Available for download at
www.JUSTNET.org

CELL PHONE FORENSICS IN A CORRECTIONAL SETTING

GUIDEBOOK

NIJ

NLECTC
Corrections Technology
Center of Excellence

CELL PHONE FORENSICS IN A CORRECTIONAL SETTING

GUIDEBOOK

Prepared for
National Institute of Justice, through the National Law Enforcement and Corrections Technology Center (NLECTC), Corrections Technology Center of Excellence

By John S. Shaffer, Ph.D., Institutional Corrections Program Manager, Corrections Technology Center of Excellence

October 2014

This publication was prepared by the National Law Enforcement and Corrections Technology Center's Corrections Technology Center of Excellence, supported by Cooperative Agreement 2010-IJ-CX-K003 awarded by the U.S. Department of Justice, National Institute of Justice (NIJ). Points of view or opinions contained within this document are those of the authors and do not necessarily represent the official position or policies of the U.S. Department of Justice. Please note that providing information on law enforcement and corrections technology or the mention of specific manufacturers, products or resources does not constitute the endorsement of the U.S. Department of Justice or its component parts. Agencies are encouraged to gather as much information as possible, from multiple sources, and make their own determinations regarding solutions that best fit their particular needs.

TABLE OF CONTENTS

EXHIBITS

FOREWORD

This guidebook was developed by the National Law Enforcement and Corrections Technology Center (NLECTC) System's Corrections Technology Center of Excellence (CoE).

Operated by the University of Denver (DU), the Corrections Technology CoE serves as the authoritative resource within the NLECTC System for both practitioners and developers with respect to technologies that support institutional and community corrections. The Center's position within DU allows it to leverage a wide array of multidisciplinary research units to accomplish its mission.

In its primary role, this CoE assists in the transition of technology from the laboratory into practice by first adopters within the correctional community. Specifically, the Corrections Technology CoE supports NIJ's research, development, test and evaluation activities within the corrections portfolio by:

- Assisting NIJ in identifying practitioner technology requirements by coordinating and conducting Technology Working Groups (TWGs).
- Supporting NIJ research and development programs by assisting with program objective definition and refinement, assessing ongoing NIJ projects, scouting relevant technology efforts and participating in national and regional groups.
- Testing, evaluating and demonstrating technologies by conducting and coordinating operational evaluations and conducting, facilitating and coordinating demonstrations with corrections agencies.
- Supporting the adoption of new technologies by introducing these tools to practitioners, providing practitioner requirements to developers, assisting developers in commercialization and providing support to first adopter agencies for effectiveness evaluation.
- Coordinating and developing technology guidelines for planning, selecting and implementing technology solutions.
- Providing technology assistance and support to corrections agencies on a national basis, including providing science and engineering advice and assisting first adopters with new tools and methods.

To facilitate the development of this guidebook, the Corrections Technology CoE entered into a contract with John S. Shaffer, Ph.D., LLC to act as primary author. Dr. Shaffer, a former executive deputy secretary for the Pennsylvania Department of Corrections, is an independent criminal justice consultant who specializes in matching emerging technology solutions to correctional needs.

A number of subject-matter experts assisted with the preparation of this guidebook, including (in alphabetical order): Sam Brothers, Sterling Bryan, Todd Craig, Mark Farsi, Alex Fox, Dorothy Fox, Jay Miller, Jeff Peterson, Jeff Poling, Joe Russo, Darnell Stewart and Bill Teel.

EXECUTIVE SUMMARY

Cell Phone Forensics in a Correctional Setting Guidebook was developed for the National Institute of Justice (NIJ) based on a recommendation from its Institutional Corrections Technology Working Group (TWG). The TWG, which consists of leaders from correctional agencies across the country, has recognized the growing importance of cell phone forensics as an investigative tool.

This guidebook provides correctional administrators with a brief, yet comprehensive and informative, view of cell phone forensic technologies. It reviews the evolving role of cell phone forensics in correctional institutions and presents issues to consider when acquiring and implementing these technologies. It also addresses the opportunities and challenges involved in selecting technologies and implementing them in correctional settings.

Methodologies

Methodologies used in preparing this guidebook include literature reviews of primary and secondary sources, as well as collecting input from corrections practitioners and technical experts with experience in conducting forensic examinations of confiscated mobile devices. Every attempt has been made to provide references and citations to sources used. URLs are provided as "hot links" when available. This guidebook does not represent original research, but rather, is a review of existing resources.

Chapter Review

The guidebook contains the following chapters:

1. Introduction: Statement of the Problem

This section discusses the reasons that cell phone forensics is becoming an important capability for correctional institutions. The rapid increase in the number of contraband cell phones smuggled into institutions has created the need to be able to forensically examine recovered phones. In general, forensic laboratories are overwhelmed and are not equipped to handle the workload generated by confiscated cell phones.

2. What Agencies Need to Know About Cell Phone Forensics

This section covers the many benefits that can be reaped through a cell phone forensic program, including an understanding of the types of communications that occur through contraband cell phones, intelligence data that can support criminal investigations and understanding linkages between inmates and persons in the community. In addition, the ability to recover data may prove to be a deterrent factor; as more and more inmates are successfully prosecuted using digital forensic evidence, this decreases the likelihood that inmates will bring cell phones into a facility in the first place.

3. Technology

This section covers the technologies currently available to assist agencies in examining contraband cell phones. An overview of each tool's distinguishing features, strengths and weaknesses, and cost will be provided.

4. Establishing a Cell Phone Forensics Capability

This section provides readers with an understanding of the issues they need to consider when establishing a cell phone forensics capability. These issues include the funding needed for start-up and ongoing operations, issues related to procuring technology tools, staff resources required, training requirements (both startup and ongoing) and physical site requirements.

