visited on 12/9/2016

NIST Special Publication 800-101
Revision 1

Guidelines on Mobile Device Forensics

Rick Ayers
Sam Brothers
Wayne Jansen

http://dx.doi.org/10.6028/NIST.SP.800-101r1

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

visited on 12/9/2016

NIST Special Publication 800-101
Revision 1

Guidelines on Mobile Device Forensics

Rick Ayers
Software and Systems Division
Information Technology Laboratory

Sam Brothers
U.S. Customs and Border Protection
Department of Homeland Security
Springfield, VA

Wayne Jansen
Booz Allen Hamilton
McLean, VA

http://dx.doi.org/10.6028/NIST.SP. 800-101r1

May 2014

U.S. Department of Commerce
Penny Pritzker, Secretary

National Institute of Standards and Technology
Patrick D. Gallagher, Under Secretary of Commerce for Standards and Technology and Director

visited on 12/9/2016

Authority

This publication has been developed by NIST in accordance with its statutory responsibilities under the Federal Information Security Management Act of 2002 (FISMA), 44 U.S.C. § 3541 *et seq.*, Public Law (P.L.) 107-347. NIST is responsible for developing information security standards and guidelines, including minimum requirements for Federal information systems, but such standards and guidelines shall not apply to national security systems without the express approval of appropriate Federal officials exercising policy authority over such 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 Circular A-130, Appendix IV: *Analysis of Key Sections*. Supplemental information is provided in Circular A-130, Appendix III, *Security of Federal Automated Information Resources*.

Nothing in this publication should be taken to contradict the 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. This publication may be used by nongovernmental organizations on a voluntary basis and is not subject to copyright in the United States. Attribution would, however, be appreciated by NIST.

National Institute of Standards and Technology Special Publication 800-101r1
Natl. Inst. Stand. Technol. Spec. Publ. 800-101 Revision 1, 87 pages (May 2014)
http://dx.doi.org/10.6028/NIST.SP. 800-101r1
CODEN: NSPUE2

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 NIST, nor is it intended to imply that the entities, materials, or equipment are necessarily the best available for the purpose.

There may be references in this publication to other publications currently under development by NIST in accordance with its assigned statutory responsibilities. The information in this publication, including concepts and methodologies, may be used by Federal agencies even before the completion of such companion publications. Thus, until each publication is completed, current requirements, guidelines, and procedures, where they exist, remain operative. For planning and transition purposes, Federal agencies may wish to closely follow the development of these new publications by NIST.

Organizations are encouraged to review all draft publications during public comment periods and provide feedback to NIST. All NIST Computer Security Division publications, other than the ones noted above, are available at http://csrc.nist.gov/publications.

visited on 12/9/2016

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 analyses to advance the development and productive use of information technology. ITL's responsibilities include the development of management, administrative, technical, and physical standards and guidelines for the cost-effective security and privacy of other than national security-related information in Federal information systems. The Special Publication 800-series reports on ITL's research, guidelines, and outreach efforts in information system security, and its collaborative activities with industry, government, and academic organizations.

Abstract

Mobile device forensics is the science of recovering digital evidence from a mobile device under forensically sound conditions using accepted methods. Mobile device forensics is an evolving specialty in the field of digital forensics. This guide attempts to bridge the gap by providing an in-depth look into mobile devices and explaining technologies involved and their relationship to forensic procedures. This document covers mobile devices with features beyond simple voice communication and text messaging capabilities. This guide also discusses procedures for the validation, preservation, acquisition, examination, analysis, and reporting of digital information.

Keywords

cell phone forensics; forensic tools; mobile devices; mobile device forensics; mobile device tools; smart phones

visited on 12/9/2016

Acknowledgements

The authors, Rick Ayers from NIST, Sam Brothers from U.S. Customs and Border Protection and Wayne Jansen from Booz-Allen-Hamilton, wish to thank colleagues who reviewed drafts of this document. In particular, our appreciation goes to Barbara Guttman from NIST and Simson Garfinkle from the Naval Postgraduate School for their technical support and written contributions to this document.

Our appreciation also goes out to Bob Elder from TeelTech Canada, Gary Kessler from Gary Kessler Associates, Rick Mislan from Rochester Institute of Technology and Daren Melson for their assistance on technical issues that arose in our work. The authors would also like to thank all others who assisted with our review process.

visited on 12/9/2016

Table of Contents

TABLE OF CONTENTS V
LIST OF FIGURES VII
LIST OF TABLES VIII
EXECUTIVE SUMMARY 1
1. INTRODUCTION 1
1.1 PURPOSE AND SCOPE 1
1.2 AUDIENCE AND ASSUMPTIONS 1
1.3 DOCUMENT STRUCTURE 1
2. BACKGROUND 3
2.1 MOBILE DEVICE CHARACTERISTICS 3
2.2 MEMORY CONSIDERATIONS 5
2.3 IDENTITY MODULE CHARACTERISTICS 7
2.4 CELLULAR NETWORK CHARACTERISTICS 10
2.5 OTHER COMMUNICATIONS SYSTEMS 12
3. FORENSIC TOOLS 15
3.1 MOBILE DEVICE TOOL CLASSIFICATION SYSTEM 15
3.2 UICC TOOLS 23
3.3 OBSTRUCTED DEVICES 24
3.4 FORENSIC TOOL CAPABILITIES 25
4. PRESERVATION 27
4.1 SECURING AND EVALUATING THE SCENE 27
4.2 DOCUMENTING THE SCENE 28
4.3 ISOLATION 28
4.4 PACKAGING, TRANSPORTING, AND STORING EVIDENCE 33
4.5 ON-SITE TRIAGE PROCESSING 33
4.6 GENERIC ON-SITE DECISION TREE 35
5. ACQUISITION 37
5.1 MOBILE DEVICE IDENTIFICATION 37
5.2 TOOL SELECTION AND EXPECTATIONS 39
5.3 MOBILE DEVICE MEMORY ACQUISITION 40
5.4 TANGENTIAL EQUIPMENT 45
5.5 CLOUD BASED SERVICES FOR MOBILE DEVICES 46
6. EXAMINATION AND ANALYSIS 48
6.1 POTENTIAL EVIDENCE 48
6.2 APPLYING MOBILE DEVICE FORENSIC TOOLS 50
6.3 CALL AND SUBSCRIBER RECORDS 52

visited on 12/9/2016

7. REPORTING 55
8. REFERENCES 58
8.1 BIBLIOGRAPHIC CITATIONS 58
8.2 FOOTNOTED URLS 62
APPENDIX A. ACRONYMS 64
APPENDIX B. GLOSSARY 67
APPENDIX C. STANDARDIZED CALL RECORDS 72
APPENDIX D. ONLINE RESOURCES FOR MOBILE DEVICE FORENSICS 75

visited on 12/9/2016

List of Figures

Figure 1: Memory Configurations 6

Figure 2: SIM Card Size Formats [Orm09] 8

Figure 3: SIM File System (GSM) 9

Figure 4: Cellular Network Organization..... 12

Figure 5: Satellite Phone Network..... 13

Figure 6: Mobile Device Tool Classification System..... 17

Figure 7: Generic Triage Decision Tree 36

visited on 12/9/2016

List of Tables

Table 1: Hardware Characterization 4

Table 2: Software Characterization 5

Table 3: Mobile Device Forensic Tools 21

Table 4: Memory Cards..... 46

Table 5: Example Record Structure..... 72

Table 6: Technical Resource Sites..... 75

Table 7: Databases for Identification Queries..... 75

visited on 12/9/2016

Executive Summary

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 devices are commonplace in today's society, used by many individuals for both personal and professional purposes. Mobile devices vary in design and are continually undergoing change as existing technologies improve and new technologies are introduced. When a mobile device is encountered during an investigation, many questions arise: What is the best method to preserve the evidence? How should the device be handled? How should valuable or potentially relevant data contained on the device be extracted? The key to answering these questions begins with a firm understanding of the hardware and software characteristics of mobile devices. This guide discusses procedures for the preservation, acquisition, examination, analysis, and reporting of digital evidence. The issue of ever increasing backlogs for most digital forensics labs is addressed and guidance is provided on handling on-site triage casework.

The objective of the guide is twofold: to help organizations evolve appropriate policies and procedures for dealing with mobile devices and to prepare forensic specialists to conduct forensically sound examinations involving mobile devices. This guide is not all-inclusive nor is it prescribing how law enforcement and incident response communities should handle mobile devices during their investigations or incidents. Specific vendors and mobile forensic acquisition guidance is not specified. However, from the principles outlined and other information provided, organizations should find this guide helpful in establishing their 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 proper technical training and extensive guidance provided by legal advisors, officials, and management. This guide is the first revision to NIST SP800-101. While much of the information provided herein has been carried over from the original guide, the material has been updated and augmented to reflect the current state of the discipline.

visited on 12/9/2016

1. Introduction

1.1 Purpose and Scope

This guide provides basic information on mobile forensics tools and the preservation, acquisition, examination and analysis, and reporting of digital evidence present on mobile devices. This information is relevant to law enforcement, incident response and other types of investigations. This guide focuses mainly on the characteristics of cellular mobile devices, including feature phones, smartphones, and tablets with cellular voice capabilities. It also covers provisions to be taken into consideration during the course of an incident investigation.

This 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 mobile devices and associated electronic media. It is also intended to complement existing guidelines and delve more deeply into issues related to mobile devices and their examination and analysis.

Procedures and techniques presented in this document are a compilation of best practices within the discipline and references have been taken from existing forensic guidelines. This publication is not to be used as a step-by-step guide for executing a proper forensic investigation when dealing with mobile devices nor 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 are applicable.

1.2 Audience and Assumptions

The intended audience is varied and ranges from forensic examiners to response team members handling a computer security incident to organizational security officials investigating an employee-related incident. The practices recommended in this guide are designed to highlight key technical principles associated with the handling and examination of mobile devices. Readers are assumed to have a basic understanding of traditional digital forensic methodologies and capabilities involving stand-alone computers. Due to the changing nature of mobile devices and their related forensic procedures and tools, readers are expected to be aware of and employ additional resources for the most current information.

1.3 Document Structure

The guide is divided into the following chapters and appendices:

- Chapter 1 explains the authority, purpose and scope, audience and assumptions of the document and outlines its structure.
- Chapter 2 provides a background on mobile device characteristics, the internal memory of mobile devices, and characteristics of identity modules and cellular networks.

visited on 12/9/2016

- Chapter 3 discusses the mobile device forensic tool classification system, methods for handling obstructed devices and the capabilities of forensic tools.
- Chapter 4 discusses considerations for preserving digital evidence associated with mobile devices and techniques for preventing network communication.
- Chapter 5 examines the process of mobile device and identity module data acquisition, tangential equipment and cloud-based services for mobile devices.
- Chapter 6 outlines the examination and analysis process, common sources of evidence extracted from mobile devices and identity modules, features and capabilities of tools for examination and call/subscriber records.
- Chapter 7 discusses an overview of report creation and the reporting of findings.
- Chapter 8 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 provides an example of the structure of call records maintained by cell phone carriers.
- Appendix D provides links to online resources.

visited on 12/9/2016

2. Background

This chapter gives an overview of the hardware and software capabilities of mobile devices and their associated cellular networks. The overview provides a summary of general characteristics and, where useful, focuses on key features relevant to forensics. Developing an understanding of the components and organization of mobile devices (e.g., memory organization and its use) is a prerequisite to understanding the intricacies involved when dealing with them forensically. For example, mobile device memory that contains user data may be volatile (i.e., DRAM/SRAM) and require continuous power to maintain content similar to RAM in a personal computer. Similarly, features of cellular networks are an important aspect of mobile device forensics, since logs of usage, geographic location, and other data are maintained. Mobile device technologies and cellular networks are rapidly changing, with new technologies, products, and features being introduced regularly. Because of the fast pace with which mobile device technologies are evolving, this discussion captures a snapshot of the mobile device discipline at the present time.

2.1 Mobile Device Characteristics

Mobile devices perform an array of functions ranging from a simple telephony device to those of a personal computer. Designed for mobility, they are compact in size, battery-powered, and lightweight. Most mobile devices 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 a mobile device may be stored in either NAND or NOR memory while code execution typically occurs in RAM.

Currently, mobile devices are equipped with system-level microprocessors that reduce the number of supporting chips required and include considerable internal memory capacity currently up to 64GB (e.g., Stacked NAND). Built-in Secure Digital (SD) memory card slots, such as one for the micro Secure Digital eXtended Capacity (microSDXC), may support removable memory with capacities ranging from 64GB to 2TB of storage. Non-cellular wireless communications such as infrared (i.e., IrDA), Bluetooth, Near Field Communication (NFC), and WiFi may also be built into the device and support synchronization protocols to exchange other data (e.g., graphics, audio, and video file formats).

Different mobile devices have different technical and physical characteristics (e.g., size, weight, processor speed, memory capacity). Mobile devices may also use different types of expansion capabilities to provide additional functionality. Furthermore, mobile device capabilities sometimes include those of other devices such as handheld Global Positioning Systems (GPS), cameras (still and video) or personal computers. Overall, mobile devices can be classified as feature phones that are primarily simple voice and messaging communication devices or smartphones that offer more advanced capabilities and services for multimedia, similar to those of a personal computer. Table 1 highlights the general hardware characteristics of feature and smartphone models, which underscore this diversity.

The classification scheme is illustrative and intended to give a sense of the range of hardware characteristics currently in the marketplace. Over time, characteristics found in smartphones tend to appear in feature phones as new technology is introduced to smartphones. Though the

visited on 12/9/2016

lines of delineation are somewhat fuzzy and dynamic, the classification scheme nevertheless serves as a general guide.

Table 1: Hardware Characterization

	Feature Phone	**Smartphone**
Processor	Limited speed (~52Mhz)	Superior speed (~1GHz dual-core)
Memory	Limited capacity (~5MB)	Superior capacity (~128GB)
Display	Small size color, 4k – 260k (12-bit to 18-bit)	Large size color, 16.7 million (~24-bit)
Card Slots	None, MicroSD	MicroSDXC
Camera	Still, Video	Still, Panoramic, and Video (HD)
Text Input	Numeric Keypad, QWERTY-style keyboard	Touch Screen, Handwriting Recognition, QWERTY-style keyboard
Voice Input	None	Voice Recognition (Dialing and Control)
Cell Interface	Voice and Limited Data	Voice and High Speed Data (4G LTE)
Positioning	None, GPS receiver	GPS receiver
Wireless	IrDA, Bluetooth	Bluetooth, WiFi, and NFC
Battery	Fixed/Removable, Rechargeable Li-Ion Polymer	Fixed/Removable, Rechargeable Li-Ion Polymer

Both feature phones and smartphones support voice, text messaging, and a set of basic Personal Information Management (PIM) type applications including phonebook and calendar facilities. Smartphones add PC-like capability for running a wide variety of general and special-purpose applications. Smartphones are typically larger than feature phones, support higher video resolutions (e.g., ~300 PPI) and may have an integrated QWERTY keyboard or touch sensitive screen. Smartphones generally support a wide array of applications, available through an application storefront. Table 2 lists the differences in software capabilities found on these device classes.

visited on 12/9/2016

Table 2: Software Characterization

	Feature Phone	Smartphone
OS	Closed	Android, BlackBerry OS, iOS, Symbian, WebOS and Windows Phone
PIM (Personal Information Management)	Phonebook, Calendar and Reminder List	Enhanced Phonebook, Calendar and Reminder List
Applications	Minimal (e.g., games, notepad)	Applications (e.g., games, office productivity and social media)
Call	Voice	Voice, Video
Messaging	Text Messaging, MMS	Text, Enhanced Text, Full Multimedia Messaging
Chat	Instant Messaging	Enhanced Instant Messaging
Email	Via text messaging	Via POP or IMAP Server
Web	Via WAP Gateway	Direct HTTP

Feature phones typically use a closed operating system with no published documentation. A number of companies specializing in embedded software also offer real-time operating system solutions for manufacturers of mobile devices. Smartphones generally use either a proprietary or an open source operating system. Nearly all smartphones use one of the following operating systems: Android, BlackBerry OS, iOS, Symbian, WebOS or Windows Phone. Unlike the more limited kernels in feature phones, these operating systems are multi-tasking and full-featured, designed specifically to match the capabilities of high-end mobile devices. Many smartphone operating systems manufacturers offer a Software Development Kit (SDK) (e.g., the Android[1] or iOS[2] SDKs).

