an important piece of information. The date and time may be obtained from the network or manually set by the user. Suspects may manually set the day or time to a completely different value from the actual one to leave misleading values in the call and message records found on the phone. If the phone was on when seized, the date and time maintained and differences from a reference clock should have already been recorded, as mentioned earlier. Nevertheless, confirmation at acquisition may prove useful. If the phone was off when seized, the date and time maintained and differences from a reference clock should be recorded immediately when first turned on in the laboratory. Note that actions taken during acquisition, such as removal of the battery to view the device label, may affect the time value maintained.

Unlike desktop machines or network servers, only a few phones have a hard disk and rely instead completely on semiconductor memory. Specialized software exists for performing a logical acquisition of PIM data and, for certain phones, producing a physical image. However, the contents of a phone are typically dynamic and continually changing. Two back-to-back acquisitions of a device using the same tool may produce different results overall (e.g., if memory compaction occurs), though the majority of information, such as PIM data, remains unchanged.

Increasingly, mobile phones come with a built-in slot for some family of memory cards. Forensic tools that acquire the contents of a resident memory card normally perform a logical acquisition. To recover deleted data that might reside on the memory card, a direct acquisition can be performed on it after the contents of the mobile phone have been successfully acquired. With either type of acquisition, the forensic tool may or may not have the capability to decode recovered phone data stored on the card (e.g., SMS text messages), requiring additional manual steps to be taken.

After an acquisition is finished, the forensic specialist should always confirm that the contents of a device were captured correctly. On occasion, a tool may fail its task without any error notification and require the specialist to reattempt acquisition with the same tool or another tool. Similarly, some tools do not work as well with certain devices as others do, and may fail with an error notification. Thus, where possible, it is advisable to have multiple tools available and be prepared to switch to another if difficulties occur with the initial tool.

Invariably, not all relevant data viewable on a phone using the available menus can be captured through a logical acquisition. For example, draft and archived messages are sometimes not recovered by forensic tools. Manually scrutinizing the contents via the phone interface menus while video recording the process not only allows such items to be captured and reported, but also confirms that the contents reported by the tool are consistent with observable data. Manual acquisition must always be done with care, preserving the integrity of the device in case further, more elaborate acquisitions need to be conducted.

The contents of a phone's memory often contain information, such as deleted data, that is not recoverable through either a logical acquisition or a manual examination. Lacking a software tool able to perform a physical acquisition, it may be necessary to turn to a hardware-based technique. Two techniques commonly used for non-volatile memory are acquisition through a standardized Joint Test Action Group (JTAG) test interface, if supported on the device, and acquisition by directly reading memory that has been removed from the device [Will05]. The techniques are discussed in a bit more detail in section 6.5.3, under Hardware Base Methods.

6.4.2 GSM Phone Considerations

CDMA phones and other mobile phones that do not use an identity module are relatively straightforward insofar as the acquisition entails a single device. The considerations described above are the main considerations to be addressed. GSM phones on the other hand are slightly more complex because of the handset/(U)SIM partitioning of the phone. Depending on the type of phone, whether it is on or off, and other conditions, the phone and (U)SIM could be acquired jointly or separately.

If the mobile phone is active, a joint acquisition of the handset and (U)SIM contents should be carried out before the (U)SIM is acquired directly. A direct acquisition recovers deleted

messages present on a (U)SIM, while an indirect acquisition via the handset does not. The SIM must be removed from the phone and inserted into an appropriate reader for direct acquisition. One reason for this sequence is that removal of the (U)SIM, which is typically located beneath the battery, can result in the loss of non-volatile memory due to the power disruption. Additionally, the fact that the device was kept in an active state when seized may be an indication that some concern exists about triggering authentication or some other security mechanism if power is lost.

A well-known forensic issue that arises when following this sequence is that the reported status of unread SMS text messages is inconsistent between each (U)SIM acquisition – the first one declaring it to be unread, while the second one read. Reading an unread SMS message from a (U)SIM indirectly through the handset causes the operating system of the phone to change the status accordingly. Had the (U)SIM been read directly by a tool, no change in status would occur. One way to avoid the inconsistency is to omit selecting the recovery of (U)SIM-resident SMS text messages when performing the joint acquisition, if the tool allows such an option.

If the mobile phone is inactive, the contents of the (U)SIM may be acquired independently before that of the handset. The (U)SIM acquisition should be done directly through a (U)SIM reader. The handset acquisition should be attempted without the (U)SIM present. Many phones permit an acquisition under such conditions, allowing PIN entry for the (U)SIM to be bypassed, if it were enabled. If the acquisition attempt is unsuccessful, the (U)SIM can be reinserted and a second attempt made. Performing separate independent acquisitions (i.e., acquiring the (U)SIM before acquiring the contents of the handset) avoids any operating system-related forensic issues associated with an indirect read of (U)SIM data. However, removing the SIM can reportedly cause data to be deleted on some phones [Goo03]. In addition, if removing the battery is required to gain access to the SIM, a loss of the date and time values can occur in certain phones [Mel04]. Similarly, when the battery is removed from certain smart phones, the user data present in volatile memory can be lost if a second backup battery is not built-in to support battery replacement or cannot maintain volatile memory for a sufficient time. In situations where lost data can occur, the acquisition sequence described at the beginning of this section for active phones should be followed.

6.4.3 (U)SIMs

Similar to a mobile phone, to acquire data from a (U)SIM, a connection must be established from the forensic workstation to the device, using a reader. As before, the version of the tool being used should be documented, along with any applicable patches or errata from the manufacturer applied to the tool. Once the connection has been established, the forensic software tool can proceed to acquire data from the device.

Capturing a direct image of the (U)SIM data is not possible because of the protection mechanisms built into the module. Instead, forensic tools send command directives called Application Protocol Data Units (APDUs) to the (U)SIM to extract data logically, without modification, from each elementary data file of the file system. The APDU protocol is a simple command-response exchange. Each element of the file system defined in the GSM standards has a unique numeric identifier assigned, which can be used to walk through the file system and recover data by referencing an element and performing some operation, such as reading its contents.

Because (U)SIMs are highly standardized devices, few issues exist with regard to a logical acquisition. The main consideration is selecting a tool that reports the status of any PINs and recovers the data of interest. Vast differences exist in the data recovered by (U)SIM tools, with some recovering only the data thought to have the highest relevance in a typical investigation, and others performing a complete recovery of all data, even though much of it is network related with little investigative value.

6.5 Obstructed Devices

Obstructed devices typically refer to devices that are shut off and require successful authentication using a password or some other means to gain access. Common obstructed devices include mobile phones with missing identity modules, with PIN-enabled identity modules, or with an enabled phone lock setting. Password locked memory cards are beginning to emerge as the capability to set such locks appears in more phones. Content encryption capabilities are currently not offered as a standard feature in most cell phones, but may be available through an add-on application.

A number of ways exist to recover data from obstructed devices. They fall into three classes: investigative, software-based, and hardware-based methods. Experimenting with a seized device to bypass or overcome its security mechanisms should be avoided and instead done with a test device of the same make, model, and version of software. Seemingly simple actions can cause the device to lock permanently or lose data, making evidence recovery more difficult or impossible. PIN and password-protected devices may require the expertise of a specially trained forensic specialist to gain access to the device contents in a forensically sound manner, once conventional techniques have been exhausted. Preserving the contents of the device when conventional techniques are applied is vital to allow more sophisticated techniques to succeed.

Software and hardware-based methods are often directed at a particular device or narrow class of device, as are some investigative methods. In developing a method, the following actions should be considered for determining possible approaches:

- Contacting the device manufacturer and service provider for information on known backdoors and vulnerabilities that might be exploited.
- Reviewing manufacturer specifications and other documentation when formulating plausible approaches.
- Contacting commercial evidence recovery professionals that specialize in handheld devices.
- Searching Internet sites for developer, hacker, and security exploit information.
- Contacting device maintenance and repair companies, as well as commercial organizations that provide architecture information on handheld device products.[26]

[26] For handheld device architecture information, see http://www.portelligent.com/prodserv.asp.

6.5.1 Investigative Methods

Investigative methods are procedures the investigative team can apply, which require no forensic software or hardware tools. The most obvious methods are the following:

- **Ask the suspect** – If a device is protected with a password, PIN, token, or other authentication mechanism involving knowledge-based authentication, the suspect can be queried for this information during the initial interview.

- **Review seized material** – Passwords or PINs may be written down on a slip of paper and kept with or near the phone, at a desktop computer used to synchronize with the phone, or on the suspect's person, such as within a wallet, and may be recovered through visual inspection. Packaging material for a (U)SIM or a GSM phone may disclose a PIN unlocking key (PUK) that can be used to reset the value of the PIN.

- **Manually supply commonly used input** – Users may weaken a mechanism by the way in which it is used. For example, if the (U)SIM of a mobile phone requires a 4-digit PIN, an examiner may wish to try a commonly used PIN combination (e.g.,1-2-3-4, 0-0-0-0, etc.), as one of the three attempts allowed before the device is completely locked down [Kni02]. Most (U)SIM tools, but not all, report the remaining number of attempts.

- **Ask the service provider** – If a GSM mobile phone is protected with a PIN-enabled (U)SIM, the SIM's identifier (i.e., the ICCID) can be obtained from it and used to request the PUK from the service provider and reset the PIN. Some service providers offer the ability to retrieve the PUK on-line, by entering the telephone number of the phone and certain subscriber information into public web pages set up for this purpose.

- **Exploit possible insecure settings** – Some models of phones may easily yield access because of common user configuration errors. For example, certain Motorola phones provide a two-level access mechanism that can be enabled on the handset: a phone lock needed to gain access to the device and a security code needed to reset the phone lock in case it is forgotten. A user may set the phone lock, but not change the security code from its default value, allowing anyone to gain access using the default security code value to reset or disable the phone lock.

6.5.2 Software-based Methods

Software-based methods involve software techniques used to break or bypass authentication mechanisms. While some general-purpose software techniques and tools may apply to a class of mobile phones, most of the techniques are specialized for a specific model within a class. When a specialized technique is developed, it is normally programmed and tested on an identical test device. Software-based methods include the following:

- **Exploit known weaknesses in authentication** – If an authentication mechanism is weak, exploiting the weaknesses to defeat it may be possible. For example, early password protection schemes on Palm OS PDAs obfuscated the password using a reversible algorithm [Kin01], allowing it to be recovered easily from devices running version 4.0 or earlier, using a utility. Similarly, early versions of the Pocket PC

ActiveSync protocol allow unlimited authentication attempts to be made without penalty, allowing a dictionary attack of commonly used passwords to be attempted.

Some devices may have a reserve password or master password built into the authentication mechanism, which allows unfettered access when entered, bypassing the phone lock set by the user [Kni02, Smi06]. For example, the master security code for overriding the phone lock mechanism on certain Nokia handsets can be calculated directly from the equipment identifier.[27] A number of GSM mobile phones allow acquisition, if a PIN-enabled (U)SIM is missing or removed from the device, as mentioned earlier. It is also possible to create a substitute (U)SIM for certain models of phones that fools them into treating the (U)SIM as though it were the original and allowing access.

- **Gain access through a backdoor** – Manufacturers often build in test facilities or have other software backdoors that an examiner can exploit to obtain information. For example, a few software tools are able to acquire the memory of certain phones directly through a diagnostic/debugging protocol that bypasses the authentication mechanism. Scanning the memory contents can reveal authentication information such as passwords or phone locks.

  The bootloaders on some mobile phones and PDA devices also support functions that, among other things, allow the devices' memory to be read. For instance, the iPAQ 3900 and other models in that product series support the parrot bootloader, an unadvertised utility so named because of the bird that appears on the display [Log01]. When triggered by a specific combination key chord and provided appropriate commands via the serial port, the bootloader returns the contents of memory or copies it to a memory card. Similarly, the penguin bootloader for Linux handheld devices can be used to copy memory to a memory card.

- **Exploit known system vulnerabilities** – Mobile systems may possess system vulnerabilities within a standard interface protocol that an examiner can exploit to bypass authentication and gain access to information. For example, access to the device may be possible via a misconfigured network service [Cha02], a flaw in a standard networking protocol supported by the device, or an error in the protocol's implementation that makes it susceptible to an attack method such as a buffer overflow. Possible communications interfaces for exploitation include the serial, USB, IrDA, Bluetooth, WiFi, and GSM/GPRS facilities.

Substitute (U)SIMs: Occasionally, a (U)SIM may not be recovered with a phone, or may be intentionally damaged and unusable with the phone, but needed for the acquisition of the phone with a forensic tool. One of the most common mistakes a forensic specialist can make is to insert another available (U)SIM into the phone to acquire the data with a forensic tool. Certain data stored in the memory of the phone, such as call logs (missed, incoming and outgoing calls) and SMS messages, is linked to the last (U)SIM used. Inserting a different (U)SIM causes that data to be erased from the phone's memory. Some phones may also start copying SIM data to the phone memory when another (U)SIM is inserted.

[27] For more information, see http://www.fonefunshop.co.uk/Unlocking/nokiasecuritycode.htm.

A better approach is to create a substitute (U)SIM to use with the phone that mimics key characteristics of the original (U)SIM, tricking the phone to accept it as the original. Several tools that can be used to create a substitute (U)SIMs are the Forensic SIM Toolkit, GSM .XRY SIM ID Cloner, SIMgen, and the TULP 2G SIMIC protocol plug-in.

Substitute (U)SIMs, sometimes referred to as access cards, can be useful in a number of situations:

- As already mentioned, if the (U)SIM for a phone is missing or damaged and needed for acquisition with a forensic tool, a substitute (U)SIM allows phone data to be recovered.

- If the (U)SIM for a phone is present, but requires a PUK code, a substitute (U)SIM allows acquisition to proceed immediately without having to contact the service provider for the PUK.

- If radio isolation is needed to prohibit communications to acquire evidence from a phone, avoiding incoming calls or messages from altering or modifying evidence, a substitute (U)SIM can be used in lieu of a Faraday room or enclosure.

- If the forensic tool used to examine a handset accesses the resident (U)SIM indirectly, using a substitute (U)SIM in the handset eliminates the possibility of the original being altered during examination.

The values by which the phone remembers the previously inserted (U)SIMs are the ICCID and the IMSI. Often only one of these values is used. Both identifiers are unique and used to authenticate the user to the network. If these values are known for a specific phone (e.g., either indirectly through the service provider records or directly by reading memory from the phone), it may be possible to prepare a substitute (U)SIM with the correct values needed to trick the phone to accepting it. While the minimum data needed to create a (U)SIM may be simply one of these two values, some phones may require additional data to be populated on the (U)SIM to be correctly recognized. The possibility exists that data, other than user data, may change on the handset as the result of inserting a substitute (U)SIM [INT06].