5. Implementation

This section provides an overview of how agencies currently use cell phone forensics. It also gives the reader relevant case examples. Included in this section are legal issues and case law that has emerged, issues relating to law enforcement coordination, how agencies prioritize evidence to prevent backlogs, evidence collection and retention issues, the importance of policies and procedures, lessons learned and success stories.

6. Conclusions

This section summarizes the Guidebook's key points.

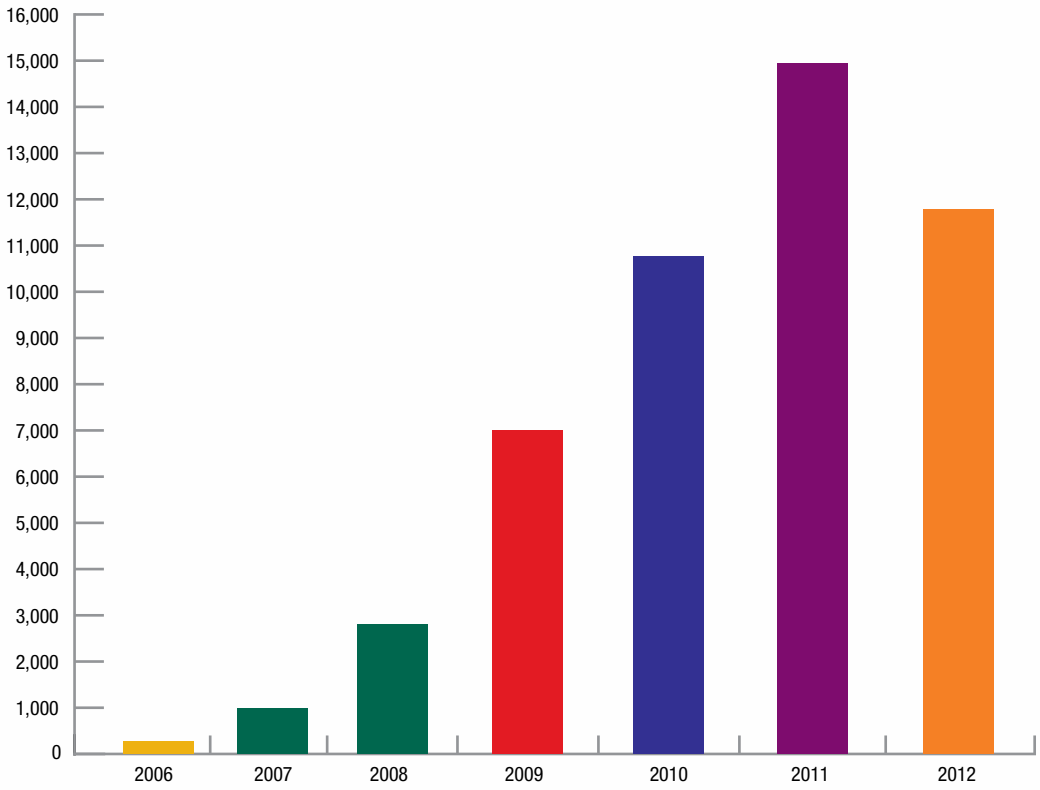
7. Appendixes

Appendix A provides a listing of sample policies and procedures for the operation of an internal cell phone forensics lab and a list of contacts for additional information. Appendix B lists the references used in compiling this guidebook. Appendix C provides a list of the acronyms used in this publication and Appendix D is a glossary of terms.

CHAPTER 1
STATEMENT OF THE PROBLEM

The use of contraband cell phones within jails and prisons is a growing concern among correctional administrators across the country. The California Department of Corrections and Rehabilitation (CDCR) reports confiscating more than 48,000 contraband cell phones between 2006 and 2012 (see Exhibit 1).

Exhibit 1. California Department of Corrections and Rehabilitation Total Cell Phones Found 2006-2012



Source: CDCR, 2013

Other correctional agencies report large and growing numbers of confiscated cell phones. The Maryland Department of Public Safety and Correctional Services (MD PSCS) confiscated 741 phones in 2007, 1,236 in 2008, 1,658 in 2009, 1,128 in 2010 and 1,304 in 2011 (MD PSCS, 2012). The number of phones confiscated by the Federal Bureau of Prisons (BOP) doubled between 2008 and 2010 (California Associated Press, Nov. 21, 2011). The Mississippi Department of Corrections (MDOC) reported finding 930 cell phones in 2007, 2,214 in 2008, 3,597 in 2009 and 4,233 in 2010 (MDOC, 2011).

Several theories have been offered to explain the increasing numbers of contraband cell phones making their way into correctional institutions. Exhibit 2 highlights the most frequently cited reasons.

The increasing number of cell phones in prisons, and the inability to record and monitor cell phone conversations, has resulted in a significant loss of potentially valuable security and law enforcement intelligence. Security threat groups (STGs) operate with impunity when their internal communications networks are secure. MDOC and MD PSCS have reported a significant loss of revenue from their legitimate inmate telephone systems, which they attribute to the increased use of cell phones by inmates. For these reasons, it is a high priority to eradicate contraband cell phones and to conduct a forensic analysis on recovered phones.

Most correctional agencies lack the internal capacity to conduct forensic analysis on a cell phone. They depend on state police and/or FBI electronic crime labs that are often overwhelmed with their own backlogs. Also, time is of the essence when conducting an internal investigation, and in many cases, corrections investigators cannot wait for an external forensic lab to analyze their confiscated devices. Therefore, it is becoming increasingly important for correctional agencies to understand cell phone forensics and to develop the internal capacity to conduct these analyses themselves.