2.2 Memory Considerations

Mobile devices contain both non-volatile and volatile memory. Volatile memory (i.e., RAM) is used for dynamic storage and its contents are lost when power is drained from the mobile device. Non-volatile memory is persistent as its contents are not affected by loss of power or overwriting data upon reboot. For example, solid-state drives (SSD) that stores persistent data on solid-state flash memory.

Mobile devices typically contain one or two different types of non-volatile flash memory. These types are NAND and NOR. NOR flash has faster read times, slower write times than NAND and is nearly immune to corruption and bad blocks while allowing random access to any memory location. NAND flash offers higher memory storage capacities, is less stable and only allows sequential access.

[1] For more information, visit: http://developer.android.com/sdk/index.html

[2] For more information, visit: https://developer.apple.com/devcenter/ios/index.action

visited on 12/9/2016

Memory configurations among mobile devices have evolved over time. Feature phones were among the first types of devices that contained NOR flash and RAM memory. System and user data are stored in NOR and copied to RAM upon booting for faster code execution and access. This is known as the first generation of mobile device memory configurations.

As smartphones were introduced, memory configurations evolved, adding NAND flash memory. This arrangement of NOR, NAND and RAM memory is referred to as the second generation. This generation of memory configurations stores system files in NOR flash, user files in NAND and RAM is used for code execution.

The latest smartphones contain only NAND and RAM memory (i.e., third generation), due to requirements for higher transaction speed, greater storage density and lower cost. To facilitate the lack of space on mobile device mainboards and the demand for higher density storage space (i.e., 2GB – 128GB) the new Embedded MultiMedia Cards (eMMC) style chips are present in many of today's smartphones.

Figure 1 illustrates the various memory configurations contained across all mobile devices.

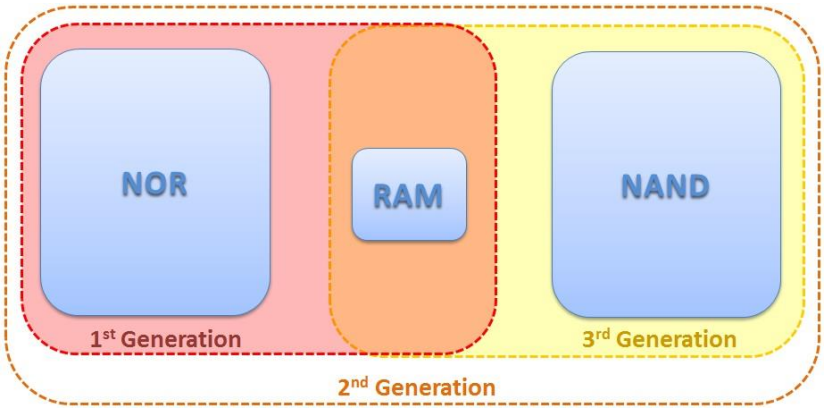


Figure 1: Memory Configurations

RAM is the most difficult to capture accurately due to its volatile nature. Since RAM is typically used for program execution, information may be of value to the examiner (e.g., configuration files, passwords, etc.). Mobile device RAM capture tools are just beginning to become available.

NOR flash memory includes system data such as: operating system code, the kernel, device drivers, system libraries, memory for executing operating system applications and the storage of user application execution instructions. NOR flash will be the best location for data collection for first generation memory configuration devices.

NAND flash memory contains: PIM data, graphics, audio, video, and other user files. This type of memory generally provides the examiner with the most useful information in most cases. NAND flash memory may leave multiple copies of transaction-based files (e.g., databases and logs) due to wear leveling algorithms and garbage collection routines. Since NAND flash memory cells can be re-used for only a limited amount of time before they become unreliable, wear leveling algorithms are used to increase the life span of Flash memory storage, by arranging data so that erasures and re-writes are distributed evenly across the SSD.

visited on 12/9/2016

Garbage collection occurs because NAND flash memory cannot overwrite existing data, the data must first be erased before writing to the same cell [Bel10].

2.3 Identity Module Characteristics

Identity modules (commonly known as SIM cards) are synonymous with mobile devices that interoperate with GSM cellular networks. Under the GSM framework, a mobile device is referred to as a Mobile Station and is partitioned into two distinct components: the Universal Integrated Circuit Card (UICC) and the Mobile Equipment (ME). A UICC, commonly referred to as an identity module (e.g., Subscriber Identity Module [SIM], Universal Subscriber Identity Module [USIM], CDMA Subscriber Identity Module [CSIM]), is a removable component that contains essential information about the subscriber. The ME and the radio handset portion cannot fully function without a UICC. The UICC's main purpose entails authenticating the user of the mobile device to the network providing access to subscribed services. The UICC also offers storage for personal information, such as phonebook entries, text messages, last numbers dialed (LND) and service-related information.

The UICC partitioning of a mobile device stipulated in the GSM standards has brought about a form of portability. Moving a UICC between compatible mobile devices automatically transfers the subscriber's identity and some of the associated information (e.g., SMS messages and contacts) and capabilities. In contrast, 2G and 3G CDMA mobile devices generally do not contain a UICC card. Analogous UICC functionality is instead directly incorporated within the device. However, newer CDMA (i.e., 4G/LTE) devices may employ a CDMA Subscriber Identity Module (CSIM) application running on a UICC.

A UICC can contain up to three applications: SIM, USIM and CSIM. UICCs used in GSM and UMTS mobile devices use the SIM and UMTS SIM (USIM) applications, while CDMA devices use the CSIM application. A UICC with all three applications provides users with additional portability through the removal of the UICC from one mobile device and insertion into another. Because the SIM application was originally synonymous with the physical card itself, the term SIM is often used to refer to the physical card in lieu of UICC. Similarly the terms USIM and CSIM can refer to both the physical card as well as the respective applications supported on the UICC.

At its core, a UICC 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 UICC's file system resides in persistent memory and stores data such as: as phonebook entries, text messages, last numbers dialed (LND) and service-related information. Depending on the mobile device used, some information managed by applications on the UICC may coexist in the memory of the mobile device. Information may also reside entirely in the memory of the mobile device instead of available memory reserved for it in the file system of the UICC.

The UICC operating system controls access to elements of the file system [3GP07]. Actions such as reading or updating may be permitted or denied unconditionally, or allowed conditionally with certain access rights, depending on the application. Rights are assigned to a subscriber through 4-8 digit Personal Identification Number (PIN) codes. PINs protect core subscriber-related data and certain optional data.

visited on 12/9/2016

A preset number of attempts (usually three) are allowed for providing the correct PIN code to the UICC before further attempts are blocked completely, rendering communications inoperative. Only by providing a correct PIN Unblocking Key (PUK) may the value of a PIN and its counter be reset on the UICC. If the number of attempts to enter the correct PUK value exceeds a set limit, normally ten, the card becomes blocked permanently. The PUK for a UICC may be obtained from the service provider or network operator by providing the identifier of the UICC (i.e., Integrated Circuit Chip Identifier or ICCID). The ICCID is normally imprinted on the front of UICC, but may also be read from an element of the file system.

UICCs are available in three different size formats. They are: Mini SIM (2FF), Micro SIM (3FF), and Nano SIM (4FF). The Mini SIM with a width of 25 mm, a height of 15 mm, and a thickness of .76 mm, is roughly the footprint of a postage stamp and is currently the most common format used worldwide. Micro (12mm x 15mm x .76mm) and Nano (8.8mm x 12.3mm x .67mm) SIMs are found in newer mobile devices (e.g., iPhone 5 uses the 4FF).

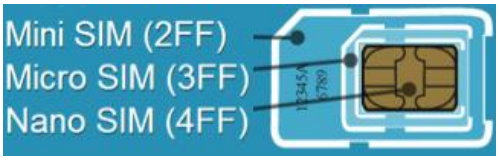


Figure 2: SIM Card Size Formats [Orm09]

Though similar in dimension to a miniSD removable memory card, UICCs follow a different set of specifications with vastly different characteristics. For example, their pin connectors are not aligned along the bottom edge as with removable media cards, but instead form a contact pad integral to the smart card chip, which is embedded in a plastic frame, as shown in Figure 2. UICCs also employ a broad range of tamper resistance techniques to protect the information they contain.

The slot for the UICC card is normally not accessible from the exterior of the mobile device to protect insertion and removal as with a memory card. Instead, it typically is found beneath the battery compartment. When a UICC is inserted into a mobile device handset and pin contact is made, a serial interface is used for communicating between them.

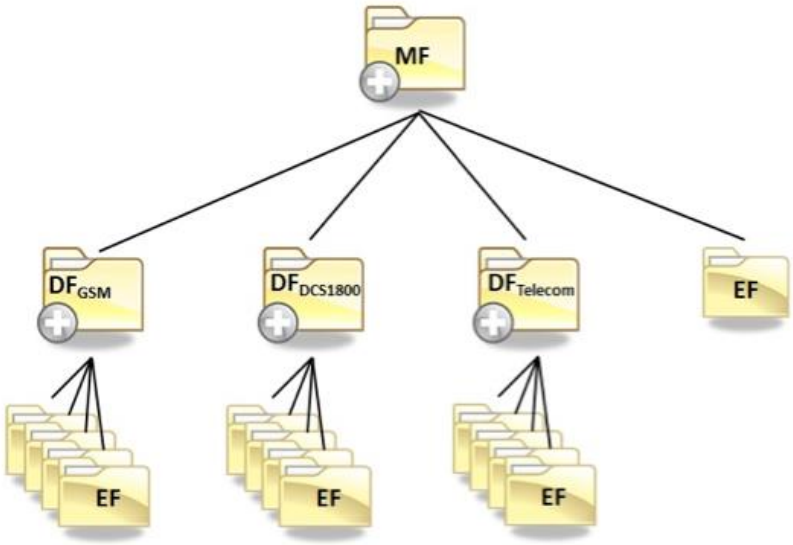
In most cases, the UICC should be removed from the handset first and read using a Personal Computer/Smart Card (PC/SC) reader. Removal of the UICC provides the examiner with ability to read additional data that may be recovered (e.g., deleted text messages).

Authenticating a device to a network securely is a vital function performed via the UICC. 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 UICC and gain access to a subscriber's services. Cryptographic key information in the UICC also supports stream cipher encryption to protect against eavesdropping on the air interface.

A UICC is similar to a mobile device as it has both volatile and non-volatile memory that may contain the same general categories of data as found in a mobile device. It can be thought of as a trusted sub-processor that interfaces to a device and draws power from it. The file system resides in the non-volatile memory of a UICC and is organized as a hierarchical tree structure.

visited on 12/9/2016

For example, the SIM applications file system is composed of three types of elements: the root of the file system (MF), subordinate directory files (DF), and files containing elementary data (EF). Figure 3 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.



MF - Master File (root and main container of DF and EF)
DF - Directory File
EF - Elementary File

Figure 3: SIM File System (GSM)

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

- Service-related Information including unique identifiers for the UICC, the Integrated Circuit Card Identification (ICCID) and the International Mobile Subscriber Identity (IMSI)

- Phonebook and call information known respectively as the Abbreviated Dialing Numbers (ADN) and Last Numbers Dialed (LND)

- Messaging information including both Short Message Service (SMS) text messages and Enhanced Messaging Service (EMS) simple multimedia messages

- The USIM application supports the storage of links to incoming (EFICI) and outgoing (EFOCI) calls. The EFICI and EFOCI are each stored using two bytes. The first byte

visited on 12/9/2016

points to a specific phone book and the second points to an abbreviated dialing number (EFADN) entry[3]

- Location information including Location Area Information (LAI) for voice communications and Routing Area Information (RAI) for data communications.

2.4 Cellular Network Characteristics

Within the U.S., different types of digital cellular networks follow distinct incompatible sets of standards. The following sections discuss digital cellular networks, Mobile IP and satellite phones.

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 exists.

CDMA refers to a technology designed by Qualcomm in the U.S., which employs spread spectrum communications for the radio link.[4] 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 was CDMA2000. CDMA2000 is backward compatible with its previous 2G iteration IS-95 (cdmaOne). The successor to CDMA2000 is Qualcomm's Long Term Evolution (LTE). LTE adds faster data transfer capabilities for mobile devices and is commonly referred to as 4G LTE. Verizon and Sprint are common CDMA network carriers in the U.S.

GSM is a cellular system used worldwide that was designed in Europe, primarily by Ericsson and Nokia. AT&T and T-Mobile are common GSM network carriers 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 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. 4G LTE is also available to GSM mobile devices providing higher data transmission rates to its customers.[5]

---

[3] For more information, visit: http://www.3gpp.org/ftp/Specs/html-info/31102.htm

[4] For more information, visit: http://www.qualcomm.com/

[5] For more information, visit: http://www.radio-electronics.com

visited on 12/9/2016

TDMA is also used to refer specifically to the standard covered by IS-136. 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 TDMA cellular networks that follow IS-136. Many mobile forensic tools refer to these devices as iDEN/TDMA phones. Mobile devices operating over the iDEN network often utilize a Push-To-Talk (PTT) function provide subscribers with the ability to communicate with one another over a cellular network in a "walkie-talkie" fashion.

Integrated Digital Enhanced Network (iDEN), a mobile telecommunications technology developed by Motorola provided the benefits of a two-way radio system and a cellular telephone. The iDEN project originally began as MIRS (Motorola Integrated Radio System) in early 1991 and was phased out the summer of 2013 for the US markets although coverage still exists in Mexico and Canada.

Digital AMPS (D-AMPS), IS-54 and IS-136 are 2G mobile phone systems once prevalent within the United States and Canada in the 1990s. Existing networks were mostly replaced by GSM/GPRS or CDMA2000 technologies.

Mobile devices work with certain subsets of the network types mentioned, typically those associated with a service provider from whom the phone was obtained and with whom a service agreement was entered. Mobile devices may also be acquired without service from any manufacturer, vendor, or other source and subsequently have their service set up separately with a service provider or network operator. Mobile devices that are permitted to be provisioned to more than one specific carrier are commonly referred to as "unlocked" as they may be used on a variety of carriers by switching UICC's for GSM mobile devices.

Mobile devices do exist that provide the user with both GSM and CDMA capabilities. Such devices are sometimes referred to as hybrid phones or global phones. These types of mobile devices contain two types of cellular radios for voice and data, providing the ability to operate over either the GSM or CDMA network.

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 device moves from one cell to another, a cellular arrangement requires active connections to be monitored and effectively passed along between cells to maintain the connection. 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 is captured and maintained by the network system.