6.5.3 Hardware-based Methods

Hardware-based methods involve a combination of software and hardware to break or bypass authentication mechanisms and gain access to the device. For example, the value of a phone lock can be readily recovered from a memory dump of certain phones, allowing for a follow-on logical acquisition. Few general-purpose hardware-based methods apply to a general class of mobile phone. Most of the techniques are specialized for a specific model within a class. As with software-based methods, when a specialized technique is developed, a test device identical to the one under examination should be used. The device manufacturer may also provide useful information and tools for extracting data. Hardware-based methods include the following:

- **Gain access through a hardware backdoor** – Hardware backdoors, such as interfaces for debugging, production testing, or maintenance, may be used to gain access to memory. For example, some mobile phones have active hardware test points on the circuit board that can be used to probe the device. Many manufacturers now support the JTAG standard, which defines a common test interface for processor, memory, and other semiconductor chips, on their devices [Int96]. Forensic examiners can communicate with a JTAG-compliant component by utilizing software and an add-in hardware controller in a personal computer card slot or a special purpose

standalone programmer device to probe defined test points [Will05]. The JTAG testing unit can send commands and data to the JTAG-compliant component and return the results to the unit for storage and rendition [Bre06, Xjt03]. JTAG gives specialists another avenue for imaging devices that are locked or devices that may have minor damage and cannot be properly interfaced otherwise.

- **Examine memory independently of the device** – An experienced examiner may be able to examine memory chips directly on the device and extract information from them. For example, the Netherlands Forensic Institute has developed a general-purpose tool for examining a wide range of memory chips. Once physically connected via a memory clip, the tool is able not only to read and store memory contents, but also to overwrite them [Kni02]. Memory may also be acquired by dismantling the phone, heating the circuit board sufficiently to desolder the memory chips, and using a memory chip reader to access their contents [Will05].

- **Find and exploit vulnerabilities** – Mobile phone vulnerabilities discovered through close study and experimentation are sometimes posted on the Web.[28] They can also be discovered through reverse engineering. Reverse engineering involves retrieving the operating system code from the ROM of a mobile phone identical to the one under examination and analyzing the code to understand its structure and use of the device hardware [Haa04]. With the understanding gained, any plausible vulnerabilities noted can be systematically tested to determine a useful exploit technique. For example, for a password authentication mechanism, it may be possible using memory injection to overwrite the password with a known value or replace the authentication program with a version that always authenticates successfully [Kni02]. Similarly, flipping two bits in a data structure, which determine whether the start-up password is active and configured, may turn off the mechanism completely, as reported for the XDA PDA/phone hybrid device [Its].

- **Infer information by monitoring physical device characteristics** – Techniques that monitor power consumption or other device characteristics have been effective in systematically determining the password or PIN. For example, forensic specialists report that the passwords of some electronic organizers have been uncovered by determining the address area of the password and, as characters are entered, systematically monitoring the data and address bus of those memory locations to reveal the value one character at a time [Kni02]. Differential power analysis, which has been shown to be effective in gaining information from smart cards, is another technique that could be applied [Aig]. Simply observing data on an interface can also reveal information. For example, the dialog between the phone and a password-protected memory card can be monitored to reveal the password supplied by the phone to unlock the card, which can then be used in an external examination to access the memory card contents.

- **Use automated brute force** – If a password mechanism has no restrictions on the number of manual attempts made and the examiner had time to spare, a brute force dictionary attack could be attempted. Normally, this approach would be out of the

[28] For example, a security hole discovered in the Motorola MPx200 is discussed at http://msmobiles.com/news.php/1640.html.

question. However, with automated keystroke entry, it is plausible. For example, the Netherlands Forensic Institute developed an automated password entry system for devices with a keyboard and screen. Equipped with a robot arm and video camera, the unit can systematically enter passwords until the correct entry is detected or, in the worst case, the keys become damaged [Kni02].

6.6 Tangential Equipment

Tangential equipment includes devices that contain memory and are associated with a mobile phone. The two main categories are memory cards and host computers to which a mobile phone has synchronized its contents. Surprisingly, USB memory drives, which are a common peripheral for host computers, are generally not a factor for mobile phones because of interface issues.

Mobile phones, especially higher smart phones, typically support Secure Digital (SD), MultiMedia Cards (MMC), and other types of removable media designed specifically for handheld devices, which can contain significant amounts of data. Memory cards are typically semiconductor memory, used as auxiliary user file storage, for backup of important content, or as a means to convey files to and from the device. The physical sizes of memory cards supported by handheld devices are noteworthy insofar as they are quite small, about the size of a coin, and easy to overlook. Therefore, investigators should take their time and thoroughly search the premises when seizing material. Data can be acquired from removable media with the use of a media reader and a forensic application used to image hard drives.

The data contained on a mobile phone is often present on a personal computer, due to the capability of mobile phones to synchronize or otherwise share information among one or more host computers. Such personal computers or workstations are referred to as synched devices. Because of synchronization, a significant amount of evidence on a mobile phone may also be present on the suspect's laptop or personal computer, and recovered using a conventional computer forensic tool for hard drive acquisition and examination.

6.6.1 Synched Devices

Synchronization refers to the process of resolving differences in certain classes of data, such as e-mail residing on two devices (i.e., a mobile phone and a computer), to obtain a version that reflects any actions taken by the user (e.g., deletions or additions) on one device or the other. Synchronization of information may occur at either the record level or the file level. When done at the file level, any discrepancies from the last synchronization date and time result in the latest version automatically replacing the older version. Occasionally manual intervention may be needed if both versions were modified independently since the last synchronization occurred. Record level synchronization is done similarly, but with more granularity, whereby only out-of-date parts of a file are resolved and replaced.

Phones are typically populated with data from the personal computer during the synchronization process. A significant amount of informative data, therefore, may reside locally on a personal computer. Data from the phone can also be synchronized to the computer, through user-defined preferences in the synchronization software. Because the synchronized contents of a phone and personal computer tend to diverge quickly over time, additional information may be found in one device or the other.

The synchronization software and the device type determine where the phone's files are stored on the PC. Each synchronization protocol has a default installation directory, but the locale can be user specified.

6.6.2 Memory Cards

Mobile phones use a wide array of memory cards, ranging from the size of a contact lens to that of a matchbook. Unlike RAM within a device, such removable media is non-volatile storage and requires no battery to retain data. Memory card storage capacity ranges from 8MB to 2GB and beyond. As technological advances are made, such media becomes smaller and offers larger storage densities. Removable media extends the storage capacity of mobile phones, allowing individuals to store additional files beyond the device's built-in capacity and to share data between compatible devices.

Some forensics tools are able to acquire the contents of memory cards; many are not. If the acquisition is logical, deleted data present on the card is not recovered. Fortunately, such media can be treated similarly to a removable disk drive, and imaged and analyzed using conventional forensic tools with the use of an external media reader. Memory card adapters exist that support an Integrated Drive Electronics (IDE) interface. Such adapters allow removable media to be treated as a hard disk and used with a write blocker, which ensures that the removable media remains unaltered. A Universal Serial Bus (USB) memory card reader used with write blocker hardware is also an available alternative.

Data contained on the media can be imaged and searched, and deleted files can be recovered, providing possibilities of uncovering evidence. One drawback is that phone data, such as SMS text messages, stored on the media may require manual decoding or a separate decoding tool to interpret. A more serious issue is that content protection features incorporated into the card may block the recovery of data. The most notable example is MMC cards that conform to version 4.1 of the standard, which provides for password protection and is supported increasingly on newer models of phones. Table 5 gives a brief overview of various storage media in use today.

Table 5: Memory Cards

Name	Characteristics
Compact Flash Card (CF)	Matchbook size (length-36.4 mm, width-42.8 mm, thickness-3.3 mm for Type I cards and 5mm for Type II cards) 50-pin connector, 16-bit data bus
MMCplus (compatible with original MultiMedia Card or MMC)	Postage stamp size (length-32 mm, width-24 mm, and thickness-1.4 mm) 13-pin connector, 1, 4, or 8 bit data bus (7-pin connector, 1-bit data bus, MCC compatibility)
MMCmobile (compatible with original Reduced Size MMC or RS-MMC)	Thumbnail size (length-18 mm, width-24 mm, and thickness-1.4 mm) 13-pin connector, 1, 4, or 8 bit data bus (7-pin connector, 1-bit data bus, RS-MMC compatibility) Requires a mechanical adapter to be used in a full size MMCplus slot
MMCmicro	Contact lens size (length-14 mm, width-12 mm, and thickness-1.1 mm) 10-pin connector and a 1 or 4-bit data bus Requires a mechanical adapter to be used in a full size MMCplus slot
Secure Digital (SD) Card	Postage stamp size (length-32 mm, width-24 mm, and thickness-2.1mm) 9-pin connector, 1 or 4-bit data bus Features a mechanical erasure-prevention switch

Name	Characteristics
MiniSD Card	Thumbnail size (length-21.5 mm, width-20 mm, and thickness-1.4 mm) 9-pin connector, 1 or 4-bit data bus Requires a mechanical adapter to be used in a full size SD slot
MicroSD (formerly Transflash)	Contact lens size (length-15 mm, width-11 mm, and thickness-1 mm) 6-pin connector, 1 or 4-bit data bus Requires a mechanical adapter to be used in a full size SD slot
Memory Stick	Chewing gum stick size (length-50 mm, width-21.45 mm, thickness-2.8 mm) 10-pin connector, 1-bit data bus Features a mechanical erasure-prevention switch
Memory Stick Duo	Partial chewing gum stick size (length-31mm, width-20 mm, thickness-1.6 mm) 10-pin connector, 4-bit data bus Features a mechanical erasure-prevention switch Requires a mechanical adapter to be used in a full size Memory Stick slot
Memory Stick Micro	Contact lens size (length-12.5 mm, width-15 mm, and thickness-1.2 mm) 11-pin connector, 4-bit data bus Requires a mechanical adapter to be used in a full size Memory Stick slot

Memory cards may support extensions for added functionality. For example, the X-Mobile Card from Renesas is a MultiMedia card that contains both a smart card and a memory chip. Through the use of a built-in controller, the card is able to function in either mode. Another example is SD cards that have WiFi or other wireless capability.

6.6.3 USB Memory Drives

USB drives, sometimes referred to as thumb drives, are chewing-gum-pack size hardware components with a USB connector at one end, and built as a printed circuit board within a plastic housing that encases a processor and memory. USB memory drives can be treated similarly to a removable disk drive, and imaged and analyzed using conventional forensic tools.

Many manufacturers produce USB memory drives of various capacities. Currently, however, very few mobile phones support host USB ports, which are needed to interface with these peripherals. Moreover, few if any USB drive manufacturers provide the necessary drivers for mobile phone operating systems. This situation is understandable, given that host USB specifications intend for an interface to be capable of supporting multiple devices sharing the port, which if permitted would place a significant power drain on the battery of the device. Other factors include the restrictions in mobility imposed by a USB drive sticking out of the side of a mobile phone compared to the benefits of providing one or more memory card slots that completely contain a card when inserted.

As with memory card extensions, USB drives may offer additional capabilities such as a wireless interface. Access to memory contents may also be protected through a built-in fingerprint reader or some other mechanism such as a smart card, which complicates the acquisition process. However, for the reasons mentioned above these peripherals are not normally associated with mobile phones.

7. Examination and Analysis

The examination process uncovers digital evidence, including that which may be hidden or obscured. The results are gained through applying established scientifically based methods, and should describe the content and state of the data fully, including the source and the potential significance. Data reduction, separating relevant from irrelevant information, occurs once the data is exposed. The analysis process differs from examination in that it looks at the results of the examination for its direct significance and probative value to the case [ACPO]. Examination is a technical process that is the province of a forensic specialist. However, analysis may be done by roles other than the forensic analyst, such as the investigator or the forensic examiner.

The examination process begins with a copy of the evidence acquired from the device. Fortunately, compared with classical examination of individual workstations or network servers, the amount of acquired data to examine is much smaller with mobile phones. Because of the prevalence of proprietary case file formats, the forensic toolkit used for acquisition will typically be the one used for examination and analysis. Interoperability among the acquisition and examination facilities of different tools is also unlikely for this reason, with the exception of certain Palm OS devices and perhaps other devices with a PDA lineage.

The examiner should have studied the case, if possible, and become familiar with the parameters of the wrongdoing, the parties involved, and potential evidence that might be found. Conducting the examination in a partnership with the forensic analyst or the investigator guiding the case construction is advisable for the examiner. The investigator or analyst provides insight into the types of things sought, while the forensic examiner provides the means to find relevant information that might be on the system [Wol03].

If the forensic examiner performs the analysis independently, without conferring directly with the forensic analyst or investigator, the understanding gained by studying the case should provide ideas about the type of data to target and specific keywords or phrases to use when searching the acquired data. Depending on the type of case, the strategy varies. For example, a case about child pornography may begin with browsing all of the graphic images on the system, while a case about an Internet-related offense might begin with browsing the Internet history files [Wol03].

Examination often reveals not only potentially incriminating data but also useful information such as passwords, network logon names, and Internet activity. Certain data can also provide linkage to other potential sources of evidence maintained elsewhere, particularly by network service providers. In addition to evidence directly related to an incident, information can be uncovered about the lifestyle of suspects, their associates, and the types of activities in which they are involved.

7.1 Potential Evidence

Mobile phone manufacturers typically offer a similar set of information handling features and capabilities, including Personal Information Management (PIM) applications, messaging and e-mail, and Web browsing. The set of features and capabilities can vary, of course, with the era in which the phone was manufactured, the version of firmware running, modifications

made for a particular service provider, and any modifications or applications installed by the user. The potential evidence on these devices includes the following items:

- Subscriber and equipment identifiers
- Date/time, language, and other settings
- Phonebook information
- Appointment calendar information
- Text messages
- Dialed, incoming, and missed call logs
- Electronic mail
- Photos
- Audio and video recordings
- Multi-media messages
- Instant messaging and Web browsing activities
- Electronic documents
- Location information

Other data found on a mobile phone may also prove useful in an investigation. For example, something seemingly immaterial such as ring tones can have relevance, given that mobile phone users often load distinctive ring tones onto a phone to distinguish theirs from others'. A witness to an incident may recall having heard a particular tune on a suspect's phone, which may contribute to the identification of an individual. Even esoteric network information found on a (U)SIM may prove useful in an investigation. For example, if a network rejects a location update from a phone attempting to register itself, the list of forbidden network entries in the Forbidden PLMNs elementary file is updated with the code of the country and network involved [3GP05a]. The phone of an individual suspected of traveling to a neighboring country might be checked for this information.