Exhibit 2. Frequently Cited Reasons for the Increase in Contraband Cell Phones

- Inmates Want Cell Phones to Make Calls That Are Less Expensive Than Calls on the Legitimate Inmate Calling System
- Inmates Want to Circumvent the Recording and Monitoring Features on the Legitimate Inmate Calling System So That They Can Pursue Criminal Activities Undetected
- High Value of Contraband Cell Phones ($300 to $1,000) Has Compromised Correctional Staff and Encouraged Some to Smuggle Cell Phones for Profit
- Lax Perimeter and Portal Security Has Made it Easy for Outside Accomplices and Inmates' Visitors to Introduce Contraband Cell Phones
- Many Jurisdictions Lack Legislation That Makes It Illegal to Possess a Cell Phone in Prison
- The Reluctance of Some Prosecutors to Prosecute Contraband Cell Phone Cases Has Minimized the Potential Deterrent Effect of Smuggling

Source: National Institute of Justice Technology Institute for Corrections, Annapolis, Md., August 2013

CHAPTER 2

WHAT AGENCIES NEED TO KNOW ABOUT CELL PHONE FORENSICS

According to the corrections practitioners who participated in the 2013 Technology Institute for Corrections, sponsored by the National Institute of Justice (NIJ), they believe the majority of inmate telephone calls on contraband cell phones are conducted for relatively benign purposes. These practitioners, representing state and large county correctional agencies from across the country, contend that most calls connect inmates with their families and friends, and are motivated more by the lower cost of cell phone calls than a desire to commit some illicit activity.

Another motivation for inmates to have cell phones is simply for convenience and privacy. Most agencies turn their legitimate telephone system off at night. When an inmate has a contraband cell phone, he/she can make calls at any time of the day or night from the relative privacy of his/her cell. But, even if calls are made for benign purposes, all calls conducted on contraband cell phones circumvent the recording and monitoring features of the legitimate inmate telephone systems, and they reduce the commissions that would otherwise accrue to the agencies. In jurisdictions where it is illegal for inmates to possess a cell phone, even benign calls constitute a criminal offense.

Although most calls may be for benign purposes, the primary focus of cell phone forensics is to identify and prosecute illegal activities conducted via contraband cell phones. Exhibit 3 lists the types of illegal communications that occur through contraband cell phones.

After a contraband cell phone is recovered, a forensic analysis may reveal a significant amount of intelligence about calls made with the device. The call detail records indicate the telephone numbers of all incoming and outgoing calls, as well as all text messages. The inmate's contacts list will reveal the names and contact information for his/her associates. Photographs and videos may also provide important clues for law enforcement. This data can be analyzed in context with other data sources (e.g., inmate accounting transactions, visiting records) to enable investigators to "follow the money" and identify STG affiliations and other criminal associations.

Exhibit 3. Illegal Communications That Occur Through Contraband Cell Phones

- Coordination of Escape Attempts and/or Contraband Smuggling With Co-Conspirators
- Coordination of Intra- and Inter-Institution Disturbances With Other Inmates
- Orchestration of Criminal Enterprises With Co-Conspirators on the Outside
- Intimidation of Witnesses
- Harassment of Victims
- Inappropriate Fraternization Between Staff and Inmates
- Unauthorized Communication Between Inmates
- Orchestration of Contract "Hits" on Victims in the Community
- Distribution of Child Pornography
- Threats to Public Officials (Legislators, Judges, etc.)

There are documented cases that directly link contraband cell phones with escape plans, threats to public officials, witness intimidation and contract "hits" (see Exhibit 4).

The inability to record and monitor cell phone communications results in the loss of potentially valuable security and law enforcement intelligence. Although it is generally illegal to monitor cell phone voice conversations without a court order, there is still a great deal of intelligence available through a forensic analysis of the data residing on a recovered cell phone. Other data sources can be mined for evidence of illegal activity. This intelligence data can support criminal investigations by understanding the linkages between inmates and persons in the community. Some practitioners subscribe to the "paperweight theory" (i.e., terminate the calling feature either through a jamming or managed access system and render the cell phone into a useless "paperweight.") It is likely that proponents of the paperweight theory do not understand the capabilities of the technology or the continuing threat to security that cell phones pose if they are not confiscated. Cell phones, in the hands of an inmate, can still be used as a camera, a video recorder, a word processor and/or a local text messaging hotspot, even when the signal to the cell phone tower is interrupted. Even without voice call functionality, cell phones can still be used for nefarious purposes, and can still yield a significant amount of security intelligence when forensically analyzed.

In addition, the ability to quickly recover data and take appropriate action may prove to be a deterrent factor. As more persons are prosecuted for criminal activity linked to contraband cell phones, the likelihood that people will smuggle cell phones into a facility in the first place should decrease.

Exhibit 4. Documented Adverse Events Perpetrated by Inmates With Contraband Cell Phones