Despite their differences in technology, cellular networks are organized similarly to one another, in a manner illustrated in Figure 4 [Gib02]. The main components are the radio transceiver equipment that communicates with mobile devices, 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 Node B, representing a Base Transceiver Station (BTS), the Radio Network Controller (RNC), and the Mobile Switching Center (MSC). The RNCs and the Node B units controlled are sometimes collectively referred to as a Radio Access Network (RAN).

visited on 12/9/2016

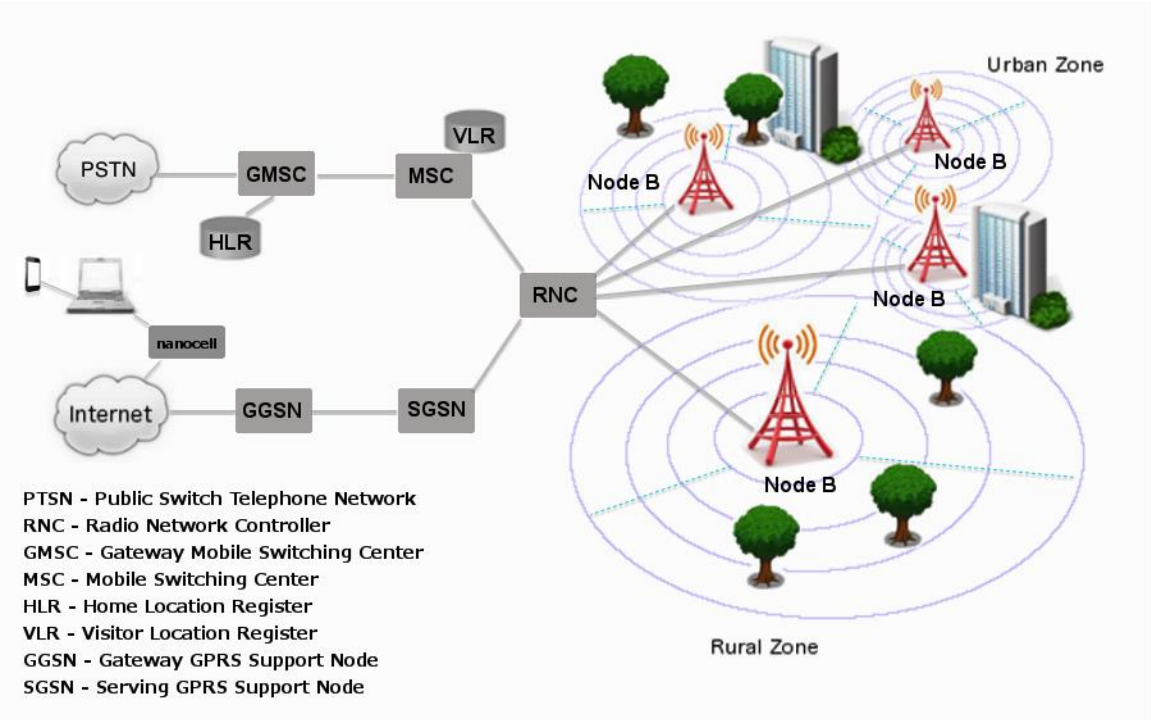


Figure 4: Cellular Network Organization

Each MSC controls a set of RNCs and manages overall communications throughout the cellular network, including registration, authentication, location updating, handovers, and call routing. An MSC interfaces with the public switch telephone network (PSTN) via a Gateway MSC (GMSC). To perform its tasks, an 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 is the Visitor Location Register (VLR), which is used for mobile devices roaming outside of their service area. An SGSN (Serving GPRS Support Node) performs a similar role as that of MSC/VLR, but instead supports General Packet Radio Service (GPRS) (i.e., packet-switched services) to the Internet. Likewise, GGSN (Gateway GPRS Support Node) functionality is close to that of a GMSC, but for packet-switched services.

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 (CDR). The subscriber account data, CDRs, and related technical information obtained from the network carrier are often a valuable source of evidence in an investigation [Con09].

2.5 Other Communications Systems

Mobile IP is an Internet Engineering Task Force (IETF)[6] standard communications protocol that is designed to allow mobile device users to move from one network to another while

[6] For more information, visit: http://www.ietf.org/

visited on 12/9/2016

maintaining a permanent IP address.[7] With the original IP protocol, each time a mobile device moved to a new Internet point of attachment, all active network connections had to be restarted and the device possibly needed to be rebooted. Mobile IP instead allows a mobile user to move about transparently while continuing to use the same IP address (the user's "home address"), avoiding these problems and enabling new mobile applications. Mobile IP was designed to support seamless and continuous Internet connectivity. Mobile IP is most often found in wireless environments where users need to carry their mobile devices across multiple Local Area Network (LAN) subnets. Examples of use are in roaming between overlapping wireless systems e.g., Wireless Local Area Network (WLAN), Worldwide Interoperability for Microwave Access (WiMAX), IP over Digital Video Broadcasting (DVB) and Broadband Wireless Access (BWA).[8]

Individuals requiring communication services from remote locations (e.g., aviation, emergency services, government, military, etc.) are often equipped with satellite phones. Satellite phones are mobile devices that establish connectivity with satellites rather than cellular towers. Typically, satellite phones require a direct line of sight to the satellite without obstruction of objects (e.g., buildings, trees, etc.) impacting the signal strength and quality of the call. Depending on the service, coverage may range from a specific area all the way to the entire earth. For example, the Iridium satellite constellation is made up of 66 Low Earth Orbiting (LEO) satellites with spares, providing worldwide voice and data communications.

Figure 5: Satellite Phone Network

Satellite phones communicate by sending radio signals to a satellite that transmits a signal back down to earth where a station routes the call to the PSTN. In some cases, the satellite phone

[7] For more information, visit http://en.wikipedia.org/wiki/Mobile_IP

[8] For more information, visit http://nislab.bu.edu/sc546/sc441Spring2003/mobileIP

visited on 12/9/2016

provider will transmit from one satellite to another satellite that has a connection to an Earth station. Much like GSM based mobile devices, satellite phones are equipped with a UICC and provide users with a wide variety of features (e.g., contact list, text messaging, voicemail, call forwarding, etc.).

visited on 12/9/2016

3. Forensic Tools

The availability of forensic software tools for mobile devices is considerably different from that of personal computers. While personal computers may differ from mobile devices from a hardware and software perspective, their functionality has become increasingly similar. Although the majority of mobile device operating systems are open source (i.e., Android), feature phone OS's are typically closed. Closed operating systems make interpreting their associated file system and structure difficult. Many mobile devices with the same operating system may also vary widely in their implementation, resulting in a myriad of file system and structure permutations. These permutations create significant challenges for mobile forensic tool manufacturers and examiners.

The types of software available for mobile device examination include commercial and open source forensic tools, as well as non-forensic tools intended for device management, testing, and diagnostics. Forensic tools are typically designed to acquire data from the internal memory of handsets and UICCs without altering their content and to calculate integrity hashes for the acquired data. Both forensic and non-forensic software tools often use the same protocols and techniques to communicate with a device. However, non-forensic tools may allow unrestricted two-way flow of information and omit data integrity hash functions. Mobile device examiners typically assemble a collection of both forensic and non-forensic tools for their toolkit. The range of devices over which they operate is typically narrowed to: distinct platforms, a specific operating system family or even a single type of hardware architecture. Short product release cycles are the norm for mobile devices, requiring tool manufacturers to continually update their tools providing forensics examiners with an forensic solution. The task is formidable and tool manufacturers' support for newer models may lag significantly behind the introduction of a device into the marketplace. Models of older functioning mobile devices, though out of date, can remain in use for years after their initial release. Mobile device models introduced into one national market may also be used in areas by exchanging the UICC of one cellular carrier with that from another carrier. The current state is likely to continue, keeping the cost of examination significantly higher than if a few standard operating systems and hardware configurations prevailed.

3.1 Mobile Device Tool Classification System

Understanding the various types of mobile acquisition tools and the data they are capable of recovering is important for a mobile forensic examiner. The classification system used in this section provides a framework for forensic examiners to compare the extraction methods used by different tools to acquire data. The objective of the tool classification system is to enable an examiner to easily classify and compare the extraction method of different tools. The tool classification system is displayed in Figure 6 [Bro08]. As the pyramid is traversed from the bottom, Level 1, to the top, Level 5, the methodologies involved in acquisition become more technical, invasive, time consuming, and expensive.

Level 1, Manual Extraction methods involve recording information brought up on a mobile device screen when employing the user interface. Level 2, Logical Extraction methods are used most frequently at this time and are mildly technical, requiring beginner-level training. Methods for levels 3 to 5 entail extracting and recording a copy or image of a physical store (e.g., a memory chip), compared to the logical acquisitions used at level 2 involve capturing a copy of logical storage objects (e.g., directories and files) that reside on a logical store (e.g., a

visited on 12/9/2016

file system partition). Level 3, Hex Dumping/JTAG Extraction methods, entail performing a "physical acquisition" of mobile device memory in situ and require advanced training. Level 4 Chip-Off methods involve the physical removal of memory from a mobile device to extract data, requiring extensive training in electronic engineering and file system forensics. Level 5, Micro Read methods involve the use of a high-powered microscope to view the physical state of gates. Level 5 methods are the most invasive, sophisticated, technical, expensive, and time consuming of all the methodologies.

There are pros and cons to performing extraction types at each layer. For example, hex dumping allows deleted objects and any data remnants present to be examined (e.g., in unallocated memory or file system space), which otherwise would be inaccessible through the use of logical acquisition methods. However, the extracted device images require parsing, decryption and decoding. Logical acquisition methods, though more limited than Hex Dumping/JTAG methods, have the advantage in that the system data structures are at a higher level of abstraction and are normally easier for a tool to extract and render. These differences are due to the underlying distinction between memory as seen by a process via the operating system facilities (i.e., a logical view), versus memory as seen in raw form by the processor or another hardware component (i.e., a physical view). Based upon a wide variety of circumstances (e.g., type of data needed, time available, urgency, available tools, etc.), an examiner may select a specific level to begin their examination. It is important to note that once a level is used, alternate levels may not be possible. For example, after performing chip-off (level 4) lower level tools may not be physically possible. Forensic examiners should be aware of such issues and perform the appropriate level of extraction commensurate with their training and experience. With each methodology, data may be permanently destroyed or modified if a given tool or procedure is not proper utilized. The risk of alteration and destruction increases in tandem with the levels. Thus, proper training and mentoring is critical in obtaining the highest success rate for data extraction and analysis of the data contained within mobile devices.

visited on 12/9/2016

Figure 6: Mobile Device Tool Classification System

The following discussion provides a more detailed description of each level and the methods used for data extraction.

- **Manual Extraction** – A manual extraction method involves viewing the data content stored on a mobile device. The content displayed on the LCD screen requires the manual manipulation of the buttons, keyboard or touchscreen to view the contents of the mobile device. Information discovered may be recorded using an external digital camera. At this level, it is impossible to recover deleted information. Some tools have been developed to provide the forensic examiner with the ability to document and categorize the information recorded more quickly. Nevertheless, if there is a large amount of data to be captured, a manual extraction can be very time consuming and the data on the device may be inadvertently modified, deleted or overwritten as a result of the examination. Manual extractions become increasingly difficult and perhaps unachievable when encountering a broken/missing LCD screen or a damaged/missing keyboard interface. Additional challenges occur when the device is configured to display a language unknown to the investigator; this may cause difficulty in successful menu navigation.

- **Logical Extraction** – Connectivity between a mobile device and the forensics workstation is achieved with a connection using either a wired (e.g., USB or RS-232) or wireless (e.g., IrDA, WiFi, or Bluetooth) connection. The examiner should be aware of the issues associated when selecting a specific connectivity method, as different connection types and associated protocols may result in data being modified (e.g., unread SMS) or different amounts or types of data being extracted. Logical extraction tools begin by sending a series of commands over the established interface from the computer to the mobile device. The mobile device responds based upon the command request. The response (mobile device data) is sent back to the workstation and presented to the forensics examiner for reporting purposes.

- **Hex Dumping and JTAG** – Hex Dumping and Joint Test Action Group (JTAG) extraction methods afford the forensic examiner more direct access to the raw

visited on 12/9/2016

information stored in flash memory. One challenge with these extraction methods is the ability of a given tool to parse and decode the captured data. Providing the forensic examiner with a logical view of the file system, and reporting on other data remnants outside the file system that may be present are challenging. For example, all data contained within a given flash memory chip may not be acquired, as many tools, such as flasher boxes, may only be able to extract specific sections of memory [Bre07]. Methods used at this level require connectivity (e.g., cable or WiFi) between the mobile device and the forensic workstation.

Hex Dumping – this technique is the more commonly used method by tools at this level. This involves uploading a modified boot loader (or other software) into a protected area of memory (e.g., RAM) on the device. This upload process is accomplished by connecting the mobile device's data port to a flasher box and the flasher box is in turn connected to the forensic workstation. A series of commands is sent from the flasher box to the mobile device to place it in a diagnostic mode. Once in diagnostic mode, the flasher box captures all (or sections) of flash memory and sends it to the forensic workstation over the same communications link used for the upload. Some flasher boxes work this way or they may use a proprietary interface for memory extractions. Rare cases exist where extractions can be accomplished using WiFi (i.e., early Jonathan Zdziarski (JZ) Methods) [Zdz12].

JTAG – Many manufacturers support the JTAG standard, which defines a common test interface for processor, memory, and other semiconductor chips. Forensic examiners can communicate with a JTAG-compliant component by utilizing special purpose standalone programmer devices to probe defined test points [Wil05]. The JTAG testing unit can be used to request memory addresses from the JTAG-compliant component and accept the response for storage and rendition [Bre06]. JTAG gives specialists another avenue for imaging devices that are locked or devices that may have minor damage and cannot be properly interfaced otherwise. This method involves attaching a cable (or wiring harness) from a workstation to the mobile device's JTAG interface and access memory via the device's microprocessor to produce an image [Bre07]. JTAG extractions differ mainly from Hex Dumping in that it is invasive as access to the connections frequently require that the examiner dismantle some (or most) of a mobile device to obtain access to establish the wiring connections.

Flasher boxes are small devices originally designed with the intent to service or upgrade mobile devices. Physical acquisitions frequently require the use of a flasher box to facilitate the extraction of data from a mobile device. The flasher box aides the examiner by communicating with the mobile device using diagnostic protocols to communicate with the memory chip. This communication may utilize the mobile device's operating system or may bypass it altogether and communicate directly to the chip [Jon10]. Flasher boxes are often accompanied by software to facilitate the data extraction process working in conjunction with the hardware. Many flasher box software packages provide the added functionality of recovering passwords from mobile device memory as well in some configurations. Although acquisition methods differ between flasher boxes, a general process is used [Bre07]. Limitations of the use of flasher boxes include the following:

visited on 12/9/2016

- Rebooting of the mobile device is frequently required to begin the extraction process; this may cause authentication mechanisms to activate preventing further analysis.

- Many flasher boxes recover the data in an encrypted format requiring the examiner to either use the software provided by the flasher box manufacturer to decrypt the data or may require reverse engineering the data's encryption scheme by the analyst.

- Many phone models do not provide the acquisition of the entire memory range within a given mobile device. Only certain ranges may be available for certain mobile devices

- The flasher box service software often has many buttons that are labeled with nearly identical names. This confusion may easily lead even an experienced examiner to press the wrong button, erasing the contents of the mobile device instead of dumping the memory.

- Lack of documentation on the use of the flasher box tools is common. Extraction methods are frequently shared on forums supported by the vendor and moderated by more seasoned users. Caution should be taken when advice is provided, as not all the information provided is correct.