The items present on a device are dependent not only on the features and capabilities of the phone, but also on the voice and data services subscribed to by the user. For example, prepaid phone service typically does not include data services and rules out the possibility for multi-media messaging, electronic mail, and Web browsing. Similarly, a contract subscription may selectively exclude certain types of service, though the phone itself could support them.

Reported Examples: News articles sometimes describe the types of digital evidence found on a mobile phone that was used successfully in an investigation. Some illustrative examples are given below.

- *Text Message and Call Data* – "A pastor of the Pentecostal congregation in the small community of Knutby was sentenced to life in prison for persuading one of his lovers (the au pair) to shoot and kill his wife and trying to kill the husband of another mistress. Two days after the murder, the pastor's au pair Sarah S. claimed that she did it. Despite her claims … the police believed she had an accomplice."

  "The strongest evidence against the pastor was the extensive communication through text messages and voice calls between him and the au pair on the day of the murder and just before that. What they did not know was that their (anonymously sent and) carefully deleted text messages were possible to recover." [Bur05]

- *Email Data* – "The case against Dan Kincaid was strong. A homeowner in northern Boise, Idaho, had identified Mr. Kincaid, 44, as the person who had broken into his suburban house. But eyewitness testimony isn't always rock solid, and Mr. Kincaid was refusing to talk. The police wanted more. So they searched Mr. Kincaid's BlackBerry e-mail-capable phone electronically, and found all the evidence they needed."

  "'Just trying to find a way out of this neighborhood without getting caught,' Mr. Kincaid wrote to his girlfriend on Aug. 1, 2005, shortly after he had been spotted. 'Dogs bark if I'm between or behind houses. ... ' 'Cops know I have a blue shirt on,' he continued. 'I need to get out of here before they find me.' Faced with his e-mailed admission, Mr. Kincaid agreed to a deal with prosecutors over that crime and a string of others." [Sha06]

- *Image and Multi-media Message Data* – "It was alleged that a young boy had conducted a serious assault on another child whilst his friend took pictures on his mobile phone. The young boy was initially denying all knowledge of the incident, until the Police were informed that there was evidence on the mobile phone." "… analysts recovered the pictures in question in a forensically sound manner following ACPO guidelines. They also recovered a deleted multimedia text message sent to another child with one of the pictures attached to it."[29]

- *Location Data* – "Mr Bristowe told BBC News Online: 'It was mobile phone evidence which made the police look more closely at Huntley. He had been Mr. Useful, helping them to search the college grounds, but when they checked Jessica's phone and discovered when and where it had been switched off alarm bells began to ring… (Jessica's phone) disengaged itself from the network, in effect it says goodbye' at 1846 BST on the Sunday when the girls disappeared. Jessica's phone contacted the Burwell mast when it was turned off."

  "'The police provided us with a map of the route they thought the girls would have taken, and the only place on that route where the phone could have logged on to Burwell (and disengaged itself) was inside or just outside Huntley's house.' It is believed to be that crumb of crucial evidence which forced Huntley to change his story earlier this year and suddenly admit the girls died in his bathroom." [Sum03]

Two types of computer forensic investigations generally take place. The first type is where an incident has occurred, but the identity of the offender is unknown (e.g., a hacking incident). The second is where the offender and the incident are both known (e.g., a child-porn investigation). Prepared with the background of the incident, the forensic examiner and analyst can proceed toward accomplishing the following objectives:

- Gather information about the individual(s) involved {who}.
- Determine the exact nature of the events that occurred {what}.
- Construct a timeline of events {when}.
- Uncover information that explains the motivation for the offense {why}.

[29] For more information, see "Mobile Phone Analysis – video retrieval" Case Study at http://www.ccl-forensics.com/Case_Studies-27.html?linkto=38.

- Discover what tools or exploits were used {how}.

Table 6 below provides a cross reference of generic evidence sources commonly found on mobile phones and their likely contribution toward satisfying the above objectives. In many instances, the data is peripheral to an investigation, useful in substantiating or refuting the claims of an individual about some incident. On occasion, direct knowledge, motivation, and intention may be established. Most of the evidence sources are from PIM data, call data, messaging, and Internet related information. Other support applications that run on the device potentially provide other evidence sources. User files placed on the device for rendition, viewing, or editing are also another important evidence source. Besides graphic files, other relevant file content includes audio and video recordings, spreadsheets, presentation slides, and other similar electronic documents. Installed executable programs may also have relevance in certain situations. Perhaps the most important data recovered is that which links to information held by the service provider. Service providers maintain databases for billing or debiting accounts based on call logs, which can be queried using the subscriber or equipment identifiers. Similarly, undelivered SMS text messages, multi-media, or voice messages may also be recoverable.

Table 6: Cross Reference of Sources and Objectives

	Who	What	Where	When	Why	How
Subscriber/Device Identifiers	X					
Call Logs	X			X		
Phonebook	X					
Calendar	X	X	X	X	X	X
Messages	X	X	X	X	X	X
Location			X	X		
Web URLs/Content	X	X	X	X	X	X
Images/Video	X	X	X	X		X
Other File Content	X	X	X	X	X	X

7.2 Applying Tools

Once a copy of the acquisition results is available, the next steps involve searching the data, identifying evidence, creating bookmarks, and developing the contents of a final report. Knowledge and experience with the tools used for examination is extremely valuable, since proficient use of the available features and capabilities of a forensic tool can greatly speed the examination process.

Forensic tools are a crucial component, as they translate data from a raw encoded form to a format and structure that is understandable by the examiner, enabling identification and recovery of evidence. A variety of different and sometimes unusual encodings are used with

cell phone data and found in the memory of handsets and (U)SIMS, such as text encoded in the packed 7-bit GSM alphabet, which would be onerous, errorful, and time consuming to decode manually.

It is important to note that forensic tools have the possibility to contain some degree of error in their operation. For example, the implementation of the tool may have a programming error; the specification of a file structure used by the tool to translate bits into data comprehensible by the examiner may be inaccurate or out of date; or the file structure generated by another program as input may be incorrect, causing the tool to function improperly [Car02]. Experiments conducted with mobile phone forensic tools indicate a prevalence of such errors [Aye05, Jan06, Aye07]. Therefore, having a high degree of trust and understanding of the tool's ability to perform its function properly is essential.

A knowledgeable suspect may tamper with device information, such as purposefully misnaming a file extension to foil the workings of a tool, altering the date/time of the phone to falsify timestamps associated with logged activities, creating false transactions in the memory of the phone or (U)SIM, or applying a wiping tool to remove or eliminate data from memory. Seasoned experience with a tool provides an understanding of its limitations, allowing an examiner to compensate for them and avoid error to achieve the best possible results.

To uncover evidence, specialists should gain a background of the suspect and offense and determine a set of terms for the examination. Search expressions can be developed in a systematic fashion, such as using contact names that may be relevant. By proceeding systematically, the specialist creates a profile for potential leads that may unveil valuable findings. Forensic Examination of Digital Evidence – A Guide for Law Enforcement, produced by the U.S. Department of Justice [DOJ04], offers the following suggestions for the analysis of extracted data:

- **Ownership and possession** – Identify the individuals who created, modified, or accessed a file, and the ownership and possession of questioned data by placing the subject with the device at a particular time and date, locating files of interest in non-default locations, recovering passwords that indicate possession or ownership, and identifying contents of files that are specific to a user.

- **Application and file analysis** – Identify information relevant to the investigation by examining file content, correlating files to installed applications, identifying relationships between files (e.g., e-mail files to e-mail attachments), determining the significance of unknown file types, examining system configuration settings, and examining file metadata (e.g., documents containing authorship identification).

- **Timeframe analysis** – Determine when events occurred on the system to associate usage with an individual by reviewing any logs present and the date/time stamps in the file system, such as the last modified time. Besides call logs, the date/time and content of messages and e-mail can prove useful. Such data can also be corroborated with billing and subscriber records kept by the service provider [Hos98].

- **Data hiding analysis** – Detect and recover hidden data that may indicate knowledge, ownership, or intent by correlating file headers to file extensions to show intentional obfuscation; gaining access to password-protected, encrypted, and compressed files;

gaining access to steganographic information detected in images; and gaining access to reserved areas of data storage outside the normal file system.

The capabilities of the tool and the richness of its features, versus the operating system and type of device under examination, determines what information can be recovered, identified, and reported, and the amount of effort needed. The search engine plays a significant role in the discovery of information used for the creation of bookmarks and final reporting. For example, some tools used to search for textual evidence identify and categorize files based on file extension, where others use a file signature database. The latter feature is preferable since it eliminates the possibility of missing data because of an inconsistent file name extension (e.g., eliminating a text file whose extension was changed to that of a graphics or image file). Similarly, the ability for the tool to find and gather images automatically into a common graphics library for examination is extremely useful.

Searching data for positive results on incriminating evidence takes patience and can be time consuming. Some tools have a simple search engine that matches an input text string exactly, allowing only for elementary searches to be performed. Other tools incorporate more intelligent and feature rich search engines, allowing for generalized regular expression patterns (grep) type searches, including wildcard matches; filtering of files by extension, directory, etc.; and batch scripts that search for specific types of content (i.e., e-mail addresses, URLs). The greater the tool's capabilities, the more the forensic examiner benefits from experience with and knowledge of the tool.

7.3 Call and Subscriber Records

Records maintained by the service provider capture information needed to accurately bill a subscriber or, in the case of a prepaid service plan, debit the balance. The records collected are referred to as call detail records, which are generated by the switch handling an originating call or SMS message from a mobile phone. For some service providers, the records may also include fixed line, international gateway, and voice over IP transaction information. While the content and format of these records can differ widely from one service provider to another, the fundamental data needed to identify the subscriber/device initiating the call, the initial cell servicing the call, the number dialed, and the duration of the call is captured. Detailed information such as the identifier of the cell (i.e., the BTS) and the sector involved are often included. Appendix D gives an example of the data elements of a call detail record, specified in the GSM standards. As one can see, considerable discretion about what is implemented is left open to the service providers and network operators.

The retention period for maintaining call detail and other types of records varies among service providers [GSM05]. However, the period is generally limited, requiring immediate action to avoid data loss. One should act quickly to have the cellular carrier preserve any data that can be used to identify communications that have occurred and are linked to the parties of interest, stressing non-disclosure of that action to the account subscriber [Ala03, Ala04]. The data available may include subscriber records, the content of email servers (i.e., undelivered email), email server logs, RADIUS or other IP address authentication logs, the content of SMS and MMS message servers, and the content of voicemail servers. Note that certain types of undelivered content, such as voicemail, may be considered in transit from a legal standpoint in some jurisdictions, and obtaining or listening to them without the proper authority may be treated as an illegal interception of communications [Ala03]. While the USA PATRIOT Act

eliminated this issue at the federal level, state statutes may be intentionally more restrictive or not yet be realigned completely with the federal statute.[30]

Call detail records can be obtained from U.S. service providers through their law enforcement point of contact, with the appropriate legal documents. Procedures may vary among states in the U.S., and new laws regarding proper seizure are continually legislated. Procedures also vary for getting records from service providers and network operators located in other countries. Close and continuing consultation with legal counsel is advised. Various on-line law enforcement forums can also be helpful in identifying points of contact and sharing tips on procedures for accurately obtaining the required data.[31]

Besides call detail records, subscriber records maintained by a service provider can provide data useful in an investigation. For example, for GSM systems, the database usually contains the following information about each customer [Wil03]:

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

Other useful information, including phone numbers (i.e., work or home), contact information (e.g., email address), and credit card numbers used, may also be retained in subscriber records. Pay-as-you-go prepaid phones purchased anonymously over the counter may also have useful information maintained with their accounts, which was supplied by the subscribers, such as the credit card numbers used for purchases of additional time or an email address registered online for receipt of notifications. Gaining access to the call records of prepaid phones should not be ruled out.

Call detail records and other records maintained by the service provider can be requested using subscriber or equipment identifier information seized or acquired from a phone or (U)SIM. Subscriber information often used for this purpose includes the IMSI from the (U)SIM and the cell phone number. Equipment identifiers used are the ESN or IMEI of the phone and the

---

[30] For example, see the California wiretap clarification bill at http://info.sen.ca.gov/pub/bill/asm/ab_1301-1350/ab_1305_cfa_20050603_115538_sen_comm.html.

[31] For example, see the PhoneForensics Yahoo Group at http://groups.yahoo.com/group/phoneforensics/ or the High Tech Crime Consortium mail list at https://htcc.secport.com/mailman/listinfo/htcc.

serial number (i.e., ICCID) of the (U)SIM. The search criteria used could be, for example, all calls received by a certain phone number (e.g., that of a victim) or all calls handled by a base station responsible for a particular cell (i.e., to determine who was in a certain area at a certain time) [Wil05]. The analysis of the initial set of records obtained usually leads to additional requests for related records of other subscribers and equipment, based on the data uncovered. For example, frequent calls to a victim's mobile phone from one or more other phones before a homicide would logically lead to interest in obtaining the records of the caller(s).

Call detail records can be analyzed for a variety of purposes. For example, a service provider may use them to understand the calling patterns of their subscribers and the performance of the network [Aja06, Hin96]. Call detail records can also be used with cell site tower information obtained from the service provider to translate cell identifiers into geographical locations for the cells involved and identify the general locale from which calls were placed. While plotting call record locations and information onto a map can sometimes be useful, it does not necessarily provide a complete and accurate picture. Cell towers can service phones at distances of up to 35 kilometers (approximately 21 miles) and may service several distinct sectors. Radio frequency coverage maps maintained by the service provider can be obtained to create a more exact portrayal of the data for the sectors involved. The results of the data analysis can be used to corroborate or refute statements made by individuals regarding their whereabouts at a given time. A change of cell identifier between the beginning and the end of a call, over a series of calls, may also indicate a general direction of travel or pattern of behavior.

Cell boundaries are somewhat fuzzy. Various factors, such as terrain, seasonal changes, antenna performance, and call loading, affect the coverage area of cells and the plausible locale to associate with a call record. Detailed field tests and measurements may be required to ensure accuracy the analysis. Such surveys are regularly performed by network operators to verify and improve network performance [Ko96]. Tools also exist to aid law enforcement in performing cell site analysis and mapping activities independently.[32] In some situations, however, such as densely populated urban locations involving microcells or picocells with a limited coverage area, location determination may be relatively straightforward by the very nature of the network [Gar01].