Adverse Event	State	Date	Summary and Link
Threats to a Public Official	Texas	2008	An inmate housed on death row used a cell phone to threaten Texas State Sen. John Whitmire. See link to further details: http://usatoday30.usatoday.com/news/nation/2008-10-21-inmate-senator-threats_N.htm
Contract "Hit"	S.C.	2010	Capt. Robert Johnson of the South Carolina Department of Corrections was shot six times at point-blank range at the front door of his own home by a would-be assassin. He survived. The shooting was an alleged contract hit ordered by an inmate using a contraband cell phone. See link to further details: http://www.postandcourier.com/article/20130707/PC16/130709568/1009/cellular-providers-not-liable-in-shooting-of-sumter-prison-official-judge-rules&source=RSS
Contract "Hit"	Md.	2007	A Maryland inmate used a contraband cell phone to order the murder of a witness. The inmate was later convicted and sentenced to life without parole. See link to further details: http://www.atf.gov/press/releases/2009/05/050409-balt-byers-sentenced-on-murder-order.html
Contract "Hit"	N.J.	2005	This New Jersey case involves an inmate who used a cell phone to order a hit on his ex-girlfriend, who was to be a witness for the prosecution in an upcoming case. See link to further details: http://www.correctionsone.com/contraband/articles/2081385-NJ-inmate-used-cell-phone-to-order-girl
Witness Intimidation	Ore.	2011	This Oregon case describes an inmate's use of social media to intimidate his ex-wife. See link to further details: http://www.edgeboston.com/technology/personal_tech///126999/inmates_harras_victims_via_facebook
Witness Intimidation	D.C.	2012	This Washington, D.C., report describes an inmate's use of social media to intimidate multiple witnesses. See link to further details: http://www.examiner.com/article/social-media-from-behind-bars
Inmate Escape	Kan.	2008	A prison volunteer in Kansas smuggles a cell phone in to an inmate and coordinates an escape. See link to further details: http://online.wsj.com/article/SB120251542094755135.html
Inmate Escape	Ariz.	2010	Three Arizona inmates coordinated an escape with a cell phone. See link to further details: http://www.reviewjournal.com/news/suspect-escape-threw-guns-arizona-prison-report-says?ref=814
Coordination of Inter-Institution Events	Ga.	2010	Inmates in Georgia used cell phones to coordinate a multi-facility protest over prison conditions. See link to further details: http://www.ajc.com/news/news/local/prisoners-protest-over-for-now/nQnxt/

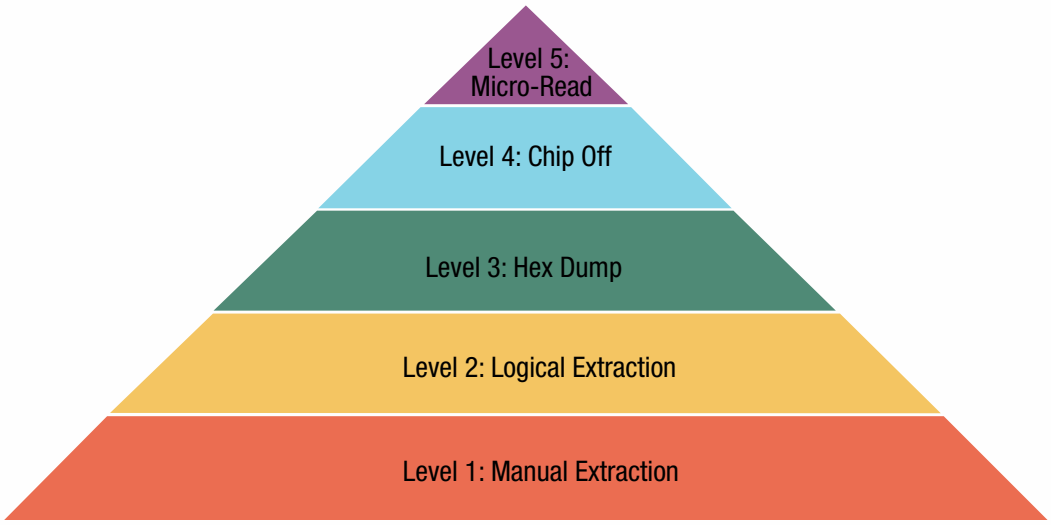
CHAPTER 3
TECHNOLOGY

There are multiple solutions available to assist agencies in the forensic examination of contraband cell phones. The National Institute of Standards and Technology (NIST) published a comprehensive report that provides an overview of each tool's distinguishing features, strengths and weaknesses titled *Cell Phone Forensic Tools: An Overview and Analysis* (NISTIR 7250, October 2005, available at http://csrc.nist.gov/publications/nistir/nistir-7250.pdf)

Since publication of the 2005 NIST Overview, there has been a great deal of software development progress. Ten years ago, most forensic tools typically supported only a limited number of cell phone devices. Now, most tools support most devices.

An important resource that reflects the current state of the discipline as of this writing was published by NIST in May 2014. *Guidelines on Mobile Device Forensics,* NIST Special Publication 800-101 Revision 1

Exhibit 5. Mobile Forensic Tool Classification



(e.g., Level 1: Manual Extraction through Level 5: Micro-Read)

was prepared to help the digital forensics community stay abreast of the latest technologies and provides basic information on mobile forensics tools and the preservation, acquisition, examination and analysis, and reporting of digital evidence present on mobile devices. (See http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-101r1.pdf).

Understanding the method by which a tool extracts data from a given mobile device can be best explained by the Mobile Device Forensics Tool Classification System developed in 2008 by Sam Brothers, a digital forensic specialist at the U.S. Customs and Border Protection Agency. Brothers' pyramid is a classification system used as a framework for forensic examiners to compare different mobile forensic tools. The objective of the tool classification system is to enable examiners to classify mobile device forensic tools based on their extraction method. Exhibit 5 illustrates the five different levels of the mobile forensics tool classification system. These links are provided for informational purposes only. (Examples of various forensic tools are provided for each level of the classification system. Appendix B provides links to websites for these tools. Please note that NIJ does not endorse any specific product.)

The classification system begins at the bottom with Manual Extraction (Level 1). Tools at this level function by recording (usually through the use of a digital camera) the information viewable on the screen of the mobile device. These tools are fairly straightforward in their use as the examiner simply uses the input feature of the mobile device (e.g., keyboard or touch screen) to view the data stored on the mobile device. Tools that function at this level lack the ability to recover deleted information (e.g., deleted call log entries) as this data is inaccessible though the menu system. Examples of Level I tools are Fernico's ZRT2 HD and Ramsey's STE-3000FAV.