- Forensic Use: Nearly all flasher boxes were not designed with a forensic use as its intended purpose. Examiners must be experienced in the use of flasher boxes and should understand the proper use and function of flasher boxes.

- Despite all of these limitations, use of a flasher box is a viable option for many forensics cases. Proper training, experience and understating of how the tools work are the keys to success.

A wide range of technical expertise and proper training is required for extracting and analyzing binary images with these methods, including locating and connecting to JTAG ports, creating customized boot loaders and recreating file systems.

- **Chip-Off** – Chip-Off methods refer to the acquisition of data directly from a mobile device's flash memory. This extraction requires the physical removal of flash memory. Chip-Off provides examiners with the ability to create a binary image of the removed chip. In order to provide the examiner with data in a contiguous binary format file, the wear-leveling algorithm must be reverse engineered. Once complete, the binary image may then be analyzed. This type of acquisition is most closely related to physical imaging a hard disk drive as in traditional digital forensics. Extensive training is required in order to successfully perform extractions at this level. Chip-Off extractions are challenging based on a wide variety of chip types, a myriad of raw data formats, and the risk of causing physical damage to the chip during the extraction process. Due to the complexities related to Chip-Off, JTAG extraction is more common.

- **Micro Read** – A Micro Read involves recording the physical observation of the gates on a NAND or NOR chip with the use of an electron microscope. Due to the extreme technicalities involved when performing a Micro Read, this level of acquisition would

visited on 12/9/2016

only be attempted for high profile cases equivalent to a national security crisis after all other acquisition techniques have been exhausted. Successful acquisition at this level would require a team of experts, proper equipment, time and in-depth knowledge of proprietary information. There are no known U.S. Law Enforcement agencies performing acquisitions at this level. Currently, there are no commercially available Micro Read tools.

Table 3 provides a classification of some tools currently used in mobile device investigations, and identifies the facilities they provide: acquisition, examination, or reporting. Additional tools do exist, but only those familiar to the authors are discussed. For a more complete an up to date list of forensic tools refer to: NIST Tool Taxonomy (http://www.cftt.nist.gov/tool_catalog/populated_taxonomy/). The tools listed in Table 3 are grouped by level starting with Level 1 (Manual Extraction) through Level 4 (Chip-Off).

The following describes each of the headings contained within Table 3:

- **Tool** – tool name
  - † Denotes a tool that supports the logical acquisition of a UICC
  - ‡ Denotes a tool that supports the logical acquisition of a UICC and the creation of a Cellular Network Isolation Card (CNIC)
- **Acquisition Level** – level(s) at which the tool performs data extractions: 1- Manual extraction, 2 - Logical extraction, 3 - Physical extraction, 4 - Chip-off, 5 - Micro Read
- **Network Type** – acquisition of devices operating over specified networks
- **Forensic Tool** – is the tool specifically designed for forensic acquisition
- **Examination/Analysis** – provides the examiner with the ability to perform examination or analysis of acquired data
- **Reporting** – provides the examiner with the ability to generate reports
- **3rd Party Tool Image Analysis (3PIA)** – supports importing of raw data produced from another manufacturer's tool
- **Chinese Chipset Support (CCS)** – mobile devices containing Chinese chipsets are increasing as they continue to flood the international market. Some mobile forensic tools provide either a logical and/or physical extraction solution.
- **Cables/Hardware Available (C/HW)** – cables are provided

visited on 12/9/2016

Table 3: Mobile Device Forensic Tools

Tool	Acquisition Level	Network Type			Forensic Tool	Exam/Analysis	Reports	MISC	
		GSM	CDMA	iDEN/TDMA					
ART	1	✓	✓	✓	✓	N/A	✓	N/A	Current tool list available at: http://www.cftt.nist.gov/tool_catalog/populated_taxonomy/
Eclipse	1	✓	✓	✓	✓	N/A	✓	N/A	
Project-A-Phone	1	✓	✓	✓	✓	N/A	✓	N/A	
STE3000 FAV	1	✓	✓	✓	✓	N/A	✓	N/A	
ZRT2	1	✓	✓	✓	✓	N/A	✓	N/A	
Aceso†	2	✓	✓	×	✓	✓	✓	C/HW	
Athena†	2	✓	✓	×	✓	✓	✓	C/HW	
BitPIM	2	×	✓	×	✓[9]	×	×	×	
CPA SIM Analyzer[10]‡	2	✓	×	×	✓	✓	✓	C/HW	
FinalMobile Forensics	2	×	✓	×	✓	✓	✓	3PIA	
iXAM[9]	2	✓	✓	×	✓	✓	✓	N/A	
BlackLight	2	✓	✓	×	✓	✓	✓	3PIA	
MOBILedit! Forensic‡	2	✓	✓	×	✓	✓	✓	C/HW	
Oxygen Forensic Suite (Analyst)	2	✓	✓	×	✓	✓	✓	CCS	
SD iPhone Recovery[12]	2	✓	✓	×	×	✓	✓	N/A	
SecureView†	2	✓	✓	✓	✓	✓	✓	3PIA, C/HW	
SIMIS†	2	✓	✓	×	✓	✓	✓	C/HW	

[9] When Read-Only mode is activated

[10] This tool only performs a logical extraction and analysis of UICCs.

visited on 12/9/2016

Tool	Acquisition Level	Network Type			Forensic Tool	Exam/Analysis	Reports	MISC
		GSM	CDMA	iDEN/TDMA				
SIMCon†	2	✓	×	×	✓	✓	✓	C/HW
SIMiFOR‡	2	✓	×	×	✓	✓	✓	C/HW
UFED Classic Logical‡	2	✓	✓	✓	✓	✓	✓	C/HW
UFED Touch Logical‡	2	✓	✓	✓	✓	✓	✓	C/HW
USIM Detective†	2	✓	×	×	✓	✓	✓	C/HW
WinMoFo	2	✓	✓	✓	✓	✓	✓	×
XRY Logical‡	2	✓	✓	✓	✓	✓	✓	C/HW
Zdziarski Method[11]	2	✓	✓	×	✓	×	×	N/A
CellXtract†	2/3	✓	✓	×	✓	✓	✓	C/HW
CellXtract TNT†	2/3	✓	✓	×	✓	✓	✓	CCS, C/HW
Device Seizure‡	2/3	✓	✓	✓	✓	✓	✓	3PIA, C/HW
EnCase Smartphone Examiner†	2/3	✓	✓	×	✓	✓	✓	3PIA, C/HW
Lantern	2/3	✓	✓	×	✓	✓	✓	3PIA
MPE+‡	2/3	✓	✓	✓	✓	✓	✓	3PIA, CCS, C/HW
Tarantula	2/3	✓	✓	×	✓	✓	✓	CCS, C/HW
UFED Classic Ultimate‡	2/3	✓	✓	✓	✓	✓	✓	3PIA, CCS, C/HW
UFED Touch Ultimate‡	2/3	✓	✓	✓	✓	✓	✓	3PIA, CCS, C/HW
XRY Complete‡	2/3	✓	✓	✓	✓	✓	✓	CCS, C/HW

Current tool list available at: http://www.cftt.nist.gov/tool_catalog/populated_taxonomy/

[11] iOS device acquisition only.

visited on 12/9/2016

Tool	Acquisition Level	Network Type			Forensic Tool	Exam/Analysis	Reports	MISC	
		GSM	CDMA	iDEN/TDMA					
CDMA Workshop	3	✓	✓	×	×	×	×	×	http://www.cftt.nist.gov/tool_catalog/populated_taxonomy/
Cell Phone Analyzer[12]†	3	✓	✓	×	✓	✓	✓	3PIA	
BeeProg2	4	✓			×	×	×	×	
FlashPAK III	4	✓			×	×	×	×	
NFI Memory Toolkit	4	✓			✓	✓	✓	×	
PC 3000 Flash	4	✓			✓	×	×	C/HW	
SD FlashDoctor	4	✓			✓	×	×	C/HW	
Soft-Center NAND Flash Reader	4	✓			×	×	×	×	
UP-828	4	✓			×	×	×	×	

† Denotes a tool that supports the logical acquisition of a UICC

‡ Denotes a tool that supports the logical acquisition of a UICC and the creation of a CNIC

MISC: 3rd Party Tool Image Analysis (3PIA), Chinese Chipset Support (CCS), Cables/Hardware Available (C/HW)

3.2 UICC Tools

A few mobile forensics tools deal exclusively with UICCs. These tools perform a direct read of a UICC's contents via a Personal Computer/Smart Card (PC/SC) reader, as opposed to an indirect read via the mobile device. The richness and scope of data acquired varies with the capabilities and features of the tool. The majority of UICC exclusive tools acquire the following data: International Mobile Subscriber Identity (IMSI), Integrated Circuit Card ID (ICCID), Abbreviated Dialing Numbers (ADN), Last Numbers Dialed (LND), SMS messages, and Location Information (LOCI) [Aye12].

Most tools provide additional information such as deleted SMS messages, properly rendered foreign language SMS and EMS messages. 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.

CSIM partitions on UICCs are being used with increasing frequency for LTE enabled mobile devices. At this time, few tools support the extraction of CSIM partition data as most only

[12] This tool only performs data analysis.

visited on 12/9/2016

support extraction of GSM and USIM partitions. CSIM data may prove to be of increasing forensic importance as this technology evolves.

3.3 Obstructed Devices

The following sections discuss techniques for bypassing an obstructed device i.e., a mobile device that requires successful authentication using a password or some other means to obtain access to the device. A number of ways exist to recover data from obstructed devices. These methods fall into one of three categories: software-based, hardware-based and investigative. Common obstructed devices include those with missing identity modules, PIN-enabled UICCs, or an enabled mobile device lock. Password locked and encrypted memory cards provide a user with additional means to protect data. This protection may make recovery of such data more complex. Content encryption capabilities are offered as a standard feature in many mobile devices or may be available through add-on applications. Software and hardware-based methods are often directed at a particular device or narrow class of device.

As mobile forensics tools have evolved, they have begun to provide automated functions allowing examiners to bypass many security mechanisms as a part of their products. For instance, some tools provide an automated function to recover passwords from locked mobile devices. In developing a method, the following sections provide actions that should be considered for determining possible approaches.

3.3.1 Software and Hardware Based Methods

Software-based methods used to break or bypass authentication mechanisms have begun to appear. For instance, some tools provide an automated function to recover passwords from locked mobile devices. This type of functionality varies greatly between mobile forensic tools and the devices models that are supported.

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 mobile device lock can be readily recovered from a memory dump of certain devices, allowing for a follow-on logical acquisition. JTAG and flasher boxes are often used this way to circumvent authentication mechanisms. Device-specific attacks, such as cold boot attacks, exist to bypass authentication mechanisms. Cold boot attacks have the ability to recover passwords from locked Android based devices by cooling the device 10 degrees below Celsius followed by disconnecting and reconnecting the battery in 500ms intervals [Mül12].

Few general-purpose hardware-based methods apply to a general class of mobile devices. Most of the techniques are tailored for a specific model within a class.

3.3.2 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 owner** – If a device is protected with a password, PIN or other authentication mechanism involving knowledge-based authentication, the owner may be queried for this information during an interview.

visited on 12/9/2016

- **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 mobile device, or with the owner, such as in a wallet, and may be recovered through visual inspection. Packaging material for a UICC or a mobile device may disclose a PIN Unlocking Key (PUK) that may be used to reset the value of the PIN. Device specific vulnerabilities may also be exploited, such as Smudge attacks. Smudge attacks involved careful analysis of the surface of a touch screen device to determine the most recent gesture lock used [Avi10].

- **Ask the service provider** – If a GSM mobile device is protected with a PIN-enabled UICC, the identifier (i.e., the ICCID) may 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 online, by entering the telephone number of the mobile device and specific subscriber information into public web pages set up for this purpose. Additionally, information may be obtained by contacting the device manufacturer (e.g., Apple).

Mobile device users may choose weak passwords to secure their device such as: 1-1-1-1, 0-0-0-0 or 1-2-3-4. Some of these numeric combinations are device default passcodes provided by the manufacturer. It is not recommended to attempt to unlock a device using these combinations due to several risk factors. They may include permanent wiping of mobile device memory, enabling additional security mechanisms (e.g., PIN/PUK) or initializing destructive applications. Mobile devices generally have a defined number of attempts before enabling further security precautions. Before making any attempts at unlocking a mobile device, it is recommended to consider the number of attempts left. There may be an instance where an examiner may choose to accept these risks in cases where this is the only option for data extraction.

3.4 Forensic Tool Capabilities

Forensic software tools strive to handle conventional investigative needs by addressing a wide range of applicable devices. More difficult situations, such as the recovery of deleted data from the memory of a device, may require more specialized tools and expertise and disassembly of the device. The range of support provided, including mobile device cables and drivers, product documentation, PC/SC readers, and the frequency of updates, may vary significantly among products. The features offered such as searching, bookmarking, and reporting capabilities may also vary considerably.

Discrepancies in recovering and reporting the data residing on a device have been noted in previous testing of tools. They include the inability to recover resident data, inconsistencies between the data displayed on workstation and that generated in output reports, truncated data in reported or displayed output, errors in the decoding and translation of recovered data, and the inability to recover all relevant data. On occasion, updates or new versions of a tool were also found to be less capable in some aspects than a previous version was [Aye11, Jan09].

Tools should be validated to ensure their acceptability and reapplied when updates or new versions of the tool become available. These results play a factor in deciding the appropriateness of the tool, how to compensate for any noted shortcomings, and whether to consider using a different version or update of the tool. Validating a tool entails defining and identifying a comprehensive set of test data, following acquisition procedures to recover the test data, and assessing the results [Aye11, Jan09]. Present-day tools seldom provide the means

visited on 12/9/2016

to obtain detailed logs of data extraction and other transactions that would aid in validation. An examiner can compare the output of several tools to verify the consistency of results. While tool validation is time consuming, it is a necessary practice to follow. As a quality measure, forensic specialists should also receive adequate up-to-date training in the tools and procedures they employ.

An 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 computing a cryptographic hash over 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 Validation: 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 may 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 using a tool such as sha1sum and retained for integrity verification. Even tools labeled as forensic tools may not compute a cryptographic hash, and in these cases an integrity hash should be computed separately.

Note that mobile devices are constantly active and update information (e.g., the device clock) continuously. 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 data items, such as individual files and directories, generally remain consistent. Hash inconsistencies may occur requiring the examiner to perform an element-by-element verification ensuring data integrity. Hash validation across multiple tools is challenging due to proprietary reporting formats.

visited on 12/9/2016

4. Preservation

Sections 4 through 7 describe the forensics process as it applies to mobile devices. Evidence preservation is the process of securely maintaining custody of 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 how to deal with mobile devices.

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 remaining sections of this chapter provide supplemental information related to mobile devices, following the paradigm of Securing and Evaluating the Scene, Documenting the Scene, Isolation, Packaging, Transporting, and Storing Evidence, and Triage/On-Site Processing.

4.1 Securing and Evaluating the Scene

Incorrect procedures or improper handling of a mobile device during seizure may cause loss of digital data. Moreover, traditional forensic measures, such as fingerprints or DNA testing, may need to be applied to establish a link between a mobile device and its owner or user. If the device is not handled properly, physical evidence may be contaminated and rendered useless.

Alertness to mobile device characteristics and issues (e.g., memory volatility) and familiarity with tangential equipment (e.g., media, cables, and power adapters) are essential. For mobile devices, sources of evidence include the device, UICC and associated media. Associated peripherals, cables, power adapters, and other accessories are also of interest. All areas of the scene should be searched thoroughly ensuring related evidence is not overlooked.