Identifying the geographical coverage of specific cells can provide valuable information when combined with call detail records, geographically establishing plausible locations with some degree of certainty for the times involved. Professional criminals are aware of these capabilities and may attempt to turn them to their advantage by having someone use their phone to establish a false alibi. Attempts at evasion may also occur. A common ploy used is to purchase, use, and quickly dispose of pay-as-you-go prepaid phones to minimize exposure or use stolen phones. To obfuscate usage and complicate analysis of records, a variety of different (U)SIMs may be swapped among different GSM/UMTS handsets.

Careful analysis of the call records in conjunction with other forms of available evidence overcomes most of these kinds of attempts at evasion. For example, call detail records of pay-as-you-go prepaid phones are maintained by and available from network providers, the same as for contract subscriptions. By analyzing the patterns and content of communications and

[32] For example, see the Cell View information at http://www.icardforensics.com/documents/CellSiteMonitor.pdf or the CSurv information at http://www.teeltech.com/tt/TeelTechCsurv.pdf.pdf.

mapping the evidence to known associates of a suspect, ownership of such phones is possible to establish. Other traditional forms of forensic evidence may also be used to establish ownership.

8. Reporting

Reporting is the process of preparing a detailed summary of all the steps taken and conclusions reached in the investigation of a case. Reporting depends on maintaining a careful record of all actions and observations, describing the results of tests and examinations, and explaining the inferences drawn from the evidence. A good report relies on solid documentation, notes, photographs, and tool-generated content.

Reporting occurs once the data has been thoroughly searched and relevant items bookmarked. Many forensic tools come with a built-in reporting facility that usually follows predefined templates and may allow customization of the report structure. Permitted customizations include allowing for organization logos and report headers and selection of styles and structure to provide a more professional look tailored to the organization's needs. Reports generated by a forensic tool typically include items from the case file, such as the specialist's name, a case number, a date and title, the categories of evidence, and the relevant evidence found. Report generation typically either outputs all of the data obtained or allows examiners to select relevant data (i.e., bookmarked items) for the final report. Including only relevant findings in the report minimizes its size and lessens confusion for the reader.

The software-generated contents are only one part of the overall report. The final report contains the software-generated contents along with data accumulated throughout the investigation that summarizes the actions taken, the analysis done, and the relevance of the evidence uncovered. Ideally, the supporting documentation is in electronic form and able to be incorporated directly into the report.

Reporting facilities vary significantly across mobile device acquisition applications. Report generation typically can render a complete report in one of several common formats (e.g., .txt, .rtf, .csv, .doc, .html) or at least provide a means to export out individual data items to compose a report manually. A few tools include no means of report generation or data export and instead require examiners to capture individual screenshots of the tool interface for later assembly into a report format. Regardless of how reports are generated, checking that the finalized report is consistent with the data presented in the user interface representation is vital to identify and eliminate any possible inconsistencies that may appear [Aye05, Jan06, Aye07].

The ability to modify a pre-existing report and incorporate data (e.g., images, video stills) captured by alternative means is advantageous. Auxiliary acquisition techniques are sometime required to recover specific data types, as mentioned earlier. For example, video recording a manual examination documents the recovery of evidence that the automated forensic tool did not acquire. Video editing software allows still images to be captured for inclusion into the report. Snapshots could also be taken of the manual exam using a digital camera, though the process is less efficient and does not document the entire process, nor allows the entire procedure to be viewed if questions arise.

The type of data determines whether it is presentable in a hard-copy format. Today, many popular cellular devices are capable of capturing video and audio. Such evidentiary data (e.g., audio, video) cannot be presented in a printed format and instead should be included with the finalized report on removable media (e.g., CD-ROM, DVD-ROM, or thumb drive) along with the appropriate application for proper display.

Reports of forensic examination results should include all the information necessary to identify the case and its source, outline the test results and findings, and bear the signature of the individual responsible for its contents. In general, the report may include the following information [DOJ04]:

- Identity of the reporting agency
- Case identifier or submission number
- Case investigator
- Identity of the submitter
- Date of receipt
- Date of report
- Descriptive list of items submitted for examination, including serial number, make, and model
- Identity and signature of the examiner
- The equipment and set up used in the examination
- Brief description of steps taken during examination, such as string searches, graphics image searches, and recovering erased files.
- Supporting materials such as printouts of particular items of evidence, digital copies of evidence, and chain of custody documentation
- Details of findings:
  - Specific files related to the request
  - Other files, including deleted files, that support the findings
  - String searches, keyword searches, and text string searches
  - Internet-related evidence, such as Web site traffic analysis, chat logs, cache files, e-mail, and news group activity
  - Graphic image analysis
  - Indicators of ownership, which could include program registration data
  - Data analysis
  - Description of relevant programs on the examined items

  - Techniques used to hide or mask data, such as encryption, steganography, hidden attributes, hidden partitions, and file name anomalies

- Report conclusions

Digital evidence, as well as the tools, techniques and methodologies used in an examination, is subject to being challenged in a court of law or other formal proceedings. Proper documentation is essential in providing individuals the ability to re-create the process from beginning to end. As part of the reporting process, making a copy of the software used and including it with the output produced is advisable. This is especially pertinent for custom tools, since confusion about the version of the software used to create the output is eliminated, should it become necessary to reproduce forensic processing results at a later time. The same practice applies to commercial software tools, which could be upgraded after an examination is completed [NTI].

9. References

[3GP02] 3GPP2 (2002), Removable User Identity Module for Spread Spectrum Systems, 3rd Generation Partnership Program 2, 3GPP2 C.S0023-A, Version 1.0, September 13, 2002, <URL: http://www.3gpp2.org/public_html/specs/C.50023-A_v1.0.pdf>.

[3GP05a] 3GPP (2005a), Specification of the Subscriber Identity Module - Mobile Equipment (SIM - ME) interface, 3rd Generation Partnership Project, TS 11.11 V8.13.0 (Release 1999), Technical Specification, (2005-06).

[3GP05b] 3GPP (2005b), Technical Realization of the Short Message Service (SMS), 3rd Generation Partnership Project, TS 23.040 V6.6.0 (Release 6), Technical Specification (2005-12).

[3GP98] 3GPP (1999), Alphabets and Language-specific Information, 3rd Generation Partnership Project, TS 03.38, version 7.2.0 (Release 1998), Technical Specification (1999-07).

[ACPO] Good Practice Guide for Computer-based Electronic Evidence, Association of Chief Police Officers, Version 3, <URL: http://www.acpo.police.uk/asp/policies/Data/gpg_computer_based_evidence_v3.pdf >.

[Aig] Manfred Aigner, Elisabeth Oswald, Power Analysis Tutorial, Seminar Paper, Institute for Applied Information Processing and Communication, <URL: http://www.iaik.tu-graz.ac.at/aboutus/people/oswald/papers/dpa_tutorial.pdf>.

[Aja06] Ireti Ajala, Spatial Analysis of GSM Subscriber Call Data Records, Directions Magazine, Mar 07, 2006, <URL: http://www.directionsmag.com/article.php?article_id=2112&trv=1>.

[Ala03] Searching Voicemail and E-mail, Point of View, Alameda County District Attorney's Office, Winter 2003, <URL: http://www.acgov.org/da/pov/documents/voicemail.pdf>.

[Ala04] Phone, E-mail, and Internet Records, Point of View, Alameda County District Attorney's Office, Fall 2004, <URL: http://www.acgov.org/da/pov/documents/phone.pdf>.

[Aye05] Rick Ayers, Wayne Jansen, Nicolas Cilleros, Ronan Daniellou, Cell Phone Forensics Tools: An Overview and Analysis, NIST Interagency Report (IR) 7250, October 2005, <URL: http://csrc.nist.gov/publications/nistir/nistir-7250.pdf>.

[Aye07] Rick Ayers, Wayne Jansen, Aurelien Delaitre, Ludovic Moenner, Cell Phone Forensics Tools: An Overview and Analysis Update, NIST Interagency Report (IR) 7387, February 2007<URL: http://csrc.nist.gov/publications/nistir/nistir-7387.pdf>.

[Bre06] Breeuwsma, M. F., Forensic imaging of embedded systems using JTAG (boundary-scan), Digital Investigation, Volume 3, Issue 1, 2006, pp.32-42.

[Bos05] Jeroen van den Bos, Ronald van der Knijf, TULP2G – An Open Source Forensic Software Framework for Acquiring and Decoding Data Stored in Electronic Devices, International Journal of Digital Evidence, Vol. 4, Issue 2, Fall 2005.

[Bur02] Michael W. Burnette, Forensic Examination of a RIM (BlackBerry) Wireless Device, June 2002, <URL: https://www.rh-law.com/ediscovery/Blackberry.pdf>.

[Bur05] Robert Burnett, Ylva Hård af Segerstad, The SMS Murder Mystery: the dark side of technology, Safety & Security in a Networked World: Balancing Cyber-Rights & Responsibilities, September 2005, <URL: http://www.oii.ox.ac.uk/microsites/cybersafety/extensions/pdfs/papers/robert_burnett.pdf>.

[Car02] Brian Carrier, Defining Digital Forensic Examination and Analysis Tools, Digital Forensics Research Workshop II, August 2002, <URL: http://www.dfrws.org/dfrws2002/papers/Papers/Brian_carrier.pdf>.

[Cas00] Eoghan Casey, Chapter 13: Forensic Examination of Handheld Devices, *Digital Evidence and Computer Crime*, Academic Press, March 2000.

[Cas06] Casadei, F. et al., Forensics and SIM cards: an Overview, International Journal of Digital Evidence, Volume 5, Issue 1, Fall 2006, <URL: http://ieeexplore.ieee.org/iel5/10612/33521/01592525.pdf?isnumber=&arnumber=1592525>.

[Dea05] Dearsley, T., Mobile Phone Forensics – Asking the Right Questions, New Law Journal, July 29, 2005, pp. 1164-1165.

[Dec93] Dechaux, C., Scheller, R., What are GSM and DECT?, Electrical Communication, 2nd Quarter, 1993, pp. 118-127.

[DOJ01] Electronic Crime Scene Investigation: A Guide for First Responders, U.S. Department of Justice, NCJ 187736, July 2001, <URL: http://www.ncjrs.org/pdffiles1/nij/187736.pdf>.

[DOJ04] Forensic Examination of Digital Evidence: A Guide for Law Enforcement, U.S. Department of Justice, NCJ 199408, April 2004, <URL: http://www.ncjrs.org/pdffiles1/nij/199408.pdf>.

[ETS99] Digital cellular telecommunications system (Phase 2) - Event and call data (GSM 12.05 version 4.3.1), European Telecommunication Standard (ETS), ETSI TS 100 616 V7.0.1, July 1999.

[Gar01] You can ring, but you can't hide, The Guardian, November 29, 2001, <URL: http://technology.guardian.co.uk/online/story/0,,608434,00.html>.

[Gas03] Ty Gast, Forensic Data Handling, Security Assurance Group, White Paper, 2003, <URL: http://www.securityassurancegroup.com/PDF/SAG-forensics-data-handling.PDF>.

[Goo03] Amanda Goode, Forensic Extraction of Electronic Evidence from GSM Mobile Phones, IEE Seminar on Secure GSM & Beyond, Digest No. 2003/10059, February 11, 2003.

[Gra02] Joe Grand, pdd: Memory Imaging and Forensic Analysis of Palm OS Devices, Proceedings of the 14th Annual FIRST Conference on Computer Security Incident Handling and Response, June, 2002, <URL: http://www.first.org/events/progconf/2002/d3-04-grand-paper.pdf>.

[GSM04] IMEI Allocation and Approval Guidelines, Version 3.3.0, GSM Association, Permanent Reference Document TW.06, December 2004, <URL: http://www.gsmworld.com/documents/twg/tw06.pdf>.

[GSM05] GSME Position On Data Retention – Implications for The Mobile Industry, GSM Europe, GSM Association, 23 August 2005, <URL: http://www.gsmworld.com/gsmeurope/documents/positions/2005/gsme_position_data_retention.pdf#search=%22GSME%20POSITION%20ON%20DATA%20RETENTION%22>.

[Haa04] Job de Haas, Reverse Engineering ARM Based Devices, Black Hat Europe, May 2004, <URL: https://www.blackhat.com/presentations/bh-europe-04/bh-eu-04-dehaas/bh-eu-04-dehaas.pdf>.

[Hin96] S. F. Hinde, Call Record Analysis, IEE Colloquium on Making Life Easier - Network Design and Management Tools, Digest No: 1996/216, 10 Oct 1996, pp. 8/1-8/4, <URL: http://ieeexplore.ieee.org/iel3/5131/13951/00644775.pdf?isnumber=&arnumber=644775>.

[Hos98] Chet Hosmer, Time Lining Computer Evidence, WetStone Technologies, Inc., 1998, <URL: http://www.wetstonetech.com/f/timelining.pdf>.

[Int96] Designing for On-Board Programming Using the IEEE 1149.1 (JTAG) Access Port, Intel, Application Note, AP-630, November 1996, <URL: http://www.intel.com/design/flcomp/applnots/29218602.PDF>.

[Its] XDA Bootloader, ITSX, <URL: http://www.itsx.com/index.html?pocketpc-bootloader.html~mainFrame>.

[ITU06] ITU-T (2006), Automatic International Telephone Credit Cards, International Telecommunications Union, Telecommunication Standardization Sector (ITU-T), Recommendation E.118, (02/01).

[INT06] Mobile Phone Forensics, 47th EWPITC meeting – Final report, European Working Party on IT Crime, INTERPOL, September 7, 2006.

[IOCE] Digital Evidence: Standards and Principles, Scientific Working Group on Digital Evidence (SWGDE), International Organization on Computer Evidence (IOCE), Forensic Science Communications, Vol. 2, No. 2, April 2000, <URL: http://www.fbi.gov/hq/lab/fsc/backissu/april2000/swgde.htm>.

[Jan06] Wayne Jansen, Rick Ayers, Forensic Software Tools for Cell Phone Subscriber Identity Modules, Conference on Digital Forensics, Association of Digital Forensics, Security, and Law (ADFSL), April 2006, <URL: http://csrc.nist.gov/mobilesecurity/publication/pp-SIM%20tools-final.pdf>.

[Kin01] Joe Grand (Kingpin) and Mudge, Security Analysis of the Palm Operating System and its Weaknesses Against Malicious Code Threats, August 2001, pp. 135-152, Proceedings of the 10th Usenix Security Symposium, <URL: http://www.usenix.org/events/sec01/full_papers/kingpin/kingpin_html>.