Logical Extractions are next at Level 2. These tools function by using a variety of protocols to communicate with the operating system of the device through a series of commands. This communication is facilitated through a cable connected between the mobile device and the examiner's computer. This method allows the examiner to extract data from a device more quickly than manual methods, however, access to some data (e.g., unallocated space) is impossible. Examples of Level 2 tools are FinalMobile Forensics and Susteen's Secure-View3.

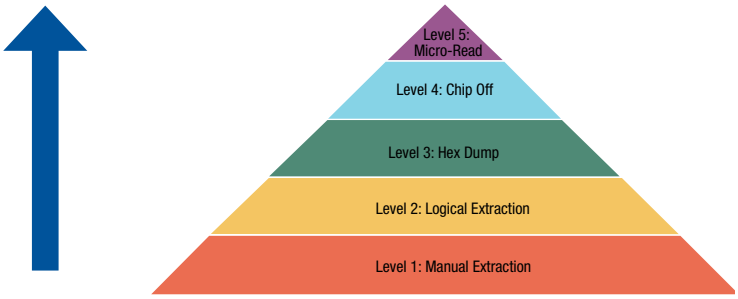
Tools that function at Level 3 are referred to as Hex Dumping tools. Level 3 begins to permit access to unallocated space through the use of joint test action group (JTAG) connections and flasher boxes. JTAG is a diagnostic connector present on many mobile devices and accessible through the main circuit board. Tools at this level function by communicating from the examiner's computer with the use of a flasher box. The flasher box is also connected to the mobile device through either a JTAG connection or through the data cable port of the mobile device. Flasher boxes communicate directly with the memory of the mobile device, bypassing the operating system altogether. The phone must be started using an external or non-device resident start-up program instead of the phone's firmware. These devices are known as boot loaders. Most boot loaders are programmed independently of phone manufacturers and are not tested, vetted or supported by the manufacturers. Improperly configured or improperly used boot loaders can irreversibly damage a phone. Examples of Level 3 tools are CelleBrite's UFED Touch Ultimate and MicroSystemation's XRY Complete.

The next level is Chip Off (Level 4). Chip Off involves removal of the Negated AND or NOT AND (NAND) or Negated OR (NOR) chip(s), which are the digital logic gates of a mobile device. The memory is then read by placing the chip in an electrically erasable programmable read-only memory (EEPROM) reader. Once read, the data (a binary dump) is interpreted and sorted either manually or through the use of automated tools. This method may provide a very holistic view of the information stored in the device and enables the examiner to review all information stored on the chip. Interpretation of the data is difficult and can be very time consuming. Often, the examiner is required to reverse-engineer much of the data manually, and once completed, the resultant recovery process is often only valuable on a per-mobile-device basis. Examples of Level 4 tools are Jingtian Electronic's UPNP 828 and Soft Center's Flash Extractor.

Finally, there is Micro Read (Level 5). This is where the chip is removed and a portion of the chip is then read by carefully removing the top layers of silicon. Once removed, the gates are read one at a time and the binary data is converted to hex. The resulting hex can then be converted to data blocks. This is a delicate process and the most time-consuming method known. Commercial tools are not available at this level and there are very few practitioners performing this type of

Exhibit 6. Tool Classification – Going Up

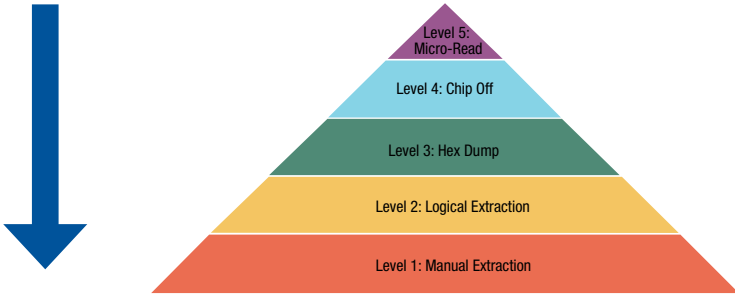
- More technical
- Longer analysis times
- More training required
- More invasive



*Cost is not proportional

Exhibit 7. Tool Classification – Going Down

- Less technical
- Shorter analysis times
- Less training required
- Less invasive



*Cost is not proportional

work. Examples of Level 5 tools are ERSA's IR 550 and Hitachi's S-450 SEM.

Tools may provide functionality at more than one level. For example, CelleBrite's UFED Touch performs logical data extractions at Level 2 for many mobile devices and also offers physical extractions for some devices as well. Another example of this dual functionality is MicroSystemation's XRY Complete product.

As one moves up through the pyramid, techniques are more technical, take longer and require more training. As one moves down through the pyramid, the inverse is generally true. However, the cost of extracting data is not reduced proportionately as one moves down the tool classification levels see Exhibit 7.

The five-level pyramid classification schema that was developed by Sam Brothers (2008) is just one model. Another source (Teel Technologies, 2013) suggests that there are basically four options for data recovery (see Exhibit 8).

Exhibit 8. Options for Data Recovery

1. Screen Captures: The simplest way. Uses a camera to take pictures of what's on the screen. Reporting tools available. Sometimes this is the only way.

   Example – When a phone cannot be examined using a commercial forensic tool (due to lack of support for the device, the communication port is turned off, etc.) and the examiner would like to create a report of data on the device that is viewable, a screen capture solution can be used. This can be done with a standard camera or a dedicated commercial tool that is typically comprised of a camera or web cam, and reporting software. Captured images or videos are recorded and formatted in a report for the examiner to analyze and distribute accordingly. Data acquired can be anything presented on the screen, including text messages, phone books, call logs, pictures, videos and more. Deleted data cannot be recovered by screen captures alone.