Equipment associated with the mobile device, such as removable media, UICCs, or personal computers, may prove more valuable than the mobile device itself. Removable media varies in size and can be easily hidden and difficult to find. Most often, removable memory cards are identifiable by their distinctive shape and the presence of electrical contacts located on their bodies that are used to establish an interface with the device. Personal computers may be particularly useful in later accessing a locked mobile device, if the personal computer has established a trusted relationship with it. For example, Apple incorporates a pairing process whereby an existing pairing record file can be used by some tools [Zdz12] to access the mobile device while it is still locked.

When interviewing the owner or user of a mobile device, consider requesting any security codes, passwords or gestures needed to gain access to its contents. For example, GSM devices may have authentication codes set for the internal memory and/or the UICC.

While securing a mobile device, caution should be taken when an individual is allowed to handle the mobile device. Many mobile devices have master reset codes that clear the contents of the device to original factory conditions. Master resets may be performed remotely requiring proper precautions such as network isolation to ensure that evidence is not modified or destroyed.

visited on 12/9/2016

Mobile devices may be found in a compromised state that may complicate seizure, such as immersion in a liquid. In these situations, forensic examiners should adhere to agency specific procedures. One method involves removal of the battery preventing electrical shorting, while the remainder of the mobile device is 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.

Mobile devices and associated media may be found in a damaged state, caused by accidental or deliberate action. Devices or media with visible external damage do not necessarily prevent the extraction of data. Damaged equipment should be taken back to the lab for closer inspection. Repairing damaged components on a mobile device and restoring the device to working order for examination and analysis may be possible.

Undamaged memory components may also be removed from a damaged device and their contents recovered independently. This method should be used with caution, as it is not possible with all devices.

4.2 Documenting the Scene

Evidence must be accurately identified and accounted for. Non-electronic materials 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. Photographing the crime scene in conjunction with documenting a report on the state of each digital device and all computers encountered may be helpful in the investigation, if questions arise later about the environment.

A record of all visible data should be created. All digital devices, including mobile devices, which may store data, should be photographed along with all peripherals cables, power connectors, removable media, and connections. Avoid touching or contaminating the mobile device 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.

4.3 Isolation

Many mobile devices offer the user with the ability to perform either a remote lock or remote wipe by simply sending a command (e.g., text message) to the mobile device.

Additional reasons for disabling network connectivity include incoming data (e.g., calls or text messages) that may modify the current state of the data stored on the mobile device. Outgoing data may also be undesirable as the current GPS location may be delivered to an advisory providing the geographic location of the forensic examiner.

Therefore, forensic examiners need to be aware and take precautions when securing mobile devices mitigating the chance of data modification. The Scientific Working Group on Digital Evidence's (SWGDE) "Best Practices for Mobile Phone Forensics" document covers best practice for the proper isolation of mobile devices [SWG13]. Some key implications for proper collection are summarized below.

visited on 12/9/2016

Isolating the mobile device 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 personal computer, pulling the plug from the back of the personal computer eliminates data transfer or synchronization overwrites. It is recommended that a capture of the personal computer's memory be extracted before "pulling the plug" as memory acquired generally proves to be of significant forensic value. Caution should be used, as removing a device that if performing a software update or backup has the potential to corrupt the mobile device's file system. The use of memory forensics tools for the capture of a personal computer's memory should be done by a qualified digital forensics professional. The mobile device should be seized along with associated hardware. Media cards, UICCs, and other hardware residing in the mobile device should not be removed. Also, seizing the computer that was connected to the mobile device provides the ability to acquire synchronized data from the hard disk that might not be obtained from the device. Any associated hardware such as media cards, UICCs, power adapters, device sleeves, or peripherals, should be seized along with related materials such as product manuals, packaging, and software.

Isolating a mobile device from all radio networks (e.g. WiFi, Cellular and Bluetooth) is important to keep new traffic, such as SMS messages, from overwriting existing data. Besides the risk of overwriting potential evidence, the question may arise whether data received on the mobile device after seizure is within the scope of the original authority granted. Vulnerabilities may exist that may exploit a weaknesses related to software vulnerabilities from the web browser and OS, SMS, MMS, third-party applications and WiFi networks. The possibility of such vulnerabilities being exploited may permit the argument that data may have been modified during the forensic examination.

Three basic methods for isolating the mobile device from radio communication and preventing these problems are to either: place the device in airplane mode, turn the device off, or lastly place the device in a shielded container. Each method has certain drawbacks.

- Enabling "Airplane Mode" requires interaction with the mobile device using 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). Note: airplane mode does not prevent the system from using other services such as GPS in all cases.

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

- Keeping the mobile device on, but radio isolated, shortens battery life due to increased power consumption as devices unable to connect to a network raise their signal strength to maximum. After some period, failure to connect to the network may cause certain mobile devices to reset or clear network data that otherwise would be useful if recovered [Smi05]. Faraday containers may 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 Faraday container (e.g., bag improperly sealed, exposed cables connected to the forensic workstation may act as an antenna) and unknowingly allowing access to the cell network also exists.

To conserve power, some mobile devices are normally configured to enter energy savings mode and shut off the display after a short period of inactivity. Some devices also shut

visited on 12/9/2016

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 such a device in the active state is troublesome, requiring periodic interaction with the device. 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 is likely. Moreover, authentication mechanisms, such as passwords, typically cannot be deactivated without first satisfying the mechanism (e.g., supplying the correct password).

The time maintained on the mobile device 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.

Security mechanisms, key remapping and malicious programs may be present on mobile devices. Certain types of modifications to the software applications and operating system of the device 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 login, biometric, and other authentication mechanisms are available for mobile devices may be 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 mobile device may contain a virus or other malicious software. Such malware[13] may attempt to spread to other devices over wired or wireless interfaces, including cross-platform jumps to completely different platforms. Common utilities or functions may also be intentionally replaced with versions of software designed to alter or damage data present on a mobile device. Such 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 chords or over the air messages) and carry out actions such as deleting the contents of the device.

- 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.

- Geo Fencing – Some devices may be configured to automatically wipe all data when the GPS in the device determines that it has left (or entered) a specific predetermined geographic area. This method may also employ WiFi towers for location determination as well.

---

[13] For more information, visit: http://appleinsider.com/articles/13/05/14/mobile-malware-exploding-but-only-for-android

visited on 12/9/2016

- Explosives and Booby Traps – Mobile devices may be rigged to detonate bombs remotely or explode themselves if a specific action is carried out on the device (e.g., receiving an incoming call, text message or pressing a specific key chord sequence, etc.).[14]

- Alarms – Many mobile devices have an audible alarm feature. The alarm function is capable of powering on an inactive device, establishing network connectivity and the potential for a remote wipe.

The following sections 4.3.1 through 4.3.3 discuss the use and characteristics of radio isolation containers and cellular network isolation techniques.

4.3.1 Radio Isolation Containers

A field test on the effectiveness of various mobile phone shielding devices (i.e., a tool designed to act as a Faraday cage) was conducted at Purdue University. There are many shielding devices that claim to radio isolate a mobile device unfortunately these tools do not always successfully prevent network communication [Kat10]. The tests conducted at Purdue used multiple shielding devices with mobile devices operating over three of the largest U.S. providers while varying the distance from the provider's towers.

The majority of the test cases proved that the shielding devices tested did not prevent network communication in all cases, and SMS messages most often penetrated the device while shielded, followed by voice calls and MMS messages. Three reasons why the shielding devices may fail are due to: the materials not providing enough attenuation, leaks or seams in the shield or the conductive shield acting as an antenna.

While many manufacturers claim the effectiveness of their shielding device it is important to understand the effectiveness of the isolation device is based upon attenuating signal between specific decibels. Therefore, the effectiveness of the isolation containers tested were not 100% effective in most cases and devices used to preserve evidence require verification.

Some of the products mentioned in the above paper have since been improved to provide a more effective radio isolation solution. Examiners should test their own products to validate that they are working properly before use.

4.3.2 Cellular Network Isolation Techniques

A number of techniques exist for isolating a mobile device from cell tower communications [INT06]. The device should be fully charged prior to examination and consideration should be given to having a fixed or portable power source attached. The following provides an overview of various cellular network isolation techniques.

- Cellular Network Isolation Card (CNIC) - A CNIC mimics the identity of the original UICC and prevents network access to/from the handset. Such cards prevent the handset from erasing call log data due to a foreign SIM being inserted. This technique permits acquisition without concern of wireless interference.

---

[14] For more information, visit: http://www.scientificamerican.com/article.cfm?id=boston-marathon-bomb-attack

visited on 12/9/2016

- Shielded Containers - A portable shielded container may allow examinations to be conducted safely once the phone is situated inside. Cables connected to the container must be fully isolated to prevent network communications from occurring. This method is one of the most frequently used.

- Shielded Work Areas - 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 workspace may also be very restrictive.

- Disabling Network Service - The cellular carrier providing service to the mobile device might be able 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 may also impose delays.

- Jamming/Spoofing Devices - Emitting a signal stronger than a cell phone's or interfering with the signal rendering communication useless. Another technique involves tricking the phone into thinking a "no service" signal is coming from the nearest cell tower. Because such devices may affect communications in the surrounding public airspace beyond the examination area, unlicensed use may be illegal in some jurisdictions. [NIJ05]

4.3.3 Cellular Network Isolation Cards

Some tools have the ability to create a Cellular Network Isolation Card (CNIC) [SWG13]. CNICs provide cellular network isolation preventing network communication that may modify data contained on a mobile device (e.g., remote wiping, incoming text messages). A CNIC lacks specific data elements required to establish connectivity between the mobile device and its associated network. For example, CNIC's do not contain a cipher key, thus preventing access with a cellular network. A CNIC may be required for mobile device data extraction, as some phones are unable to boot without a UICC present.

Some tool manufacturers and vendors refer to this as a "SIM clone." The creation of a CNIC is not a true clone of the source UICC, because the authentication key and other user data are not copied in the cloning process.

A CNIC may be created either by the examiner using the original UICC as a source or by entering the data manually. Manual entry is helpful if the UICC associated with a specific mobile device is not present. CNICs are tool specific; they are not interchangeable between the tools of various manufacturers. CNICs vary in their effectiveness and support, based on specific mobile devices. For example, CNICs may not be used for data extraction from TDMA devices.

Occasionally, a UICC may not be present with a mobile device, or may be intentionally damaged, but necessary for data acquisition. One of the most common mistakes forensic examiners make is to insert a foreign UICC into the mobile device to facilitate data acquisition. Some mobile devices are linked to a specific UICC. When this linkage exists, booting a mobile device with a foreign UICC causes data elements such as: call logs (missed, incoming and

visited on 12/9/2016

outgoing calls) and SMS messages present within the internal memory of the mobile device to be erased [Rei08].

A better approach is to create a substitute UICC (i.e., CNIC) to use with the mobile device that mimics key characteristics of the original UICC, tricking the device to accept it as the original. Most mobile forensic tools provide the forensic examiner with the ability to create a CNIC.

Substituting UICCs, sometimes referred to as CNICs, may be useful in a number of situations:

- If a mobile device's UICC is missing or damaged and is required for acquisition with a forensic tool, creation of a CNIC permits data to be recovered from the handset.
- If the UICC for a device is present, but requires a PUK code, a substitute UICC can be created providing acquisition to proceed without having to contact the service provider for the PUK.
- If cellular network isolation is required (e.g., avoiding incoming calls or text messages) a CNIC provides a method permitting acquisition of data from the handset while simultaneously denying cellular network authentication.
- If a forensic tool accesses the UICC during the acquisition process, using a CNIC in the handset eliminates the possibility of the original being modified (e.g., status flag of SMS messages modified from unread to read).

The values by which the mobile device correlates to the previously inserted UICC are the ICCID and the IMSI [Rei08]. Often only one of these values is used. Both identifiers are unique and used to authenticate the user to the network. While the minimum data needed to create a UICC may be simply one of these two values, some mobile devices may require additional data to be populated on the CNIC to be properly recognized. The possibility exists that data, other than user data, may change on the handset as the result of inserting a CNIC [INT06].

4.4 Packaging, Transporting, and Storing Evidence

Once the mobile device is ready to be seized, the forensic specialist should seal the device in an appropriate container and label it appropriately according to agency specifications.

Due to the volatile nature of some mobile devices, they should immediately be checked into a forensic laboratory for processing and the power requirements should be discussed with the evidence custodian. Battery powered devices held in storage for more than a day 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.

4.5 On-Site Triage Processing

Currently many organizations are challenged with large backlogs of digital forensics casework. An on-site triage solution is being employed more and more world-wide to accommodate for this exponential growth in digital forensic caseload. Triaging involves performing a data

visited on 12/9/2016

extraction (i.e., Manual or Logical) on-scene followed immediately by a preliminary analysis of the data extracted. Logical extraction tools are providing additional capabilities to use keywords and specific known hashes alerting the on-scene examiner immediately to potential issues that need to be addressed. Where possible, devices supporting encryption, such as Android and iOS devices, should be triage processed at the scene if they are found in an unlocked state, as the data may no longer be available to an investigator once the device's screen is locked, or if the battery exhausts. Deploying the use of field forensics tools to either acquire the device, or establish a trusted relationship with the device, will ensure that the data can be accessed at a later time, after the device has locked. [Zdz12].

On-Site Triage is especially useful in identifying:

- Media most likely to contain evidence
- Those investigations that require a more detailed and technical examination
- The investigations that could be subject of limited examination by qualified practitioners
- Material requiring urgent investigation
- Examinations suitable for outsourcing
- The extent of the assistance the unit will need to provide to an investigation [ACP11]

On-Site Triage processing benefits include:

- Reduced laboratory workload - Digital forensic laboratory submissions may be reduced when nothing of interest is found on-scene and the level of suspicion is low
- Exigency - On-scene examiners have actionable results immediately
- Better leveraging of existing resources - Intelligence resources are enhanced through the use of keywords/hash lists
- Reduced training costs - Triage tools are typically designed to require less training than deeper analysis tools and techniques
- Reduced unit cost – Triage tools are frequently more affordable than deeper analysis capable counterparts
- Live collection opportunity – Devices are often presented in an unlocked state affording the on-site examiner the potential to extract more data before the locking mechanism is activated

Organizations may wish to develop some sort of "scoring" method to aid with the prioritization of on-site triage examinations. This should be developed on a per-organization basis and should be reviewed and updated to accommodate changes.

visited on 12/9/2016

4.6 Generic On-Site Decision Tree

Figure 7 illustrates an example of an on-site decision tree that may be used as a general guideline for organizations and agencies. This provides a starting point intended for customization allowing alignment with existing policies and procedures. The following list describes some of the actions and decision points contained within the tree.