[Kni02] Ronald van der Knijff, Chapter 11: Embedded Systems Analysis, *Handbook of Computer Crime Investigation*, Edited by Eoghan Casey, Academic Press, 2002.

[Ko96] Y. F. Ko, Automatic Call Generation and Analysis - Network Testing and Cellular Survey Tools, IEE Colloquium on Making Life Easier - Network Design and Management Tools, Digest No: 1996/217, 10 Oct. 1996, pp. 7/1 - 7/6, <URL: http://ieeexplore.ieee.org/iel3/5131/13951/00644774.pdf?tp=&arnumber=644774&isnumber=13951>.

[Kru01] Warren G. Kruse II, Jay G. Heiser, *Computer Forensics – Incident Response Essentials*, Pearson Education, September 26, 2001.

[Ley01] John Leyden, How to crash a phone by SMS, The Register, November 2001, <URL: http://www.theregister.co.uk/2001/11/28/how_to_crash_a_phone/>

[Man01] Kevin Mandia, Chris Prosise, *Incident Response: Investigating Computer Crime*, McGrawHill Osborne Media, 2001.

[Mcc05] Paul McCarthy, Forensic Analysis of Mobile Phones, BS CIS Thesis, University of South Australia, School of Computer and Information Science, Mawson Lakes, October 2005, <URL: http://esm.cis.unisa.edu.au/new_esml/resources/publications/forensic%20analysis%20of%20mobile%20phones.pdf>.

[Mcc06] Paul McCarthy, Jill Slay, Mobile phones: admissibility of current forensic procedures for acquiring data, the Second IFIP WG 11.9 International Conference on Digital Forensics, 2006.

[Mel04] Barrie Mellars, Forensic Examination of Mobile Phones, Digital Investigation, Vol.1, No. 4, 2004, pp. 266-272.

[Meu02] Pascal Meunier, Sofie Nystrom, Seny Kamara, Scott Yost, Kyle Alexander, Dan Noland, Jared Crane, ActiveSync, TCP/IP and 802.11b Wireless Vulnerabilities of WinCE-based PDAs, Proceedings of the Eleventh IEEE International Workshops on Enabling Technologies: Infrastructure for Collaborative Enterprises (WETICE'02), June 2002, <URL: http://www.cs.nmt.edu/~cs553/paper3.pdf or http://www.cs.jhu.edu/~seny/pubs/wince802.pdf>.

[Moo06] Tyler Moore, The Economics of Digital Forensics, Fifth Annual Workshop on the Economics and Information Security, June 2006, <URL: http://www.cl.cam.ac.uk/~twm29/weis06-moore.pdf>.

[New07] Annalee Newitz, Courts Cast Wary Eye on Evidence Gleaned From Cell Phones, WIRED, May 10, 2007, <URL: http://www.wired.com/politics/law/news/2007/05/cellphone_forensics>.

[NIJ05] No More 'Cell' Phones, TechBeat, Winter 2005, National Law Enforcement and Corrections Technology Center, <URL: http://www.nlectc.org/techbeat/winter2005/NoMoreCellPhones.pdf>.

[Nok05] AT Command Set for Nokia GSM and WCDMA Products, Version 1.2, Nokia Corporation, July 2005, <URL: http://sw.nokia.com/id/95672052-6c77-488d-a055-acef77e4cdc5/AT_Command_Set_For_Nokia_GSM_And_WCDMA_Products_v1_2_en.pdf>.

[NTI] Computer Evidence Processing Steps, New Technologies Inc., <URL: http://www.forensics-intl.com/evidguid.html>.

[Oco04] Thomas R. O'connor, Admissibility of Scientific Evidence Under Daubert, North Carolina Wesleyan College, March 2004, <URL: http://faculty.ncwc.edu/toconnor/daubert.htm>.

[Pie99] Claire Pieterek, How to get an extra 824K using FlashPro, PalmPower Magazine, May 1999, <URL: http://www.palmpower.com/issues/issue199905/flashpro001.html>.

[Pea05] Wayne Peacock, An Introduction to Nokia F-bus, April 2005, <URL: http://www,embedtronics.com/nokia/fbus.html>.

[Pmd02] Palm Security, How-To Guide, pdaMD.com, 2002, <URL: http://www.pdamd.com/vertical/tutorials/palmsecure.xml>.

[PPC04] Palm OS Programmer's Companion, Volume I, PalmSource, Inc., May 2004, <URL: http://www.palmos.com/dev/support/docs/palmos/CompanionTOC.html>.

[Pur] Stephen R. Purdy, The Reality of Computer Forensics: Electronic Evidence Discovery and Recovery, Agile Risk Management Group LLC.

[Rei02] Mark Reith, Clint Carr, and Gregg Gunsch, An Examination of Digital Forensic Models, International Journal of Digital Evidence, Fall 2002, Volume 1, Issue 3 <URL: http://www.ijde.org/docs/02_fall_art2.pdf>.

[Sha06] Noah Shachtman Fighting Crime with Cellphones' Clues, NY Times, May 3, 2006, <URL: http://www.mobileforensicstraining.com/inthenews_main.html>.

[Smi05] Greg Smith, Switch On ~ Update = Lose Evidence, Mobile Telephone Evidence Newsletter, INDEX NO: VOL 4-MTE05- 2006, Trew & Co, 2005, <URL: http://filebucket.org/files/7019_h66bf/Switch%20On%20Update%20Lose%20Evidence>.

[Smi06] Greg Smith, Handset Password Unlock, Mobile Telephone Evidence Newsletter, INDEX NO: VOL 4-MTE03- 2006 supp: 002, Trew & Co, 2006.

[Sum03] Chris Summers, Mobile phones - the new fingerprints, BBC News Online, December 18, 2003, <URL: http://newsvote.bbc.co.uk/mpapps/pagetools/print/news.bbc.co.uk/1/hi/uk/3303637.stm>.

[Vam07] Robert Vamosi, Cell Phone 'CSI,' CNET Reviews, May 25, 2007, ,URL: http://reviews.cnet.com/4520-3513_7-6737586-1.htm>.

[Ved93] Vedder, K., 1993, Security Aspects of Mobile Communications, in Computer Security and Industrial Cryptography - State of the Art and Evolution, Lecture Notes in Computer Science, Vol. 741, pp. 193-210.

[Wie02] Officer Fred J.Wiechmann, Processing Flash Memory Media, New Technologies Inc., November 2002, <URL: http://www.forensics-intl.com/art16.html>.

[Wil03] Svein Willassen, Forensics and the GSM Mobile Telephone System, International Journal of Digital Evidence, Volume 2, Issue 1, 2003, <URL: http://www.utica.edu/academic/institutes/ecii/publications/articles/A0658858-BFF6-C537-7CF86A78D6DE746D.pdf>.

[Wil05] Svein Willassen, Forensic Analysis of Mobile Phone Internal Memory, IFIP WG 11.9 International Conference on Digital Forensics, National Center for Forensic Science, Orlando, Florida, February 13-16, 2005, in Advances in Digital Forensics, Vol. 194, Pollitt, M.; Shenoi, S. (Eds.), XVIII, 313 p., 2006.

[Wol03] Henry B.Wolfe, Evidence Analysis, Computers and Security, May 2003, Volume 22, Issue 4, pp. 289-291, <URL: http://www.sparksdata.co.uk/elseforms/order/COSE%202201.pdf>.

[Wyl00] Margie Wylie, Cell Phone Jammers, Illegal in U.S., Can Create Silent Zones, Newhouse News Service, 2000, <URL: http://www.newhousenews.com/archive/story1a092200.html>.

[Xjt03] JTAG testing with XJTAG, Version 0.1, XJTAG, March 2003, <URL: http://www.xjtag.com/images/TestingWithXJTAG.pdf>.

Appendix A. Acronyms

APDU – Application Protocol Data Unit

API – Application Programming Interface

ASCII – American Standard Code for Information Interchange

BCD – Binary Coded Decimal

BSC – Base Station Controller

BTS – Base Transceiver Station

CDMA – Code Division Multiple Access

CF – Compact Flash

EDGE – Enhanced Data for GSM Evolution

EMS – Enhanced Messaging Service

ESN – Electronic Serial Number

FCC ID – Federal Communications Commission Identification Number

GPRS – General Packet Radio Service

GPS – Global Positioning System

GSM – Global System for Mobile Communications

HTTP – HyperText Transfer Protocol

ICCID – Integrated Circuit Card Identification

IDE – Integrated Drive Electronics

iDEN – Integrated Digital Enhanced Network

IM – Instant Messaging

IMAP – Internet Message Access Protocol

IMEI – International Mobile Equipment Identity

IMSI – International Mobile Subscriber Identity

IrDA – Infra Red Data Association

JTAG – Joint Test Action Group

LCD – Liquid Crystal Display

LED – Light Emitting Diode

MD5 – Message Digest 5

MMC – Multi-Media Card

MMS – Multimedia Messaging Service

MSC – Mobile Switching Center

MSISDN – Mobile Subscriber Integrated Services Digital Network

OS – Operating System

PC – Personal Computer

PDA – Personal Digital Assistant

PIM – Personal Information Management

PIN – Personal Identification Number

POP – Post Office Protocol

RAM – Random Access Memory

ROM – Read Only Memory

SD – Secure Digital

SDK – Software Development Kit

SHA1 – Secure Hash Algorithm, version 1

SIM – Subscriber Identity Module

SMS – Short Message Service

SMTP – Simple Mail Transfer Protocol

TCP/IP – Transmission Control Protocol/Internet Protocol

TDMA – Time Division Multiple Access

UMTS – Universal Mobile Telecommunications System

URL – Uniform Resource Locator

USB – Universal Serial Bus

USIM – UMTS Subscriber Identity Module

WAP – Wireless Application Protocol

WiFi – Wireless Fidelity

XHTML – Extensible HyperText Markup Language

XML – Extensible Markup Language

Appendix B. Glossary

Acquisition – A process by which digital evidence is duplicated, copied, or imaged.

Analysis – The examination of acquired data for its significance and probative value to the case.

Authentication Mechanism – Hardware or software-based mechanisms that force users to prove their identity before accessing data on a device.

Bluetooth – A wireless protocol that allows two Bluetooth enabled devices to communicate with each other within a short distance (e.g., 30 ft.).

Brute Force Password Attack – A method of accessing an obstructed device by attempting multiple combinations of numeric/alphanumeric passwords.

Buffer Overflow Attack – A method of overloading a predefined amount of space in a buffer, which can potentially overwrite and corrupt memory in data.

Chain of Custody – A process that tracks the movement of evidence through its collection, safeguarding, and analysis lifecycle by documenting each person who handled the evidence, the date/time it was collected or transferred, and the purpose for the transfer.

Code Division Multiple Access (CDMA) – A spread spectrum technology for cellular networks based on the Interim Standard-95 (IS-95) from the Telecommunications Industry Association (TIA).

Compressed File – A file reduced in size through the application of a compression algorithm, commonly performed to save disk space. The act of compressing a file will make it unreadable to most programs until the file is uncompressed. Most common compression utilities are PKZIP and WinZip, which produce files with an extension of .zip.

Cradle – A docking station, which creates an interface between a user's PC and PDA, and enables communication and battery recharging.

Cyclical Redundancy Check – A method to ensure data has not been altered after being sent through a communication channel.

Deleted File – A file that has been logically, but not necessarily physically, erased from the operating system, perhaps to eliminate potentially incriminating evidence. Deleting files does not always necessarily eliminate the possibility of recovering all or part of the original data.

Digital Evidence – Electronic information stored or transmitted in binary form.

Duplicate Digital Evidence – A duplicate is an accurate digital reproduction of all data objects contained on the original physical item and associated media (e.g., flash memory, RAM, ROM).

Electromagnetic Interference – An electromagnetic disturbance that interrupts, obstructs, or otherwise degrades or limits the effective performance of electronics/electrical equipment.

Electronic Evidence – Information and data of investigative value that is stored on or transmitted by an electronic device.

Electronic Serial Number (ESN) – A unique 32-bit number programmed into CDMA phones when they are manufactured.

Encryption – Any procedure used in cryptography to convert plain text into cipher text to prevent anyone but the intended recipient from reading that data.

Enhanced Data for GSM Evolution (EDGE) – An upgrade to GPRS to provide higher data rates by joining multiple time slots.

Enhanced Messaging Service (EMS) – An improved message system for GSM mobile phones allowing picture, sound, animation and text elements to be conveyed through one or more concatenated SMS messages.

Examination – A technical review that makes the evidence visible and suitable for analysis; tests performed on the evidence to determine the presence or absence of specific data.

Exculpatory Evidence – Evidence that tends to decrease the likelihood of fault or guilt.

Extensible HyperText Markup Language (XHTML) – A unifying standard that brings the benefits of XML to those of HTML.

Extensible Markup Language (XML) – A flexible text format designed to describe data for electronic publishing.

File Name Anomaly – A mismatch between the internal file header and its external file name extension; a file name inconsistent with the content of the file (e.g., renaming a graphics file with a non-graphics extension).

File System – A software mechanism that defines the way that files are named, stored, organized, and accessed on logical volumes of partitioned memory.

Flash ROM – Non-volatile memory that is writable.

Forbidden PLMNs – A list of Public Land Mobile Networks (PLMNs) maintained on the SIM that the phone cannot automatically contact, usually because service was declined by a foreign provider.

Forensic Copy – An accurate bit-for-bit reproduction of the information contained on an electronic device or associated media, whose validity and integrity has been verified using an accepted algorithm.

Forensic Specialist – Locates, identifies, collects, analyzes and examines data while preserving the integrity and maintaining a strict chain of custody of information discovered.

General Packet Radio Service (GPRS) – A packet switching enhancement to GSM and TDMA wireless networks to increase data transmission speeds.

Global Positioning System – A system for determining position by comparing radio signals from several satellites.

Global System for Mobile Communications (GSM) – A set of standards for second generation, cellular networks currently maintained by the 3rd Generation Partnership Project (3GPP).

Hardware Driver – Applications responsible for establishing communication between hardware and software programs.

Hashing – The process of using a mathematical algorithm against data to produce a numeric value that is representative of that data.

HyperText Transfer Protocol (HTTP) – A standard method for communication between clients and Web servers.

Image – An exact bit-stream copy of all electronic data on a device, performed in a manner that ensures the information is not altered.

Inculpatory Evidence – Evidence that tends to increase the likelihood of fault or guilt.