2. Logical and File System Analysis: Extracting the data on a device that is viewable, as well as in some devices, the file system. On modern smartphones, some deleted data can be recovered from the file system.

   Example – The forensic software, typically using AT Commands, requests data from the device, which the device delivers and keeps available for the examiner to view and create a report. Data delivered can range from simple phone model info to complete phonebooks, call logs, text messages, pictures, app data, etc. From some devices, file system data can be recovered, which can contain deleted data in some current smartphones.

3. Physical Analysis: The practice of extracting data from the internal memory and removable memory of the device. Contains deleted data.

   Example – Using commercial forensic tools, the examiner can access the internal memory of the device through the communication port and acquire an image of the memory for analysis. Some forensic tools will decode the data and present it in a readable format, or a raw data dump is acquired and requires manual decoding and/or carving for target information. From such a physical acquisition, the logical and file system data is recovered. A physical analysis will recover all of the data available in a logical analysis, plus any data that has been deleted from the device.

4. JTAG and Chip-level Analysis: Analysis of the memory chips in the phone by accessing through JTAG ports or removing them from the device and probing them for data.

   Example – In many instances of pattern-locked Androids, the JTAG process is used to acquire a data dump from memory and acquire the pattern lock code from the data. Once the lock pattern is decoded, it can be entered into the phone for unlocking. A non-destructive process, the JTAG technique enables an examiner to access the memory by disassembling the phone and either attaching an adapter (JIG) to the device's JTAG ports (taps) or soldering to them, and using a hardware/software tool to acquire the data from memory. The phone is functional on reassembly. In addition to pattern-locks and other PIN code security, the complete memory of the device is recovered, and includes the aforementioned data acquired using both the logical and physical acquisition techniques.

   In the instance of a chip off, the examiner disassembles and removes the memory chip from the device's circuit board. The chip is read using a combination of a specific adapter that accommodates the chip, as well as a chip-reading tool with software. This is a destructive process and the device is rendered inoperable. Like above with JTAG, the complete memory of the device is recovered, and includes data acquired using both the logical and physical acquisition techniques. In both JTAG and chip off, the resulting data is a raw data dump that can either be imported into forensic software tools that will decode, or manually decode, as required.

Source: Teel Technologies, 2013.

The same type of data can be extracted from contraband cell phones whether one adheres to the Brothers (2008) or the Teel (2103) model. Both models simply demonstrate that there are varying levels of complexity that must be considered by cell phone forensics analysts when attempting to maximize the amount of intelligence that can be extracted from the devices being examined.

CHAPTER 4

ESTABLISHING A CELL PHONE FORENSICS CAPABILITY

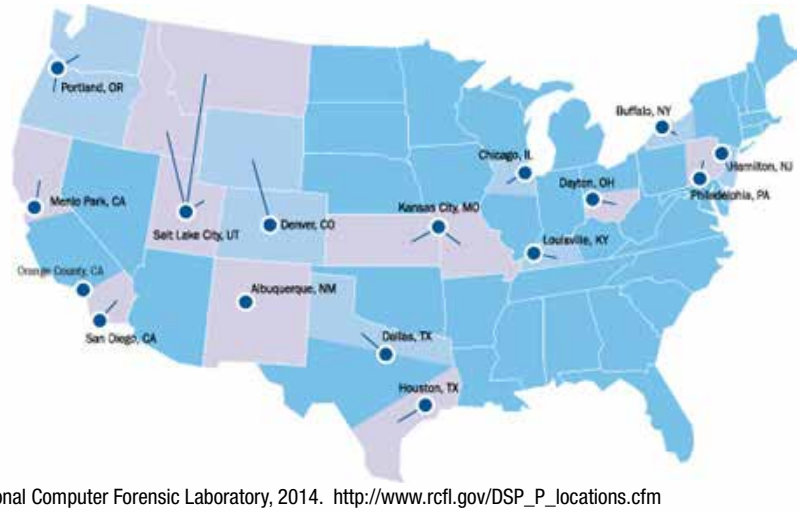
This section will provide readers with an understanding of the issues they need to consider when establishing a cell phone forensics capability. These issues include assessing resource needs based on historical and projected data, the funding needed for start-up and ongoing operations, issues related to procuring technology tools, staff resources required, training requirements and physical site requirements.

Assessing Resource Needs Based on Historical and Projected Data

The historical volume of confiscated cell phones provides a good baseline from which to project the size and scope of an agency's internal cell phone forensic lab. It may very well be that, based on historical assessment, an agency may decide that it does not have the volume of contraband devices sufficient to warrant the investment in an internal lab. The agency may enjoy an established relationship with the local state police or a nearby Federal Bureau of Investigation (FBI) forensic lab and thus have no difficulty in obtaining data recovery services on request.

The FBI maintains a national network of 16 full-service digital forensics laboratories and training centers known as Regional Computer Forensics Laboratories (RCFLs; see Exhibit 9).

Exhibit 9. Map of Regional Computer Forensics Laboratory Locations



Source: Regional Computer Forensic Laboratory, 2014. http://www.rcfl.gov/DSP_P_locations.cfm

RCFLs provide objective digital forensics expertise and services to law enforcement and are devoted to the examination of digital evidence in support of federal, state and local criminal, and national security investigations. In addition to providing digital forensics expertise, the RCFLs train local law enforcement in various digital forensics techniques in their state-of-the-art classrooms. The laboratories also feature cell phone investigative kiosks that law enforcement may use to examine mobile phones and other handheld devices (http://www.rcfl.gov/downloads/documents/CPIK_Brochure.pdf), along with loose media kiosks to review evidentiary data on, for example, USB devices and CD/DVDs. Some practitioners report that the RCFLs have backlogs that result in delays of approximately six months from the time a device is submitted until a report is provided. For more information about the RCFL program, visit www.rcfl.gov.