- Unlocked/Undamaged – Is the device in an unlocked state and functional permitting a manual or logical data extraction?
- Urgent – Do circumstances exist such that data extraction is required on site?
- Lab less than 2 hours away – Can the mobile device be transported to a forensics laboratory in less than 2 hours?
- Tool/Training – Is the device supported by the tool and has the examiner received proper training?
- Contact Expert – The on-site examiner should contact an expert for additional assistance and guidance.
- Battery More than 50% – Does the device show that it has more than 50% remaining battery power?
- Need More Data - After the extraction is successful and the examiner has reviewed the results, is additional information or analysis required?

visited on 12/9/2016

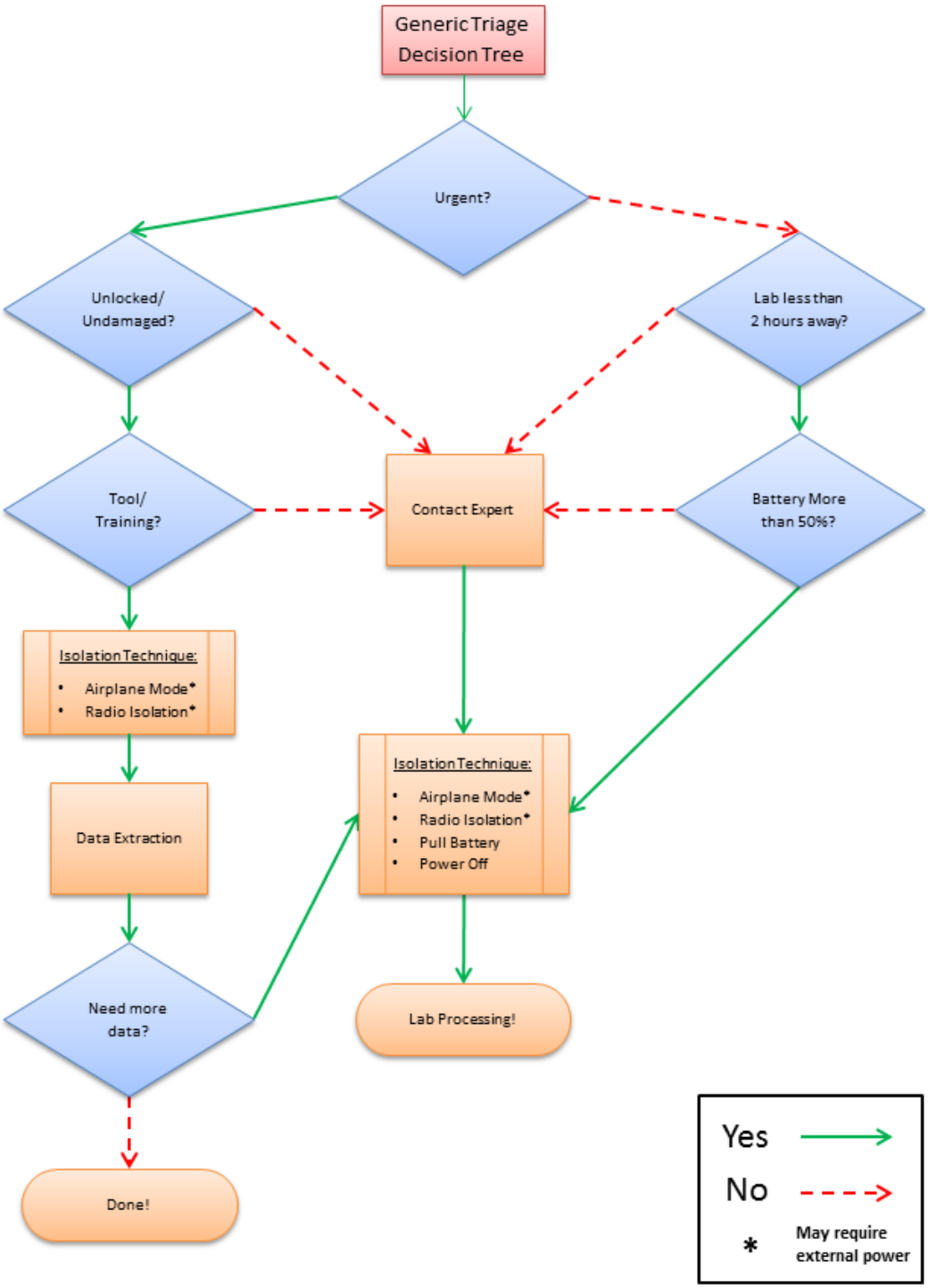


Figure 7: Generic Triage Decision Tree

visited on 12/9/2016

5. Acquisition

Acquisition is the process of imaging or otherwise obtaining information from a mobile device and its associated media. Performing an acquisition at the scene has the advantage that loss of information due to battery depletion, damage, etc. during transportation and storage is avoided. Off-site acquisitions unlike a laboratory setting may be challenging in finding a controlled setting in which to work with the appropriate equipment while satisfying additional prerequisites. For the purpose of this discussion, a laboratory environment is assumed throughout this chapter.

The forensic examination begins with the identification of the mobile device. The type of mobile device, its operating system, and other characteristics determine the route to take in creating a forensic copy of the contents of the device. The type of mobile device and data to be extracted generally dictates which tools and techniques should be used in an investigation.

5.1 Mobile Device Identification

To proceed effectively, mobile devices need to be identified by the make, model, and service provider. If the mobile device is not identifiable, photographing the front, back and sides of the device may be useful in identifying the make, model and current state (e.g., screen lock) at a later time. Individuals may attempt to thwart specialists by altering the mobile device to conceal its true identity. Device alteration may 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. These modifications should be taken into consideration on a case-by-case basis.

If the mobile device is powered on, the information appearing on the display may aid in mobile device identification. 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, MEID). Removing the battery from the cavity of a mobile device, even when powered off, may affect its state, particularly the contents of volatile memory. Most mobile devices keep user data in non-volatile memory (i.e., NAND). If the mobile device is powered on, battery removal will power it off, possibly causing an authentication mechanism to trigger when powered back on.

Other clues that allow identification of a mobile device include such things as: manufacturer logos, serial numbers, or design characteristics (e.g. candy bar, clam shell). 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 may also help to differentiate among operating system families. Further means of identification include the following:

- **Device Characteristics** – The make and manufacturer of a mobile device may 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 mobile device that may be queried based on selected attributes to identify a particular

visited on 12/9/2016

device and obtain its specifications and features.[15] Coverage is considerable, but not extensive nor complete, and may require consulting more than one repository before making a match.

- **Device Interface** – The power connector can be specific to a manufacturer and may provide clues for device identification. With familiarization and experience, the manufacturers of certain mobile devices may be readily identified. Similarly, the size, number of contacts, and shape of the data cable interface are often specific to a particular manufacturer and may prove helpful in identification.

- **Device Label** – For mobile devices that are inactive, information obtained from within the battery cavity may be of assistance, particularly when coupled with an appropriate database. The manufacturer's label often lists the make and model number of the mobile device and also unique identifiers, such as the Federal Communications Commission Identification Number (FCC ID) and an equipment identifier (IMEI or MEID). The FCC and equipment identifiers may be found on mobile devices sold in the U.S. domestic market.

  For all mobile devices that use a UICC, the identity module is typically located under the battery and 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) may be obtained by keying in *#06#. Similar codes exist for obtaining the Electronic Serial Number (ESN) or Mobile Equipment Identifier (MEID) from powered on CDMA phones. Various sites on the Internet offer databases that provide information about the mobile device based on an identifier, such as the following:

  - 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.[16]

  - The ESN is a 32-bit identifier recorded on a secure chip in a mobile device by the manufacturer. The first 8-14 bits identify the manufacturer and the remaining bits represent the assigned serial number. Many mobile devices have codes that can be input into the handset to display the ESN. Hidden menus may also be activated on certain mobile devices 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 may be obtained. Manufacturer codes may be checked online at the Telecommunications Industry Association Web site.[17]

---

[15] For more information, visit: http://www.phonescoop.com/phones/finder.php, http://www.gsmarena.com/search.php3, and http://mobile.softpedia.com/phoneFinder.

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

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

visited on 12/9/2016

- The ICCID of the UICC may 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 may be determined by the ICCID. If the ICCID does not appear on the UICC, it may be obtained with a UICC acquisition tool. The GSM numbering plan Web site supports ICCID queries for this information.[18]

- 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 mobile device, including photos, user manual, and radio frequency test results.[19]

- MEID consists of a set of characters 56-bits in length (14 hex digits). It contains three fields, including an 8-bit regional code (RR), a 24-bit manufacturer code, and a 24-bit manufacturer-assigned serial number. The check digit (CD) is not considered part of the MEID. The MEID was created to replace ESNs, as all ESN's were exhausted by November 2008.

- **Carrier Identification** – The carrier for a mobile device may have their logo printed on the exterior. This is traditionally displayed prominently to allow for advertising and branding. This may provide the examiner with insight on which carrier the mobile device operates. Mobile devices may be unlocked and possibly re-flashed to operate using a competing carrier. One method to make this determination is to examine the UICC if present. Most carriers imprint their logo on the front of the UICC. Additionally, extraction and analysis of the ICCID provides further confirmation.

- **Reverse Lookup** – 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.[20] This service covers both U.S. and Canadian phone numbers. If the telephone number of the mobile device is known, a reverse lookup may be used to identify the network operator and the originating city and state. For example, FoneFinder™ is a service to obtain such information.[21] The network operator's web site typically contains lists of supported devices that may be used to narrow down and possibly identify the mobile device in question. Because phone numbers may be ported among service providers, in many situations more up-to-date information is required.

5.2 Tool Selection and Expectations

Once the make and model of the mobile device are known, available manuals should be retrieved and studied. The manufacturer's web site is a good place to begin. Typing the model number into a search engine may also reveal a significant amount of information about the mobile device. As mentioned earlier, the device being acquired largely dictates the choice of

---

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

[19] For more information, visit http://transition.fcc.gov/oet/ea/fccid/.

[20] For more information, visit: http://www.npac.com/the-npac/access/law-enforcement-agencies-psaps.

[21] For more information, visit http://www.fonefinder.net/.

visited on 12/9/2016

forensic tools. The following criteria have been suggested as a fundamental set of requirements for forensic tools, 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 of the output of the tool has been verified
- **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
- **Tested** – the ability to determine if known data present within the mobile device internal memory is not modified and reported accurately by the tool

Experimenting with various tools on test devices to determine which acquisition tools work efficiently with specific mobile 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 setup 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 may arise sporadically that require adjustment to existing procedures, and in some situations require new procedures and methods to be devised. Some examples include: UICCs being permanently bonded into a mobile device, mobile devices capable of supporting multiple UICCs and mobile devices 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. Testing should occur on the same model of mobile device before attempting procedures on the case device. The development and validation of the procedures should be documented and include the following steps [DOJ08]:

- 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

5.3 Mobile Device Memory Acquisition

Mobile devices are often submitted for laboratory processing with only specific items requested for recovery, such as call logs or graphics. If any doubt or concerns exist about the requested data, contacting the submitter for clarification is recommended. Though it is not

visited on 12/9/2016

always necessary to recover all available data, a complete acquisition avoids having to redo the process later if additional data is requested. For examinations involving a limited scope search warrant (e.g., only text messages), a full memory data extraction may be completed but care should be taken to only report items covered by the warrant.

To acquire data from a mobile device, a connection must be established to the device from the forensic workstation. Before performing an acquisition, the version of the tool or device 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 device when handling it, for example, by pressing keys that may corrupt or erase data. Once the connection has been established, the forensic software suite or device may proceed to acquire data from the mobile device.

The date and time maintained on the mobile device is an important piece of information. The date and time may have been obtained from the network or manually set by the user. Owners may manually set the day or time to different values from the actual ones yielding misleading values in the call and message records found on the mobile device. If the device was on when seized, the date and time maintained and differences from a reference clock should have already been recorded. Nevertheless, confirmation at the time acquisition may prove useful. If the mobile device was off when seized, the date and time maintained and differences from a reference clock should be recorded immediately when first powered on. Actions taken during acquisition, such as removal of the battery to view the device label, may affect the time and date values.

Mobile devices may provide the user with an interface for a memory card. Mobile device forensic tools that acquire the contents of a resident memory card normally perform a logical acquisition. If the device is found in an active state, the mobile device internal memory should be acquired before removing and performing a physical acquisition of the associated media (e.g., microSD Card). Otherwise, if the device is found in a power off state, a physical acquisition of the removable media should be performed before the internal handset memory of the mobile device is acquired. With either type of acquisition, the forensic tool may or may not have the capability to decode recovered 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 confirm that the contents of a device were captured correctly. On occasion, a tool may fail without any error notification and require the specialist to reattempt acquisition. 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 mobile device using the available menus may be acquired and decoded through a logical acquisition. Manually scrutinizing the contents via the device 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 extraction must always be done with care, preserving the integrity of the device in case further, more elaborate acquisitions are necessary.

The contents of a mobile device's memory often contain information, such as deleted data, that is not recoverable through either a logical or manual extractions. Lacking a software tool able to perform a physical acquisition, it may be necessary to turn to hardware-based techniques. Two techniques commonly used are acquisition through a standardized JTAG test interface, if

visited on 12/9/2016

supported on the device, and acquisition by directly reading memory that has been removed from the device [Bro12].

5.3.1 GSM Mobile Device Considerations

Mobile devices that do not require a UICC are relatively straightforward as the acquisition entails a single device. Mobile devices requiring UICCs are more complex. There are two items that must be examined: the handset and the UICC. Depending on the state of the mobile device (i.e., active, inactive) the handset and UICC may be acquired jointly or separately. It is generally accepted to process the UICC first while the device is in an inactive state.

If the mobile device is active, a joint acquisition of the handset and UICC contents should be acquired first. A direct acquisition recovers deleted messages present on a UICC, while an indirect acquisition via the handset does not. The UICC must be removed from the mobile device and inserted into an appropriate reader for direct acquisition.

A well-known forensic issue that arises when performing a joint acquisition is that the status of unread text messages change between acquisitions. The first acquisition may alter the status flag of an unread message to read. Reading an unread text message from a UICC indirectly through the handset causes the operating system of the device to change the status flags. UICCs that are read directly by a tool do not make these modifications. One way to avoid this issue is to omit selecting the recovery of UICC memory when performing the joint acquisition (if the tool allows such an option) [Rei08].

If the mobile device is inactive, the contents of the UICC may be acquired independently before that of the handset. The UICC acquisition should be done directly through a PC/SC reader. The handset acquisition should be attempted without the UICC present. Many devices permit an acquisition under such conditions, allowing PIN entry for the UICC to be bypassed, if it were enabled. If the acquisition attempt is unsuccessful, the UICC may be reinserted and a second attempt made. Performing separate independent acquisitions (i.e., acquiring the UICC before acquiring the contents of the handset) avoids any operating system related forensic issues associated with an indirect read of UICC data. However, removing the SIM can reportedly cause data to be deleted on some mobile devices [Cas11].

5.3.2 iOS Device Considerations

Since mid-2009, beginning with the release of the iPhone 3G[s], Apple has shipped all iOS devices with a dedicated cryptographic chip, making hardware accelerated encryption possible. Apple has incorporated this accelerated cryptography into the operating system, marketed as a feature named Data Protection. Data Protection is the combination of hardware-accelerated encryption and an authenticated cryptographic scheme, allowing any file or piece of information to be encrypted or decrypted with a separate key.

Files protected with data protection are encrypted with a random file key, which is then encrypted using a higher tier class key, and stored as a file tag with the file. Passwords (and other sensitive small data) are stored on the device are encrypted using a similar approach, and are stored in the iOS keychain, a device key escrow mechanism built into the operating system.

Files and keychain elements are both protected by one of a number of access control keys, which are also encrypted in a way that incorporates the user's device passcode. The passcode

visited on 12/9/2016

must be known in order to decrypt the key hierarchy protecting these select files and keychain elements, and also to disable the device's GUI lock.

The implementation of Data Protection has been criticized for a number of design flaws and was originally exploited as shown by Zdziarski in 2009 [Zdz12]. Due to the simplicity of four-digit PINs or short passwords, brute forcing the device passcode is often a computationally feasible task. In many cases, brute forcing a four-digit PIN has shown to take at most 20 minutes.