Instant Messaging (IM) – A facility for exchanging messages in real-time with other people over the Internet and tracking the progress of the conversation.

Integrated Circuit Card ID (ICCID) – The unique serial number assigned to, maintained within, and usually imprinted on the (U)SIM.

Integrated Digital Enhanced Network (iDEN) – A proprietary mobile communications technology developed by Motorola that combine the capabilities of a digital cellular telephone with two-way radio.

International Mobile Equipment Identity (IMEI) – A unique identification number programmed into GSM and UMTS mobile phones.

International Mobile Subscriber Identity (IMSI) – A unique number associated with every GSM mobile phone subscriber, which is maintained on a (U)SIM.

Internet Message Access Protocol (IMAP) – A method of communication used to read electronic messages stored in a remote server.

Location Information (LOCI) – The Location Area Identifier (LAI) of the phone's current location, continuously maintained on the (U)SIM when the phone is active and saved whenever the phone is turned off.

Misnamed Files – A technique used to disguise a file's content by changing the file's name to something innocuous or altering its extension to a different type of file, forcing the examiner to identify the files by file signature versus file extension.

Mobile Subscriber Integrated Services Digital Network (MSISDN) – The international telephone number assigned to a cellular subscriber.

Multimedia Messaging Service (MMS) – An accepted standard for messaging that lets users send and receive messages formatted with text, graphics, photographs, audio, and video clips.

Password Protected – The ability to protect the contents of a file or device from being accessed until the correct password is entered.

Personal Digital Assistant (PDA) – A handheld computer that serves as a tool for reading and conveying documents, electronic mail, and other electronic media over a communications link, and for organizing personal information, such as a name-and-address database, a to-do list, and an appointment calendar.

Personal Information Management (PIM) Applications – A core set of applications that provide the electronic equivalents of such items as an agenda, address book, notepad, and reminder list.

Personal Information Management (PIM) Data – The set of data types such as contacts, calendar entries, phonebook entries, notes, memos, and reminders maintained on a device, which may be synchronized with a personal computer.

Post Office Protocol (POP) – A standard protocol used to receive electronic mail from a server.

Probative Data – Information that reveals the truth of an allegation.

Short Message Service (SMS) – A cellular network facility that allows users to send and receive text messages of up to 160 alphanumeric characters on their handset.

Simple Mail Transfer Protocol (SMTP) – The primary protocol used to transfer electronic mail messages on the Internet.

SMS Chat – A facility for exchanging messages in real-time using SMS text messaging that allows previously exchanged messages to be viewed.

Steganography – The art and science of communicating in a way that hides the existence of the communication. For example, a child pornography image can be hidden inside another graphic image file, audio file, or other file format.

Subscriber Identity Module (SIM) – A smart card chip specialized for use in GSM equipment.

Synchronization Protocols – Protocols that allow users to view, modify, and transfer/update data between a cell phone and personal computer.

UMTS Subscriber Identity Module (USIM) – A module similar to the SIM in GSM/GPRS networks, but with additional capabilities suited to 3G networks.

Universal Mobile Telecommunications System (UMTS) – A third-generation (3G) mobile phone technology standardized by the 3GPP as the successor to GSM.

Universal Serial Bus (USB) – A hardware interface for low-speed peripherals such as the keyboard, mouse, joystick, scanner, printer, and telephony devices.

Volatile Memory – Memory that loses its content when power is turned off or lost.

Wireless Application Protocol (WAP) – A standard that defines the way in which Internet communications and other advanced services are provided on wireless mobile devices.

Wireless Fidelity (WiFi) – A term describing a wireless local area network that observes the IEEE 802.11 protocol.

Write-Blocker – A device that allows investigators to examine media while preventing data writes from occurring on the subject media.

Write Protection – Hardware or software methods of preventing data from being written to a disk or other medium.

Extensible HyperText Markup Language (XHTML) – A unifying standard that brings the benefits of XML to those of HTML.

Extensible Markup Language (XML) – A flexible text format designed to describe data for electronic publishing.

Appendix C. Generic Acquisition Overview

This appendix gives an overview of the acquisition of a mobile phone and (U)SIM. Most tools have an acquisition wizard that guides one successfully through the process. An idealized explanation of the steps involved is outlined below, illustrated using excerpts of screen shots taken from a number of different tools.

C.1 Connection Identification

The initial step is identifying the type of connection to use. The three choices often offered are connecting via a cable, an infrared interface, or a Bluetooth interface, as shown in Figure 7. Generally, the order listed is the preferred order of selection. However, other forensic issues may exist for the connection type when used with a particular device. The tool manufacturer's user guide and Web site or an independent tool guidance database can sometimes be checked for clarification.

Figure 7: Connection Identification

C.2 Device Identification

Once the type of connection being used is determined, the device can be identified. Often this is done through the manufacturer name and device model number. Some tools may attempt to identify the device automatically. Note that some toolkits, such as the one shown in Figure 8, support both phone and (U)SIM acquisition and offer both choices.

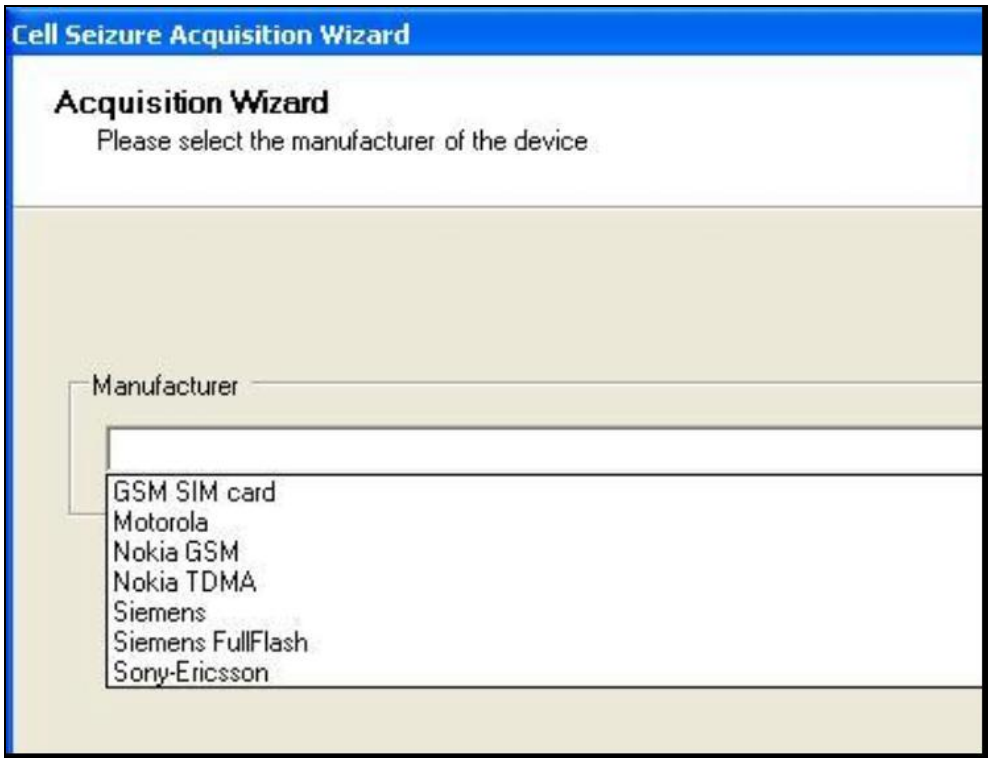

Figure 8: Device Acquisition

C.3 Data Selection

Most tools offer a choice of recovering a subset of the data expected to be recovered, such as that illustrated in Figure 9. That option might be useful if the reporting capabilities of the tool automatically generate a report of all items acquired. Alternatively, performing a complete acquisition may be reasonable if the reporting capabilities of the tool allow the selected items of interest to be selectively reported. One side benefit with this approach is that the case file can be maintained and referenced later, if additional types of information are needed.

Note that the recoverable items listed can differ among mobile phones, depending on the phone's capabilities. Note too that forensic issues may exist that might oblige one to skip recovery of a particular item.

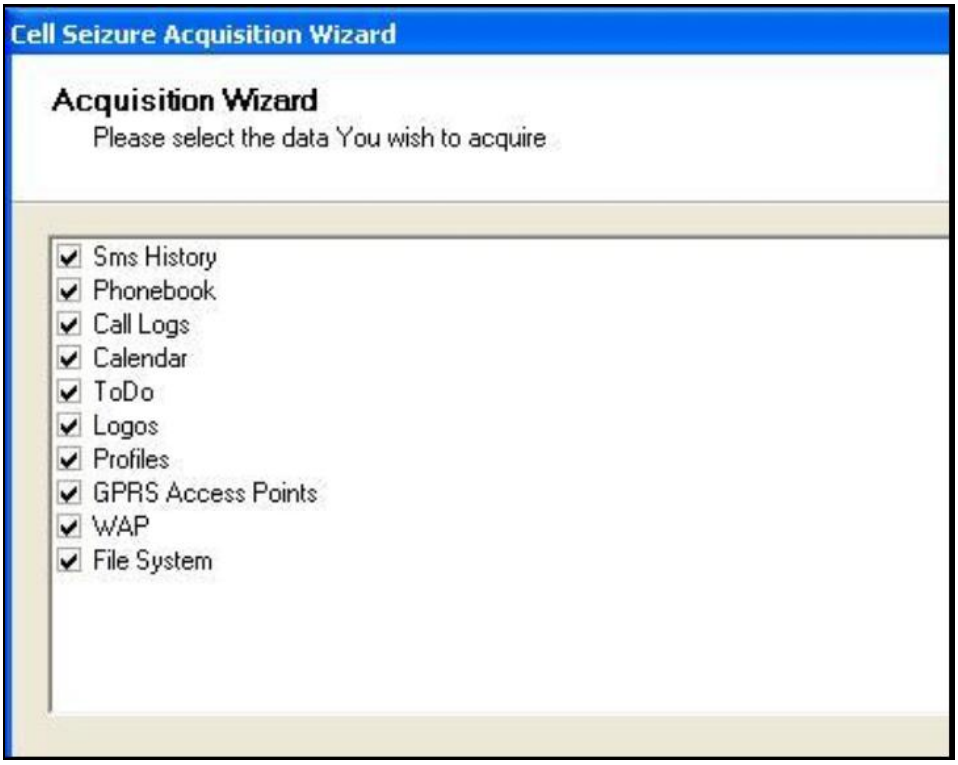

Figure 9: Data Selection

C.4 Acquisition

After the data to recover is selected, acquisition begins. Acquisition may proceed quietly with a progress bar or more informatively with a viewable log of the progress. The latter is illustrated in Figure 10, which shows a summary of the different protocols being attempted (i.e., AT commands defined in a GSM standard and proprietary FBUS commands) and the status of the attempts made.

While high level logs are informative, some tools can also capture a detailed log of the entire acquisition. Detailed logs can be useful in a number of ways: they may provide information to the tool manufacturer if the tool fails; they can confirm that the protocol commands were of a read-only nature; and they may occasionally contain useful forensic data not reported by the tool.

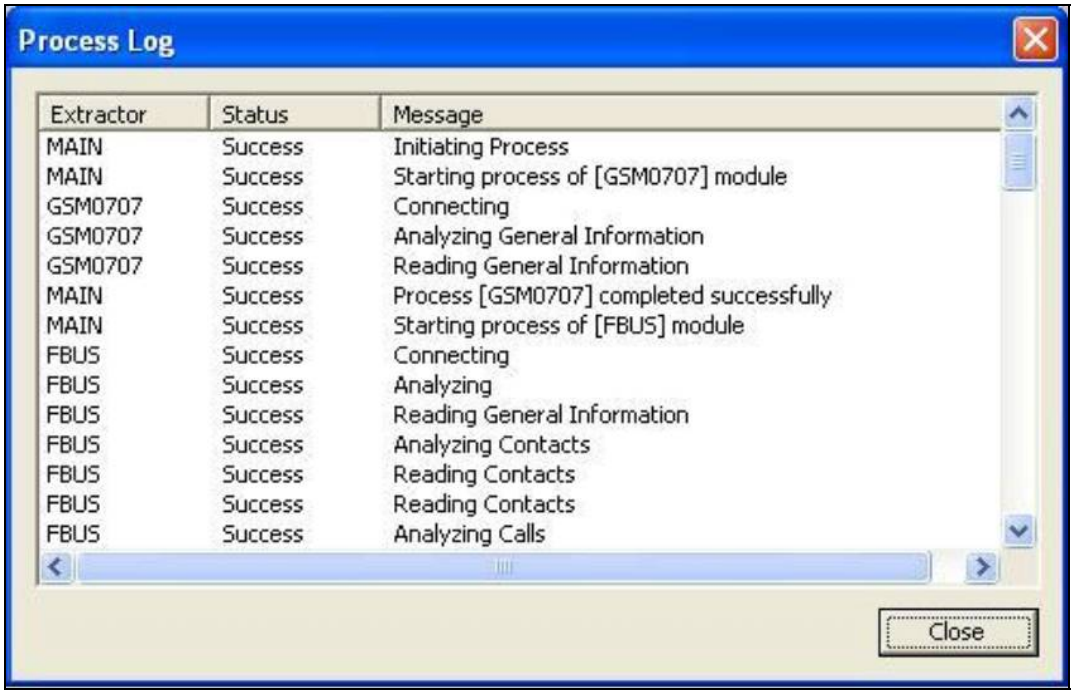

Figure 10: Acquisition

Upon completion of the acquisition, some arrangement of the recovered data is made available for selection. The items for selection are commonly presented in the form of tabbed displays or a hierarchical tree structure.

C.5 Phonebook Entries

Phonebook entries may contain more than just names and phone numbers, including such things as email and postal addresses, as shown in Figure 11. Some camera phones can also store and display a photo of individuals along with their contact information.