If the demand for service cannot be met by external support agencies, then it may be necessary to establish an internal forensic lab. Agencies must consider that it can take anywhere from several hours to several days to conduct a forensic examination of a cellular device, depending on the amount of data that it has stored. Expert analysts suggest that, on average, 16 hours should be allocated for each device to be examined, which includes the time required to complete a written report. Using that metric, it is a fairly simple process to project the number of labor hours needed to address the expected workload. It is, of course, possible to conduct simultaneous analyses on multiple devices using different forensic tools. While the data downloads, the forensic examiner can be productively engaged in analyzing data from another device or writing reports.

Clearly, the backlog of devices in hand must also be considered. It will likely be necessary to prioritize the work based on active cases and ongoing investigations. Unless the forensic examiners are dedicated full time to this work, it will be necessary to realistically evaluate how much of their workday can be allocated to this task.

Another factor to consider would be the anticipated increase in cell phones found if the agency recently installed, or soon plans to install, a cell phone detection/location or managed access system. Or perhaps the agency recently implemented, or plans to implement, other cell phone interdiction initiatives (e.g., enhanced perimeter/portal security procedures, K-9s trained to sniff for cell phones, hand-held/portable cell phone detection devices or concealed contraband detection solutions). These variables will make it difficult to project the scope of the problem, but it would be reasonable to assume that the number of phones found will initially increase with focused efforts before eventually tapering off. Even if the number of phones decreases, it will likely never reach zero. Therefore, the need for forensic capacity remains.

Funding Needed for Start-up and Ongoing Operations

The amount of funding needed for start-up and ongoing operations will be driven by the requested number of investigative and support personnel (salaries and benefits), and the hardware and software acquisition costs.

For an initial investment of approximately $20,000 to $30,000, an agency can purchase the required hardware and software for a single-user station forensic lab. Due to the rapidly evolving technology, there will be additional training costs that must be factored into the training budget. Any secure office space can be used for the lab; however, it is absolutely essential to restrict, control and document access to the lab to ensure appropriate chain of custody over the confiscated devices. Once the start-up lab is established, it can be expanded as required. If an existing staff person is assigned (either part time or full time) to the lab, there will be no increase in personnel costs.

As an alternative to a dedicated forensic lab, agencies may consider purchasing a portable mobile field kit (price range: $3,500-$6,500) and training an analyst to operate it. Exhibit 10 shows a photograph of a typical mobile field kit. There are other manufacturers that make similar portable devices. These devices can be taken onsite where analysts can examine confiscated devices in the field.

Issues Related to Procuring Technology Tools

As noted in Chapter 3, no single technology tool will have the capacity to analyze every confiscated device. Due to budget constraints, it will likely be necessary to procure hardware and software using an incremental approach. That is to say, procure tools that will work on

Exhibit 10. Photograph of Example Mobile Field Kit

Source: Teel Technologies, Inc., 2013

Exhibit 11. Photograph of Cellebrite Device

Source: Courtesy of Jeffrey Poling, NJ DOC, 2013.

the majority of the devices found, and address the outliers on an as-needed basis. Agencies should monitor the types of phones recovered most often and procure the appropriate tools. High-priority or high-complexity examinations that cannot be conducted inhouse may have to be referred to the local state police or RCFL until such time that the agency can budget for additional technology resources and training.

Below is a list of some proven technology solutions currently deployed. Most are "plug 'n' play" solutions that enable even a novice examiner to extract meaningful data with little or no training. Where possible, a brief description of the product, cost (if available and as of the date of publication), and a link to further information are provided. **Note: Neither NIJ nor NLECTC endorses any specific product. These listings are presented for informational purposes only.**

Software/Hardware

Cellebrite UFED Touch: Hardware/software device for extracting physical and logical data from phones. http://www.cellebrite.com/mobile-forensic-products.html

Cellebrite offers different packages. The Ultimate Standard Package performs physical extractions (permitting recovery of deleted data) and allows for data carving. This device also images and extracts file systems that can be imported into forensic software for further carving/searching. Pricing for the Ultimate Standard Package runs approximately $10,000, with optional annual maintenance and upgrade fees of up to $2,000. See Exhibit 11 for a photograph of a Cellebrite device.

Katana Lantern: Software to image, carve/analyze and report for all iOS, OSX and Android platforms. http://katanaforensics.com/

Used mostly for iPhones and iPads. The image it generates can be brought into forensic software for further analysis. Must be run from a MAC operating system. Pricing is $745 per license, with optional annual maintenance of $300.

BK Forensics CPA SIM Analyzer Pro: Analyze and/or clone SIM cards. Must purchase blank SIM cards in order to use the SIM cloning features. http://www.bkforensics.com/sim-analyzer.html

Price is $149.95 for law enforcement edition, which includes software, blank SIM card and a reader.

Paraben Device Seizure: Analyzes and reports on data for numerous phones. http://www.paraben.com/device-seizure.html

Pricing for software and hardware package is $1,795. Optional annual maintenance is $360.

Forensic Card Reader and Writer: Used for forensic acquisition of information found on multimedia and memory cards (e.g., the microSD cards within mobile phones). These cards often contain significant information; they are used for storage and also as RAM. These readers will protect data integrity and allow for acquisition in order to conduct a full analysis. Once an image is acquired, it can be imported to forensic software for a full analysis. Able to recover deleted photos, deleted contacts and Internet history from the memory cards.

http://www.digitalintelligence.com/products/forensic_card_reader/

Prices vary; current cost is $80.