Nevertheless, this encryption scheme poses significant challenges to the forensic investigator. The forensic examiner should be aware of these issues as well as the impact that this encryption has on any iOS based device presented for examination. Supported devices include iPhone 3GS and iPhone 4 (both GSM and CDMA models), first-gen iPad, and latest releases of iPod Touch (3rd and 4th generation). All of these devices have the option to perform a remote wipe of data contained within them. When activated, the UID is destroyed and 256 bits of the key are destroyed leaving the examiner with an extremely complex decryption problem. To avoid such scenarios, it is recommended that radio communications are blocked or disabled prior to an examination as well as during transportation to the lab for examination.

When data protection is active, the file key is obliterated when the file is deleted, leaving encrypted and generally unrecoverable file contents in unallocated space, which render traditional carving techniques for deleted files useless. Data however can often be found residing inside allocated data containers (i.e., SQLite Tables) and should not be discounted or ignored as part of any examination. Recovery of such data can be challenging as SQLite data recovery may be somewhat automated (e.g., epilog), often manual recovery may be the only option. Fortunately for the forensic investigator, a significant portion of user data is stored within allocated data containers and garbage collection is not generally performed on these containers.

Apple also offers a feature to users to encrypt all backup data when using iTunes (iOS 4 and later). This option, when used will only present encrypted files from some forensic extraction tools. These backups can be decrypted using a brute force attack. Tools exist to perform this attack using GPU acceleration to facilitate a faster brute force attack. The backup encryption feature only applies to data sent through the device's backup service, however a number of other services run on the device that provide clear text copies of data, even if backup encryption is active. If the acquisition tool is capable of communicating to these other services, a significant amount of clear text data can be recovered, even if the backup password is not known.

5.3.3 Android Device Considerations

Android is an operating system designed by Google primarily for mobile devices such as smartphones and some tablet computers. Android was first released in 2007 and the first Android based phone was released in October 2008. The Android operating system is open source and Google releases a major version about once per year.

Each one of the different versions of the operating system requires slight modifications for each family of device for full support. This has led to hundreds (if not thousands) of different distributions in the wild.

visited on 12/9/2016

Much like Apple's iTunes Store, Android has a main application repository called the Google Play Store. Analysis of submitted applications for soundness in the store are much lower and have resulted in many rogue applications making their way into the mainstream application pool. Dozens of other Android application repositories exist as well. This has led to thousands of applications that may be encountered by the examiner.

Most of the Android user and application data will be found in SQLite tables located in separate folders for each installed application. This may require the examiner to dump all data contained in all SQLite tables and perform a search of the resultant data searching for relevant material as less than 5% of the applications are supported by the majority of mobile forensic tools.

Since the operating system is designed for touch screen use, the default protection scheme for the device is a gesture password lock. The lock presents a 3X3 grid for the user to trace his/her finger connecting several cells of the grid to form a pattern. Once the correct pattern is traced, the phone is unlocked. Some forensics tools exist to obtain the gesture.key file to unlock the device.

Most of the access methods for a locked Android device rely on debug mode to be active on the device to begin the forensics extraction process. A few tools have been released that can enable debug mode from a locked device; however, the number of supported models is very small.

Most Android based mobile devices have removable microSD memory cards. The data contained on the microSD Card should not be overlooked as they frequently contain a great deal of unencrypted and unprotected data. As best practice, the microSD card should be write-blocked and imaged using standard digital forensic techniques. The image may then be examined using traditional digital forensic tools, as the media is generally a single partition formatted using exFAT.

Getting into locked devices is also possible using JTAG methods and tools to obtain all of the data from the memory of the handset. This bypasses the locked USB port (USB Debugging turned off) and probes Test Access Ports between the USB Port and the CPU. JTAG provides communication to NAND memory through the CPU allowing memory to be read.

Many tools are able to parse much of the information presented in the Android OS however all tools suffer the same problem as iOS based devices -- multitudes of applications. Hundreds of applications are added every week. Understanding and reverse engineering each one of them one-at-a-time is a time consuming process. Many vendors have chosen to focus on parsing the data from the more popular communication applications (e.g., WhatsApp, FaceBook, etc.). The more advanced examiner should be aware of this shortcoming and be prepared to perform testing and reverse engineering for some cases where support for specific applications may not yet exist.

5.3.4 UICC Considerations

Similar to a mobile device, to acquire data from a UICC, a connection must be established from the forensic workstation to the UICC, using a PC/SC 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 may proceed to acquire data from the UICC.

visited on 12/9/2016

Capturing a direct image of the UICC 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 UICC 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 UICCs 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 UICC 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.

5.4 Tangential Equipment

Tangential equipment includes devices that contain memory and are associated with a mobile device. The three main categories are memory cards, host computers to which a mobile device has synchronized its contents and cloud-based storage.

Smartphones may provide an interface that supports removable media (e.g., microSD or MMC), which may contain significant amounts of data. Memory cards are typically flash memory, used as auxiliary user file storage, or as a means to convey files to and from the device. Data may be acquired with the use of a write-blocked media reader and a forensic application.

The data contained on a mobile device is often present on a personal computer, due to the capability of mobile devices 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 data on a mobile device may be present on the owner's laptop or personal computer and recovered using a conventional computer forensic tool for hard drive acquisition and examination [Bad10].

5.4.1 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 personal 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.

Mobile devices are typically populated with data from the personal computer during the synchronization process. A significant amount of informative data may reside locally on a personal computer. Data from the mobile device may also be synchronized to the computer, through user-defined preferences in the synchronization software. Because the synchronized

visited on 12/9/2016

contents of a mobile device 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 mobile device files are stored on the PC. Each synchronization protocol has a default installation directory, but the location may be user specified.

5.4.2 Memory Cards

Memory card storage capacity ranges from 128MB and up. As technological advances are made, such media becomes physically smaller and offers larger storage densities. Removable media extends the storage capacity of mobile devices 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.

A physical acquisition of data present on removable media provides the examiner the potential to search the contents of the media and potentially recover deleted files. One drawback is that mobile device data, such as SMS text messages 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. For instance, BlackBerry™ devices provide the user with the ability to encrypt data contained on the removable media associated with the mobile device. Table 4 gives a brief overview of various storage media in use today.

Table 4: Memory Cards

Name	Characteristics
MMCmicro	Dime 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
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) and microSDXC	Dime size (length-15 mm, width-11 mm, and thickness-1 mm) 6-pin connector, 1 or 4-bit data bus
Memory Stick Micro	Dime size (length-12.5 mm, width-15 mm, and thickness-1.2 mm) 11-pin connector, 4-bit data bus

5.5 Cloud Based Services for Mobile Devices

Mobile cloud computing is the combination of mobile networks and cloud computing allowing user applications and data to be stored on the cloud (i.e., internet servers) rather than the mobile device memory. This data may be stored across geographically diverse locations.

visited on 12/9/2016

Cloud computing environments are complex in their design and frequently geographically disperse. Often, storage locations for cloud computing are chosen due to lowest cost and data redundancy requirements. One issue may be identification of the location of the data. This is an emerging field.

Cloud storage opens numerous possibilities for mobile device application developers beyond mobile device memory limitations. As mobile applications evolve data retrieval becomes seamless to the user and not apparent if data is stored on the cloud or the internal memory of the mobile device.

There are several factors within cloud computing environments that challenge forensics examiners requiring a hybrid approach to include both live and "dead box" forensic techniques. Additionally, recovery of user data stored in the cloud may become more problematic based on laws and regulations. Retrieval and analysis of cloud based data should follow agency specific guidelines on cloud forensics.

The mobile device forensics examiner should not discount cloud based data left behind (e.g., browser cache or other forensics artifacts) that may be present on tangential equipment enabling an examiner to piece together what has occurred on a device.

visited on 12/9/2016

6. 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. Examination is a technical process that is the province of a forensic specialist. However, analysis may be done by roles other than a specialist, such as the investigator or the forensic examiner.

The examination process begins with a copy of the evidence acquired from the mobile device. Fortunately, compared with classical examination of personal computers or network servers, the amount of acquired data to examine is much smaller with mobile devices. 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. While interoperability among the acquisition and examination facilities of different tools is possible, only a few tools support this feature. Examination and analysis using 3rd party tools are generally accomplished by importing a generated mobile device memory dump into a mobile forensics tool that supports 3rd party mobile device images.

The forensic examiner will need information about the case and the parties involved to provide a starting point for potential evidence that might be found. Conducting the examination is a partnership between the forensic analyst or examiner and the investigator. The investigator provides insight into the types of information sought, while the forensic examiner provides the means to find relevant information that might be on the system.

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 all Internet history files.

6.1 Potential Evidence

Mobile device 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 vary based on the era in which the device 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 may include the following items:

visited on 12/9/2016

- Subscriber and equipment identifiers
- Date/time, language, and other settings
- Phonebook/Contact information
- Calendar information
- Text messages
- Outgoing, incoming, and missed call logs
- Electronic mail
- Photos
- Audio and video recordings
- Multi-media messages
- Instant messaging
- Web browsing activities
- Electronic documents
- Social media related data
- Application related data
- Location information
- Geolocation data

Even esoteric network information found on a UICC 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 (Public Land Mobile Networks) elementary file is updated with the code of the country and network involved [3GP07]. This list is maintained on the UICC and is due to service being declined by a foreign provider. The mobile device 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 mobile device, but also on the voice and data services subscribed to by the user. For example, prepaid phone service may rule 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 may support them.

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 suspect and the incident are both known (e.g., a child-porn investigation). Prepared with the background of the incident, the forensic examiner and analyst may 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}.
- Discover what tools or exploits were used {how}.

In many instances the data is peripheral to an investigation or useful in substantiating or refuting the claims of an individual about some incident. On occasion, direct knowledge,

visited on 12/9/2016

motivation, and intention may be established. Most of the evidence sources from mobile devices are: contact data, call data, messaging, pictures, video, social media, or Internet-related information. User applications potentially provide other evidence sources. User files placed on the device for rendering, viewing, or editing are other important evidence sources. 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. Often times 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. This may allow an examiner to validate their findings as the data obtained from the device may be verified with the data obtained from the service provider.

Enhanced 911: Enhanced 911 (E911) is a technology advanced by the U.S. Federal Communications Commission (FCC) enabling mobile devices to process 911 calls and to provide the geographic location of the handset. Therefore, all U.S. based mobile devices possess the ability to establish cellular voice communication when dialing 911 regardless of their service status (i.e., active, inactive). Additionally, GSM and other UICC dependent devices may also establish cellular voice communication by dialing 911 without the presence of a UICC.

All U.S. based cellular carriers are required to handle calls regardless of the mobile device customer's specific carrier. Under the rules, all mobile devices manufactured for sale in the United States after February 13, 2000, that are capable of operating in an analog mode, including dual-mode and multi-mode handsets, must include this special method for processing 911 calls[22].

In situations where 911 was dialed on a mobile device, the location information (i.e., the latitude and longitude of the device or cell tower) for the call may be of interest to a forensic investigator. Outgoing 911 calls may or may not be logged in the memory of the mobile device or UICC.

6.2 Applying Mobile Device Forensic Tools

Once a copy of the acquisition results are 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 are extremely valuable, since proficient use of the available features and capabilities of a forensic tool can greatly speed the examination process.

It is important to note that forensic tools have the potential 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. Experiments conducted with mobile device forensic tools indicate a prevalence of errors in the formatting

[22] For more information, visit: http://transition.fcc.gov/pshs/services/911-services/enhanced911/archives/factsheet_requirements_012001.pdf.

visited on 12/9/2016

and display of data [Aye11, Jan09]. Therefore, having a high degree of trust and understanding of the tool's ability to perform its function properly is essential. The Computer Forensics Tool Testing (CFTT) project at the National Institute of Standards and Technology (NIST) produces specification, test methods and test reports that provide a foundation for toolmakers to improve tools, users to make informed choices, and provide interested parties with an overview of any anomalies found. CFTT has spent several years researching and testing forensic tools capable of acquiring data from the internal memory of mobile devices and Subscriber Identity Modules (SIMs).

A knowledgeable individual may tamper with device information, such as purposefully modifying a file extension to foil the workings of a tool, altering the date/time of the mobile device to falsify timestamps associated with logged activities, creating false transactions in the memory of the mobile device or its UICC or utilizing 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 minimize errors to achieve the best possible results.

To uncover evidence, specialists should gain a background of the suspect, offense and determine a set of terms for the examination. Search expressions should 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 [DOJ08], 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.

- **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,

visited on 12/9/2016

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 information on incriminating or exculpatory 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 and batch scripts that search for specific types of content (e.g., e-mail addresses, URLs). The greater the tool's capabilities, the more the forensic examiner benefits from experience with and knowledge of the tool.

6.3 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 (CDRs), which are generated by the switch handling an originating call or SMS message from a mobile device. 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 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 C gives an example of the data elements of a CDR, specified in the GSM standards [ETS99]. 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, 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.[23]

[23] For more information, visit: http://info.sen.ca.gov/pub/bill/asm/ab_1301-1350/ab_1305_cfa_20050603_115538_sen_comm.html.

visited on 12/9/2016

For example, CDRs will contain information such as: sender and receiver phone numbers, time and duration of the call, call type (i.e., voice, SMS), etc. CDRs may be obtained from U.S. service providers through their law enforcement point of contact, with the appropriate legal documentation. 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 online law enforcement forums can also be helpful in identifying points of contact and sharing tips on procedures for accurately obtaining the required data.[24]

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
- UICC serial number (ICCID)
- PIN/PUK for the UICC
- 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.

CDRs and other records maintained by the service provider can be requested using subscriber or equipment identifier information seized or acquired from a mobile device or UICC. Subscriber information often used for this purpose includes the IMSI from the UICC and the mobile device number (i.e., MSISDN). Equipment identifiers used are the ESN or IMEI of the phone and the serial number (i.e., ICCID) of the UICC. 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

[24] For more information, visit: http://groups.yahoo.com/group/phoneforensics/ and https://htcc.secport.com/mailman/listinfo/htcc.

visited on 12/9/2016

certain area at a certain time) [Wil03]. 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 device from one or more other mobile devices before a homicide would logically lead to interest in obtaining the records of the caller(s).

CDRs 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]. 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 determine the location of the mobile device at a given time [Oco09]. The analysis can also help to establish timelines and identify possible co-conspirators [Mil08]. 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.

The boundaries of a cell are somewhat variable. 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 an accurate analysis. Tools exist to aid law enforcement in performing cell site analysis and mapping activities independently. In some situations, 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.

Identifying the geographical coverage of specific cells may 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 mobile device 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 UICCs may be swapped among different GSM/UMTS mobile devices.

Careful analysis of the call records in conjunction with other forms of available data may be useful establishing the relationship between the mobile device and its owner. 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 mapping the dat to known associates of a suspect, ownership of such phones is possible to establish. Other traditional forms of forensic evidence (e.g., fingerprinting, DNA) may also be used to establish ownership.

Network traffic information quantifying the amount of data transferred to/from the device is also frequently reported and may aid an investigator in specific investigations.

visited on 12/9/2016

7. 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 data. 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, .csv, .doc, .html, .pdf) 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 [Aye11].

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 data that the automated forensic tool may not have acquired. Video editing software allows still images to be captured for inclusion into the report. Pictures could also be taken of the manual exam using a digital camera; though this process is less efficient and may not document the entire process, it may be the only method available.