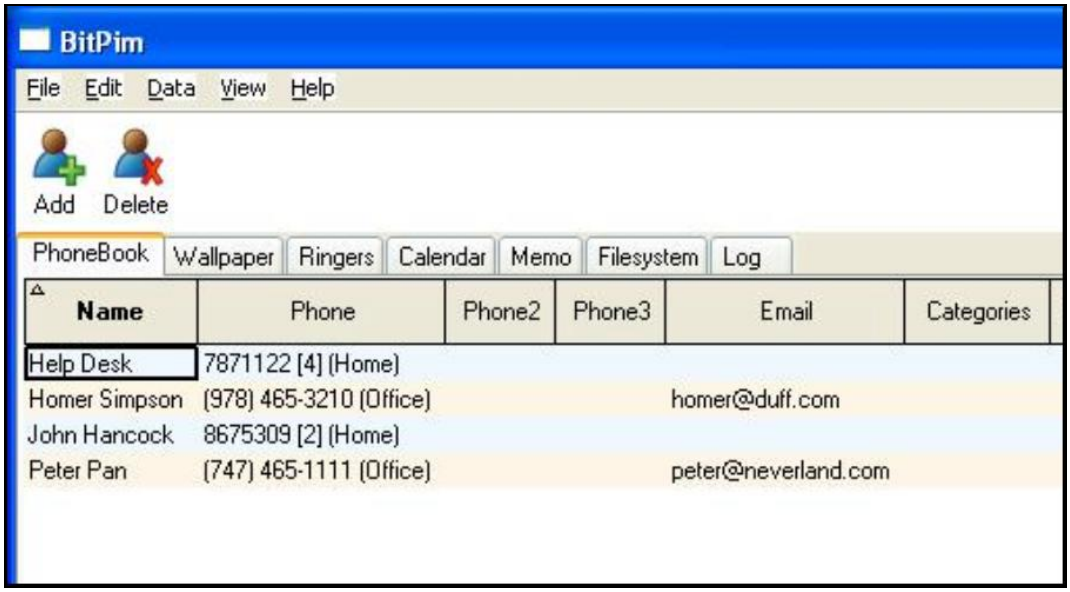

Figure 11: Phonebook Entries

C.6 Call Log Entries

Phone logs capture the set of recent calls attempted from the phone, received by the phone, and missed by the phone, as illustrated in Figure 12.

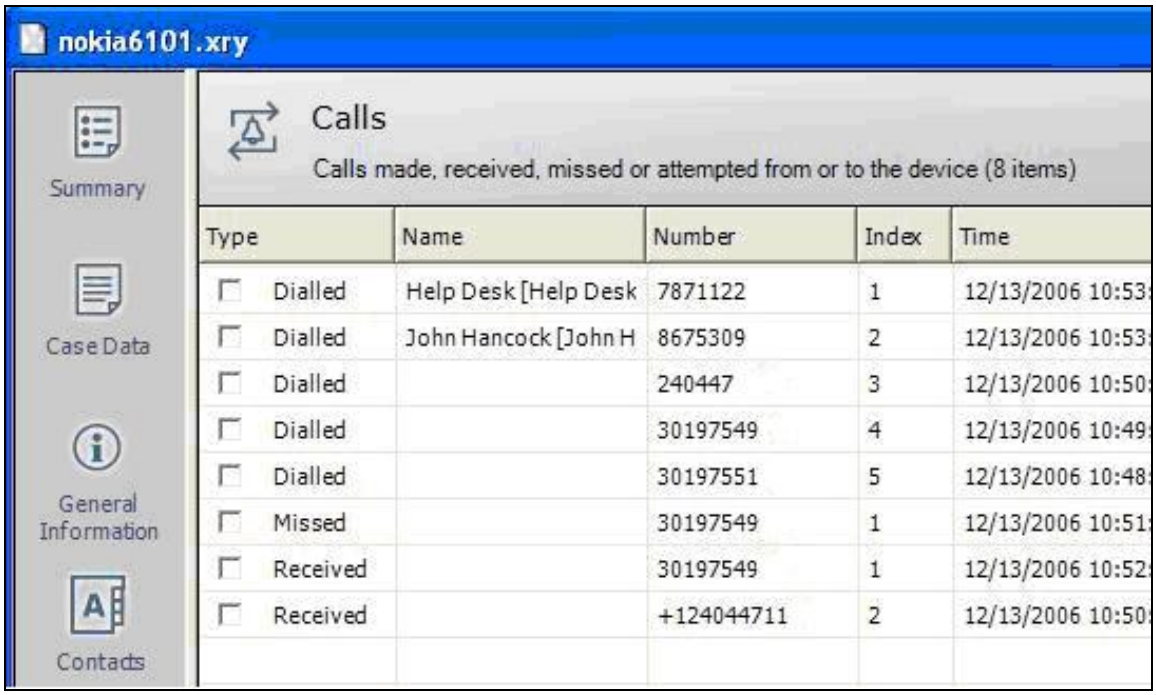

Figure 12: Call Log Entries

C.7 Message Entries

Message entries include both text and multimedia messages received and sent by the phone. Figure 13 illustrates some simple text message entries, while Figure 14 illustrates some multimedia message entries.

SMS

SMS messages sent or received from the device (32 items)

Number	Name	Message	Time	Status
+12404		This is to determine if sms messages can be properly acquired?	5/30/2006 2:17:32 PM	Read
240447		This is the last sms message i've sent.	12/11/2006 11:51:12 AM	Sent
240447		Outgoing sms message sent via nokia 6101	12/11/2006 11:48:00 AM	Sent

Figure 13: SMS Text Messages

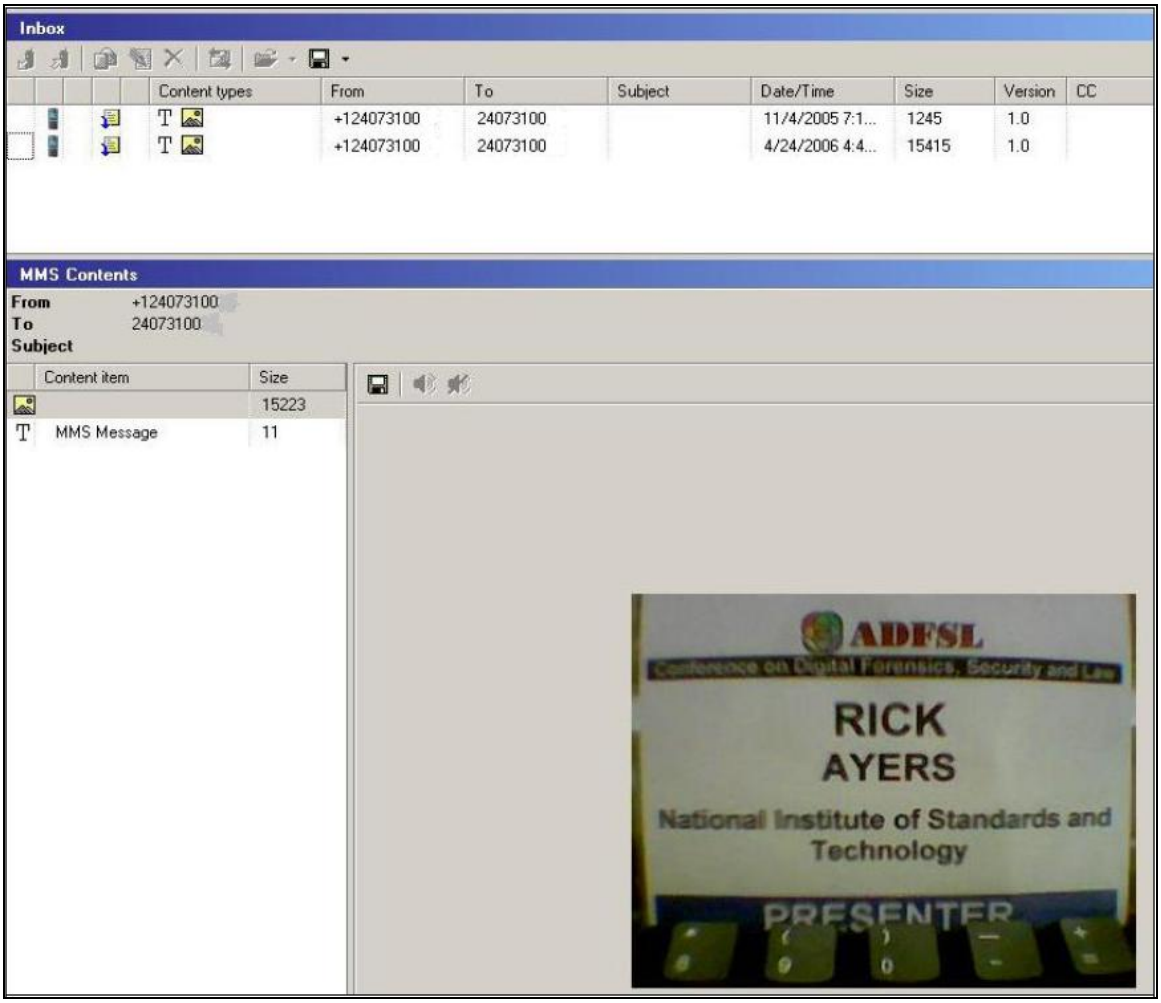

Figure 14: Multimedia Message

C.8 Calendar Entries

Calendar entries are sometimes known as appointment books. Similar to a paper agenda carried by individuals, calendar entries provide an electronic counterpart, maintaining the date and time of some scheduled event. Figure 15 illustrates a calendar page containing active entries.

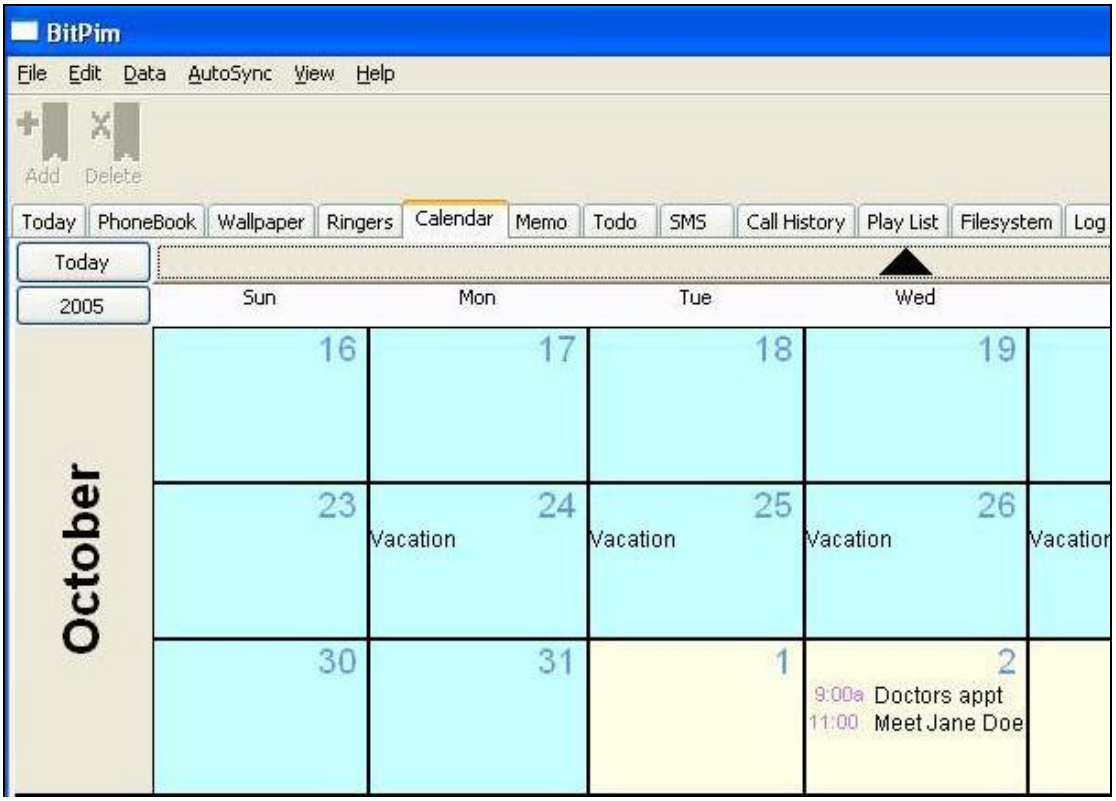

Figure 15: Calendar Entries

C.9 (U)SIM Data

(U)SIM data may be acquired in two ways: indirectly through commands sent to the phone and passed on to the (U)SIM or directly through commands sent to a (U)SIM reader into which the (U)SIM is placed. Figure 16 illustrates the latter. This presumes, of course, that the device identification selection made for the acquisition was a GSM SIM card instead of a mobile phone.

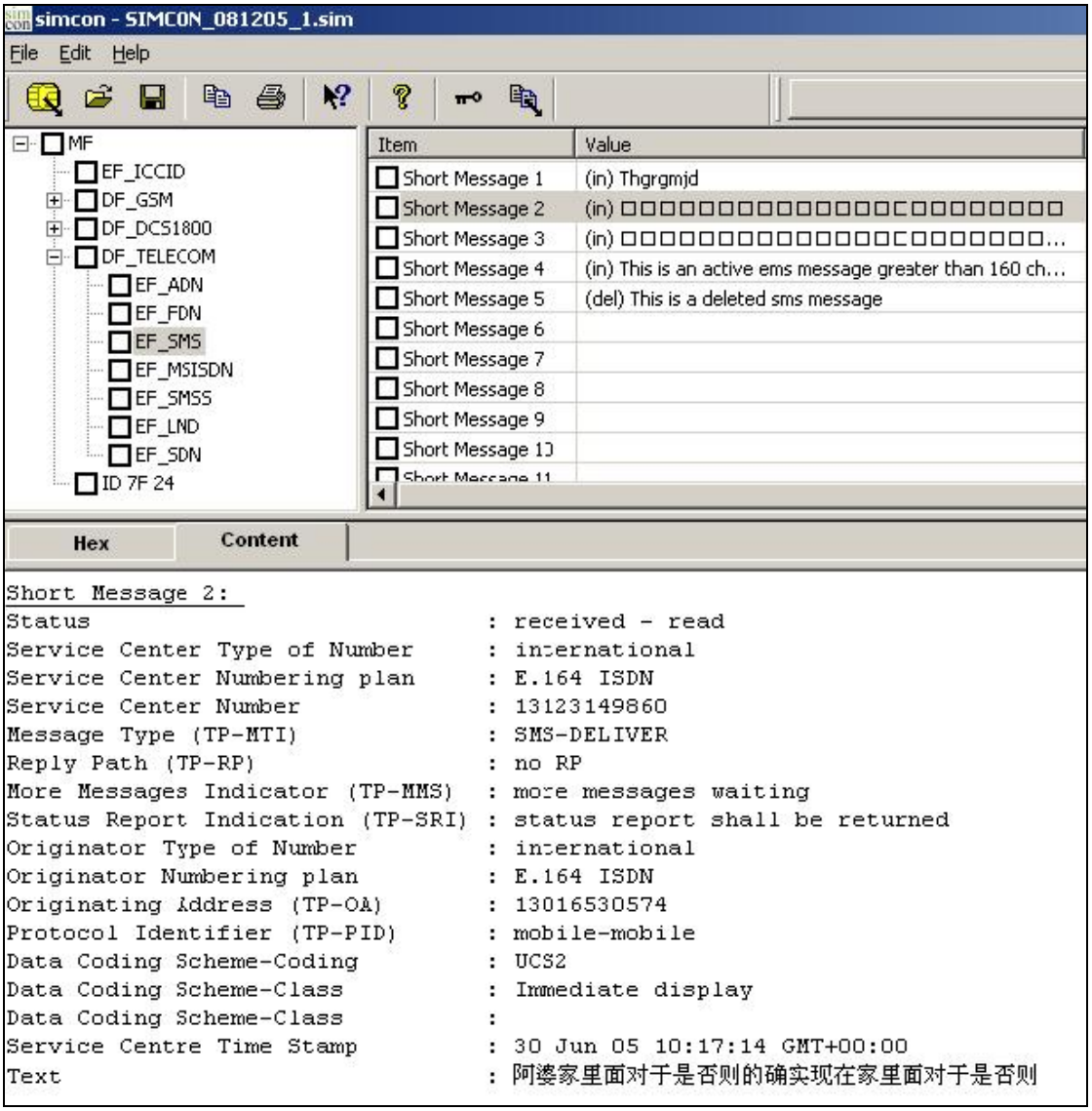

Figure 16: (U)SIM Data

The hierarchical tree structure at the upper left reflects the file system of the (U)SIM. The contents of highlighted item selected in the tree structure (i.e., SMS text messages) are shown at the upper right and also in the window below.

C.10 Picture Entries

Many mobile phones have a built-in camera and are capable of receiving messages containing photos. The photos taken can reside in the memory of the phone or in removable memory cards present in the device. Figure 17 illustrates a gallery of the images found on a mobile phone collected together for examination and displayed as thumbnail images.

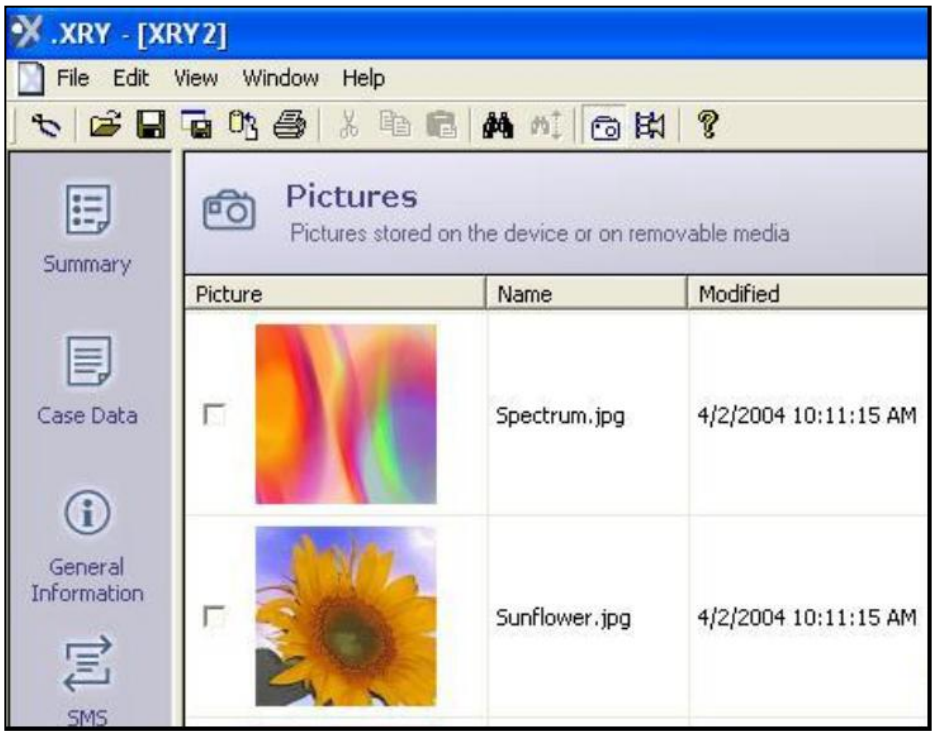

Figure 17: Picture Entries

C.11 Searching

Searching for a specific name or number within a body of digital evidence can be aided with a search facility. Figure 18 illustrates a simple name search. A tool may be able to control the scope of a search to include the current case file, a portion of the case file, or a set of case files.

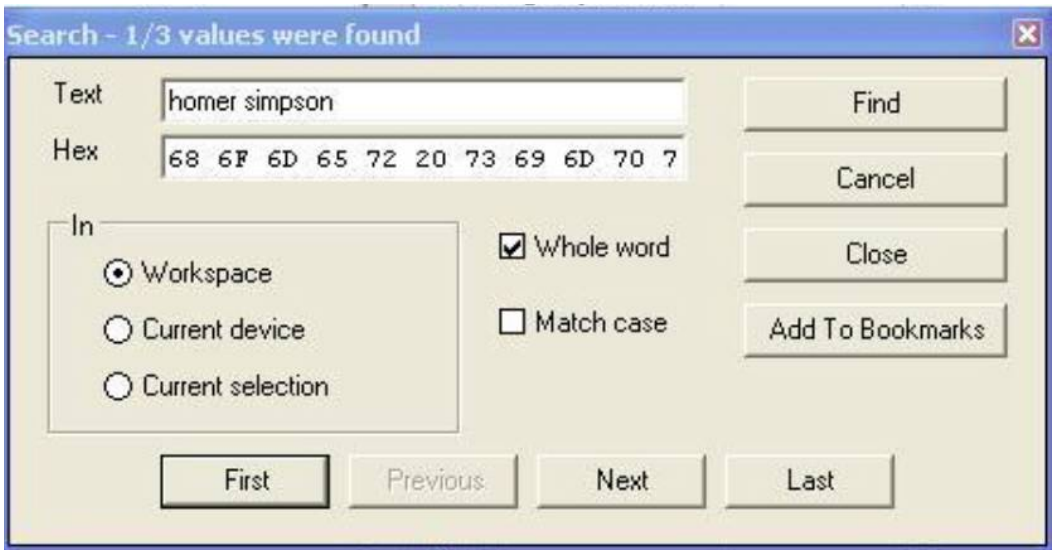

Figure 18: Search Facility

C.12 Reporting

Reporting allows the generation of a report in a variety of formats, as shown in Figure 19. Other formats that may be supported by a tool's report facility include XML and Microsoft Word. The report facility may also support tailoring of the report output to include laboratory names and logos and information acquired elsewhere, such as photos of the device at seizure or at receipt by the laboratory.

Figure 19: Report Facility

Appendix D. Standardized Call Records

The European Telecommunications Standards Institute specification for GSM event and call data provides detailed definitions for a variety of records needed in the administration of subscriber related event and call data. Table 7 gives the record structure for a mobile-originated call attempt, identifying and describing the name of the various fields involved and an indication of whether the field is mandatory (M), conditional (C), or optional (O).

Other record definitions also appear in the standard. The reader is asked to consult the standard directly for a more detailed explanation of the use of each field given in Table 7 and a better understanding of the range of records and data involved in network administration.

Table 7: Example Record Structure

Field	Key	Description
Record Type	M	Mobile originated
Served IMSI	M	IMSI of the calling party
Served IMEI	C	IMEI of the calling ME, if available
Served MSISDN	O	The primary MSISDN of the calling party
Called Number	M	The address of the called party, e.g., the number dialed by the calling subscriber
Translated Number	O	The called number after digit translation within the MSC (if applicable)
Connected Number	O	The number of the connected party if different from the Called Number
Roaming Number	O	The Mobile Station Roaming Number employed to route this connection, if applicable
Recording Entity	M	The E.164 number of the visited MSC producing the record
Incoming TKGP	O	The MSC trunk group on which the call originated, usually from the BSS
Outgoing TKGP	O	The trunk group on which the call left the MSC
Location	M	The identity of the cell in which the call originated including the location area code
Change of Location	O	A list of changes in Location Area Code / Cell Id., each time-stamped
Basic Service	M	Bearer or teleservice employed
Transparency Indicator	C	Only provided for those teleservices which may be employed in both transparent and non-transparent mode
ChangeOfService	O	A list of changes of basic service during a connection each time-stamped
Supp. Services	C	Supplementary services invoked as a result of this connection
AOC Parameters	O	The charge advice parameters sent to the MS on call setup
Change of AOC Parms	O	New AOC parameters sent to the MS, e.g., as a result of a tariff switch over, including the time at which the new set was applied
MS Classmark	M	The mobile station classmark employed on call setup
Change of Classmark	O	A list of changes to the classmark during the connection, each time-stamped
Event Time Stamps	C C O	Seizure of incoming traffic channel (for unsuccessful call attempts) Answer (for successful calls) Release of traffic channel
Call Duration	M	The chargeable duration of the connection for successful calls, the holding time for call attempts

Radio Chan. Requested	O	The type of radio traffic channel (full / half etc.) requested by the MS
Radio Chan. Used	M	The type of radio channel actually used (full or half rate)
Change of Rad. Chan.	O	A list of changes, each timestamped
Cause for Termination	M	The reason for the release of the connection
Diagnostics	O	A more detailed reason for the release of the connection
Data Volume	C	The number of data segments transmitted, if available at the MSC
Sequence No.	C	Partial record sequence number, only present in case of partial records
Call Reference	M	A local identifier distinguishing between transactions on the same MS
Additional Chg. Info	O	Charge/no charge indicator and additional charging parameters
Record Extensions	O	A set of network/manufacturer specific extensions to the record
gsmSCF address	C	Identifies the CAMEL server serving the subscriber
Service Key	C	The CAMEL service logic to be applied
Network Call Reference	C	An identifier to correlate transactions on the same call taking place in different network nodes, shall be present if CAMEL is applied
MSC Address	C	This field contains the E.164 number assigned to the MSC that generated the network call reference
Default Call Handling	O	Indicates whether or not a CAMEL call encountered default call handling – Shall be present only if default call handling has been applied
Number of HSCSD Channels Requested	C	The maximum number of HSCSD channels requested as received from the MS at call set-up
Number of HSCSD Channels Allocated	C	The number of HSCSD channels allocated to the MS at call set-up
Change of HSCSD Parameters	C	A list of network or user initiated changes of number of HSCSD channels during a connection, each timestamped – Shall only be present in case of an HSCSD call, if the basic HSCSD parameters are modified due to the user or network initiated modification procedure
Fixed Network User Rate	O	May be present for HSCSD connections
Air Interface User Rate Requested	C	The total Air Interface User Rate Requested by the MS at call setup. Shall only be present for non-transparent HSCSD connections
Channel Coding Accepted	C	A list of the traffic channels codings accepted by the MS – Shall only be present for HSCSD connections
Channel Coding Used	C	The traffic channels codings negotiated between the MS and the network at call setup – Shall only be present for HSCSD connections
Speech Version Used	O	Speech version used for that call
Speech Version Supported	O	Speech version supported by the MS with highest priority indicated by MS
Number of DP Encountered	O	Number that counts how often armed detection points (TDP and EDP) were encountered
Level of CAMEL service	O	Indicator for the complexity of the CAMEL feature used
Free format Data	C	This field contains data sent by the gsmSCF in the FCI message
CAMEL Call Leg Information	C	Set of CAMEL information IEs. Each of these IEs contains information related to one outgoing CAMEL call leg

Appendix E. Online Resources for Mobile Device Forensics

This appendix contains lists of online resources that may be useful to incident response communities and law enforcement when mobile devices are encountered during an incident or crime. The resources provide additional information on aspects of cell phone forensics.

Table 8: Technical Resource Sites

Resource	URL
The Electronic Evidence Information Center	http://www.e-evidence.info/cellular.html
High Tech Crime Consortium mail list	https://htcc.secport.com/mailman/listinfo/htcc
Phone Forensics Portal	http://www.phone-forensics.com/forum/portal.php
Phone Forensics Group	http://groups.yahoo.com/group/phoneforensics/
SEARCH: Investigator's Toolkit	http://www.search.org/files/pdf/CellphoneInvestToolkit-0806.pdf
The Netherlands Forensic Institute's procedures for preservation	http://www.holmes.nl/MPF/FlowChartForensicMobilePhoneExamination.htm
Secure Digital Homepage	http://www.Sdcard.org
Multi-Media Card Homepage	http://www.mmca.org
CDMA Documents	http://www.tiaonline.org/standards/technology/cdma2000/cdma2000table.cfm

Table 9: Databases for Identification Queries

Resource	URL
Device Characteristics	http://www.phonescoop.com/phones/finder.php http://www.gsmarena.com/search.php3 http://mobile.softpedia.com/phoneFinder
IMEI Queries	http://www.numberingplans.com/?page=analysis&sub=imeinr
Manufacturer Codes	http://www.tiaonline.org/standards/resources/esn/codes.cfm
ICCID Queries	http://www.numberingplans.com/?page=analysis&sub=simnr
FCCID Queries	http://www.fcc.gov/oet/fccid/
Phone Carrier Finder	http://www.fonefinder.net/
Phone Number Carrier Lookup	www.npac.com

Table 10: Forensic Tools

Resource	URL
Forensic Card Reader	http://www.becker-partner.de/forensic/intro_e.htm
ForensicSIM	http://www.radio-tactics.com
SIMCon	http://www.simcon.no
SIMIS	http://www.crownhillmobile.com
USIMdetective	http://www.quantaq.com/
BitPIM	http://www.bitpim.org

Resource	URL
Oxygen PM (forensic version)	http://www.opm-2.com/forensic
Oxygen PM for Symbian (forensic version)	http://www.opm-2.com/forensic
PDA Seizure	http://www.paraben-forensics.com
Pilot-Link	http://www.pilot-link.org
Cell Seizure	http://www.paraben-forensics.com
CellDEK	http://www.logicubeforensic.com
GSM .XRY	http://www.msab.com
MobilEdit!	http://www.mobiledit.com
PhoneBase	http://www.phonebase.info
Secure View	http://www.susteen.com
TULP 2G	http://tulp2g.sourceforge.net
SIMgen	http://www.3gforensics.co.uk/simgen.html

Table 11: Other Related Tools

Resource	URL
CSurv	http://www.teeltech.com/tt/TeelTechCsurv.pdf.pdf
Cell View	http://www.icardforensics.com/documents/CellSiteMonitor.pdf
Port Monitoring Utilities	http://www.sysinternals.com/Utilities/Portmon.html http://www.hhdsoftware.com/sermon.html
Master Unlock Code Calculator	http://www.fonefunshop.co.uk/Unlocking/nokiasecuritycode.htm