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

visited on 12/9/2016

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 [DOJ08]:

- Identity of the reporting agency
- Case identifier or submission number
- Case investigator
- Identity of the submitter
- Date of evidence 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

visited on 12/9/2016

- 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 when custom tools are used for examination or analysis, should it become necessary to reproduce forensic processing results.

visited on 12/9/2016

8. References

The references below are divided into two sections. The first section contains bibliographic citations. The second section contains the URLs that were footnoted throughout the guide.

8.1 Bibliographic Citations

[3GP07] 3GPP (2007), Specification of the Subscriber Identity Module - Mobile Equipment (SIM - ME) interface, 3rd Generation Partnership Project, TS 11.11 V8.14.0 (Release 1999), Technical Specification, (2007-06).

[ACP11] Good Practice and Advice Guide for Managers of e-Crime Investigation, January 2011, <URL: http://www.acpo.police.uk/documents/crime/2011/201103CRIECI14.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>.

[Alz07] Marwan Al-Zarouni, Introduction to Mobile Phone Flasher Devices and Considerations for their Use in Mobile Phone Forensics, Australian Digital Forensics Conference, December 2007, <URL: http://ro.ecu.edu.au/cgi/viewcontent.cgi?article=1015&context=adf>.

[Avi10] Adam J. Aviv, Katherine Gibson, Evan Mossop, Matt Blaze, and Jonathan M. Smith, Smudge Attacks on Smartphone Touch Screens, 4th USENIX Workshop on Offensive Technologies, August 2010, <URL: https://www.usenix.org/legacy/event/woot10/tech/full_papers/Aviv.pdf>.

[Aye11] Rick Ayers, Computer Forensic Tool Testing (CFTT) Program<URL: http://www.cftt.nist.gov/mobile_devices.htm>.

[Aye12] Rick Ayers, Forensics@NIST <URL: http://www.nist.gov/oles/upload/6-Ayers_Richard-Mobile-Device-Tool-Testing.pdf>.

[Bad10] Mona Bader, Ibrahim Baggili, iPhone 3GS Forensics: Logical Analysis using Apple iTunes Backup Utility, Small Scale Digital Device Forensics Journal, Vol. 4, No.1, September 2010, <URL: http://www.ssddfj.org/papers/SSDDFJ_V4_1_Bader_Bagilli.pdf>.

visited on 12/9/2016

[Bel10] Graeme B. Bell, Richard Boddington, Solid State Drives: The Beginning of the End for Current Practice in Digital Forensic Recovery?, The Journal of Digital Forensics Security and Law, Volume 5, Number 3, 2010.

[Bre06] Marcel Breeuwsma, Forensic Imaging of Embedded Systems using JTAG (boundary-scan), Digital Investigation, Volume 3, Issue 1, 2006, pp.32-42.

[Bre07] Marcel Breeuwsma, Martien de Jongh, Coert Klaver, Ronald van der Knijff, Mark Roeloffs, Forensic Data Recovery from Flash Memory, Small Scale Digital Device Forensics Journal, Vol. 1, No. 1, June 2007, <URL: http://www.ssddfj.org/papers/ssddfj_v1_1_breeuwsma_et_al.pdf>.

[Bro08] Sam Brothers, How Cell Phone "Forensic" Tools Actually Work – Cell Phone Tool Leveling System, Mobile Forensic World, Chicago, IL, March, 2008.

[Bro12] Sam Brothers, How Cell Phone Forensics Tools Work, AAFS 2012, Washington, DC.

[Cas11] Eoghan Casey, Benjamin Turnbull, Digital Evidence and Computer Crime, Third Edition, Elsevier Inc., 2011 <URL: http://www.elsevierdirect.com/companions/9780123742681/Chapter_20_Final.pdf >.

[Dan09] Dankar S., Ayers, R., Mislan, R., Hashing Techniques for Mobile Device Forensics, Small Scale Digital Device Forensics Journal, 2009.

[DOJ08] Electronic Crime Scene Investigation: A Guide for First Responders, Second Edition, NCJ 219941, April 2008, <URL: https://www.ncjrs.gov/pdffiles1/nij/219941.pdf>.

[Eld12] Bob Elder, Chip-Off and JTAG Analysis for Mobile Device Forensics, Evidence Technology Magazine, May-June 2012, <URL: http://www.evidencemagazine.com/index.php?option=com_content&task=view&id=922>.

[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.

[Fio09] Salvatore Fiorillo, Theory and practice of flash memory mobile forensics, Australian Digital Forensics Conference, December 2009, <URL: http://ro.ecu.edu.au/cgi/viewcontent.cgi?article=1066&context=adf>.

[For10] Dario Forte, Andrea de Donno, Chapter 10: Mobile Network Investigations, *Handbook of Digital Forensics and Investigation*, Edited by Eoghan Casey, Elsevier Academic Press, 2010.

[Gib02] K. Edward Gibbs, David F. Clark, Chapter 10: Wireless Netowrk Analysis, *Handbook of Digital Forensics and Investigation*, Edited by Eoghan Casey, Academic Press, 2002.

visited on 12/9/2016

[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>.

[Hoo11] Andrew Hoog, Katie Strzempka, 2011, iPhone and iOS Forensics: Investigation, Analysis and Mobile Security for Apple iPhone, iPad and iOS Devices, Elsevier, Jul 25, 2011>.

[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.

[Jan09] Wayne Jansen, Aurélien Delaitre, Mobile Forensic Reference Materials: A Methodology and Reification, NIST Interagency Report IR-7617, October 2009, <URL: http://csrc.nist.gov/publications/nistir/ir7617/nistir-7617.pdf>.

[Jon10] Kevin Jonkers, The forensic use of mobile phone flasher boxes5, digital investigation 6 (2010) 168–178, <URL: http://www.sciencedirect.com>.

[Kat10] Eric Katz, A Field Test of Mobile Phone Shielding Devices, 2010, College of Technology Masters Thesis, Paper 33, <URL: http://docs.lib.purdue.eud/techmasters/33>.

[Kni10] Ronald van der Knijff, Chapter 8: Embedded Systems Analysis, *Handbook of Digital Forensics and Investigation*, Edited by Eoghan Casey, Elsevier Academic Press, 2010.

[Man08] Kevin Mansell, Darren Lole, Fiona Litchfield, Recovering Deleted Data From Fat Partitions Within Mobile Phone Handsets Using Traditional Imaging Techniques, F3 Annual Conference, November 11-13, 2008, <URL: http://www.controlf.net/content/uploads/MANSELL-Imaging-FAT-Partitions-on-Phone-Handsets-Feb-09.pdf>.

[Mcc05] Paul McCarthy, Forensic Analysis of Mobile devices, BS CIS Thesis, University of South Australia, School of Computer and Information Science, Mawson Lakes, October 2005.

visited on 12/9/2016

[Mcc06] Paul McCarthy, Jill Slay, Mobile devices: 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 devices, Digital Investigation, Vol.1, No. 4, 2004, pp. 266-272.

[Mil08] Christa Miller, The other side of mobile forensics, Cygnus Business Media, July 1, 2008, <URL: http://www.officer.com/article/10248785/the-other-side-of-mobile-forensics>.

[Mül12] Tilo Müller, Michael Spreitzenbarth, and Felix C. Freiling, Forensic Recovery of Scrambled Telephones, <URL: http://www1.cs.fau.de/filepool/projects/frost/frost.pdf>.

[Mur13] Cindy Murphy, Developing Process for Mobile Device Forensics, 2013, <URL: http://www.mobileforensicscentral.com/mfc/documents/Mobile Device Forensic Process v3.0.pdf>.

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

[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>.

[Oco09] Terrence P. O'Connor, Provider Side Cell Phone Forensic, Small Scale Digital Device Forensics Journal, Vol. 3, No. 1, June 2009, <URL: http://www.ssddfj.org/papers/SSDDFJ_V3_1_OConnor.pdf>.

[Orm09] By Justin Ormont (Own work) CC-BY-SA-3.0 <URL: http://creativecommons.org/licenses/by-sa/3.0> or GFDL <URL: http://www.gnu.org/copyleft/fdl.html>, via Wikimedia Commons.

[Rei08] Lee Reiber, SIMs and Salsa, MFI Forum, Mobile Forensics, Inc., September 2008.

[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.

[SWG13] SWGDE, SWGDE Best Practices for Mobile Phone Forensics, <URL: https://www.swgde.org/documents/Current%20Documents/2013-02-11%20SWGDE%20Best%20Practices%20for%20Mobile%20Phone%20Examinations%20V2-0>.

visited on 12/9/2016

[Tha10] John (Zeke) Thackray, Flasher Boxes: Back to Basics in Mobile Phone Forensics, Digital Forensic Investigator News, July 13, 2010, <URL: http://www.dfinews.com/article/flasher-boxes-back-basics-mobile-phone-forensics>.

[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.

[Zdz12] Jonathan Zdziarski, iOS Forensic Investigative Methods, 2012, <URL: http://www.zdziarski.com/blog/wp-content/uploads/2013/05/iOS-Forensic-Investigative-Methods.pdf>.

[Zim11] Scott Zimmerman, Dominick Glavach, Cyber Forensics in the Cloud, December 2011, IAnewsletter, Vol 14, No 1, <URL: http://iac.dtic.mil/csiac/download/Vol14_No1.pdf>.

8.2 Footnoted URLs

http://developer.android.com/sdk/index.html

https://developer.apple.com/devcenter/ios/index.action

http://www.3gpp.org/ftp/Specs/html-info/31102.htm

http://www.qualcomm.com/

http://www.radio-electronics.com

http://www.ietf.org/

http://en.wikipedia.org/wiki/Mobile_IP

http://nislab.bu.edu/sc546/sc441Spring2003/mobileIP

http://appleinsider.com/articles/13/05/14/mobile-malware-exploding-but-only-for-android

http://www.scientificamerican.com/article.cfm?id=boston-marathon-bomb-attack

http://mobile.softpedia.com/phoneFinder

http://www.numberingplans.com/?page=analysis&sub=imeinr

visited on 12/9/2016

http://www.tiaonline.org/standards/resources/esn/codes.cfm

http://www.numberingplans.com/?page=analysis&sub=simnr

http://transition.fcc.gov/oet/ea/fccid/

http://www.npac.com/the-npac/access/law-enforcement-agencies-psaps

http://www.fonefinder.net/

http://transition.fcc.gov/pshs/services/911-services/enhanced911/archives/factsheet_requirements_012001.pdf

http://info.sen.ca.gov/pub/bill/asm/ab_1301-1350/ab_1305_cfa_20050603_115538_sen_comm.html

https://htcc.secport.com/mailman/listinfo/htcc

visited on 12/9/2016

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

CDR – Call Detail Record

CF – Compact Flash

CNIC – Cellular Network Isolation Card

CSIM – CDMA Subscriber Identity Module

EDGE – Enhanced Data for GSM Evolution

EMS – Enhanced Messaging Service

ESN – Electronic Serial Number

ETSI – European Telecommunications Standards Institute

eUICC – Embedded Universal Integrated Circuit Card

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

visited on 12/9/2016

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

LND – Last Numbers Dialed

MD5 – Message Digest 5

MEID – Mobile Equipment Identifier

MMC – Multi-Media Card

MMS – Multimedia Messaging Service

MSC – Mobile Switching Center

MSISDN – Mobile Subscriber Integrated Services Digital Network

NFC – Near Field Communication

OS – Operating System

PC – Personal Computer

PC/SC – Personal Computer/Smart Card

PDA – Personal Digital Assistant

PIM – Personal Information Management

PIN – Personal Identification Number

PPI – Pixels Per Inch

POP – Post Office Protocol

RAM – Random Access Memory

ROM – Read Only Memory

SD – Secure Digital

visited on 12/9/2016

SDK – Software Development Kit

SHA1 – Secure Hash Algorithm, version 1

SIM – Subscriber Identity Module

SMS – Short Message Service

SSD – Solid State Drive

TDMA – Time Division Multiple Access

UICC – Universal Integrated Circuit Card

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

visited on 12/9/2016

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 similarly equipped 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 memory storage in a buffer, which can potentially overwrite and corrupt memory beyond the buffer's boundaries.

Cellular Network Isolation Card (CNIC) – A SIM card that isolates the device from cell tower connectivity.

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 any transfers.

Closed Source Operating System – Source code for an operating system is not publically available.

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 makes it unreadable to most programs until the file is uncompressed.

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

CDMA Subscriber Identity Module (CSIM) – CSIM is an application to support CDMA2000 phones that runs on a UICC, with a file structure derived from the R-UIM card.

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.

visited on 12/9/2016

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

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 devices 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; as well as 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.

Feature Phone – A mobile device that primarily provide users with simple voice and text messaging services.

File Signature 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 mobile phone cannot automatically contact, usually because service was declined by a foreign provider.

Forensic Copy – A 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 (GPS) – A system for determining position by comparing radio signals from several satellites.

visited on 12/9/2016

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 a given 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 combines 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 devices.

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.

Key Chords –Specific hardware keys pressed in a particular sequence on a mobile device.

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

Mobile Devices – A mobile device is a small hand-held device that has a display screen with touch input and/or a QWERTY keyboard and may provide users with telephony capabilities. Mobile devices are used interchangeably (phones, tablets) throughout this document.

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.

visited on 12/9/2016

Near Field Communication (NFC) – A form of contactless, close proximity, radio communications based on radio-frequency identification (RFID) technology.

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, as well as 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.

Push-To-Talk (PTT) – A method of communicating on half-duplex communication lines, including two-way radio, using a "walkie-talkie" button to switch from voice reception to transmit mode.

Removable User Identity Module (R-UIM) – A card developed for cdmaOne/CDMA2000 handsets that extends the GSM SIM card to CDMA phones and networks.

Secure Digital eXtended Capacity (SDXC) – Supports cards up to 2 TB, compared to a limit of 32 GB for SDHC cards in the SD 2.0 specification.

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.

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.

visited on 12/9/2016

Universal Integrated Circuit Card – An integrated circuit card that securely stores the international mobile subscriber identity (IMSI) and the related cryptographic key used to identify and authenticate subscribers on mobile devices. A UICC may be referred to as a: SIM, USIM, RUIM or CSIM, and is used interchangeably with those terms.

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.

visited on 12/9/2016

Appendix C. 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 [ETS99]. Table 5 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 5 and a better understanding of the range of records and data involved in network administration.

Table 5: 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

visited on 12/9/2016

Field	Key	Description
Event Time Stamps	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 time stamped – 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

visited on 12/9/2016

Field	Key	Description
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

visited on 12/9/2016

Appendix D. 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 6: Technical Resource Sites

Resource	URL
Digital Evidence and Forensics	http://www.nij.gov/topics/forensics/evidence/digital/
High Tech Crime Consortium mail list	https://htcc.secport.com/mailman/listinfo/htcc
High Tech Crime Consortium	http://www.hightechcrimecops.org/
High Technology Crime Investigation Association	http://www.htcia.org/
Mobile Forensics Central	http://www.mobileforensicscentral.com/mfc/
National Institute of Justice	http://www.nij.gov/topics/forensics/evidence/digital/standards/cftt.htm
Phone Forensics Group	http://groups.yahoo.com/group/phoneforensics/
The Netherlands Forensic Institute's procedures for preservation	http://www.holmes.nl/MPF/FlowChartForensicMobilePhoneExamination.htm
Secure Digital Homepage	http://www.Sdcard.org
Scientific Working Group on Digital Evidence	http://www.swgde.org
Mobile & Technology eDiscovery Blog	http://trewmte.blogspot.com/

Table 7: 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
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