Access Data FTK Forensic Toolkit (FTK): http://www.accessdata.com

Guidance Software EnCase: http://www.guidancesoftware.com/encase-forensic.htm

Both FTK and EnCase allow an analyst to examine the output of most acquired images generated by the previously mentioned devices, as well as image and examine flash memory, hard drives, CD/DVDs, USB drives and so on. These are standard programs used throughout the industry. Each one is approximately $2,995 per license, not including the annual maintenance. FTK requires additional training and specific/enhanced hardware requirements for the machine running it.

Photo Documenting

Certain phones will not be able to undergo data extraction no matter what software is used. This may be due to damage to the device or to the phone's hardware/software or firmware limitations. In this event, an analyst conducts a scroll analysis and digitally photographs each screen displayed. This can be done with any digital camera make/model that has a zoom option allowing it to take a clear picture of the screen.

Paraben Project-a-Phone. Digital camera and reporting software that can capture data from a phone from which an analyst cannot capture data in any other way. Details on this digital camera with a mounting system can be found at http://www.projectaphone.com/. Paraben offers two versions. The more expensive version has an easier-to-use mounting system with a better camera. Project-A-Phone ICD-8000 sells for $395 and Project-A-Phone Flex, for $495.

Other products. There are other cellular forensic examination products on the market. **The information presented herein is not intended to be an all-inclusive or exhaustive list. Neither NIJ nor NLECTC makes any endorsements express or implied about any product.**

Oxygen Forensic Suite: http://www.oxygen-forensic.com/en/

XRY: http://www.msab.com/xry/xry-current-version

CellXtract: http://www.logicube.com/shop/cellxtract/

Tarantula (Chinese chipset phones): http://edecdf.com/products?iProdId=3

NIST has evaluated many of these forensic tools. A list of recent reports is available online at http://www.cftt.nist.gov/mobile_devices.htm

Clearly, there are many technical solutions on the market. The technology is rapidly developing and evolving. For a relatively small initial investment, an agency can procure the hardware and software required to extract forensic data from cellular devices. The greater cost lies in human resources and ongoing training.

Staff Resources Required

In addition to determining the number of staff resources necessary to stand up a new cell phone forensics lab, it will be necessary to consider the type of experience and training needed. Obviously, forensic examiners should have some familiarity with technology, and they should also have some demonstrated experience conducting investigations. Unless an agency is fortunate enough to have individuals with both skill sets, it may be necessary to have separate staff to handle the technology and investigative components. Some forensic analysts contend that it is easier to train a good investigator how to use the forensic examination tools than it is to train a good computer analyst how to conduct criminal investigations.

One veteran trainer who teaches classes for law enforcement, military and private investigators noted that, "In most cases, cell phone forensic analysts are assigned to investigative departments and assume the task of analyzing cell phones that were confiscated at a crime scenes. Most of the students have good but basic computer skills; some are computer forensic analysts and have advanced computer skills. Rarely do we get students that actually have an IT background. The IT background deals with networks where a computer science background would be more in line with forensic investigators. However, the majority of cell phone analysts are LE investigators and are self trained on the forensic tool that their agency uses (Cellebrite or XRY). They come to our classes to become certified on various forensic tools and techniques. In a Cellebrite class of

15 students, five students have never used the tool, five have used it some and five are very proficient with the tool. The minimum proficiency for cell phone forensic analysts should be that they need to be self motivated and dedicated to learning as much as possible about their new craft. This is an extremely dynamic field of science and requires continual research and creativity to keep up with the technology. The best analysts don't always have a computer science degree, but they are self motivated and have an internal desire to learn how to recover the evidence from the phone. ... (T)his is a dynamic field and requires continual education. This means that every year there should a budget set aside for training. This will ensure that the analysts continue to hone their skills and will be able to keep up with the advances and challenges of cell phone forensics. So many times I have heard that someone's agency doesn't fund advanced training for the analysts and they become stagnant and frustrated." (S. Bryan, 2014)

The number of staff resources required will depend on the anticipated workload. A single person with both technical and investigatory skills may be sufficient for an initial startup. Other investigative staff may support the cell phone forensic analyst as required. Due to the rapidly evolving nature of the technology, staff must be afforded the time and opportunity for ongoing training.

Training Requirements

An examiner should have intermediate to advanced IT skills. A computer forensics background would be an ideal asset for a digital forensics examiner. Candidates should, at a minimum, complete an introductory course in computer forensics and the vendor-specific training provided with the hardware/software package purchased. RCFLs provide training and certification. In order to access an RCFL Cell Phone Investigative Kiosk (CPIK), users must complete a one-time, hour-long training course (http://www.rcfl.gov/DSP_P_CellKiosk.cfm). These kiosks are not compatible with all makes and models of cellular devices. Additionally, kiosks are intended to function as a preview tool, extracting only a limited amount of data from a cell phone. A full examination from a certified examiner will generally yield additional data not available from the initial kiosk analysis.

The FBI does offer additional training and certifications for qualified personnel (http://www.rcfl.gov/DSP_T_CoursesLE.cfm). The FBI has also produced a series of webinars that are available to authorized personnel (http://www.rcfl.gov/DSP_top2products.cfm). Additional information about FBI training programs is available by contacting the nearest RCFL administrator (http://www.rcfl.gov/DSP_P_CellKiosk.cfm#cellkioskcontact).

The private companies listed below provide training for forensic examiners. **Note that this list is not necessarily all-inclusive, and no specific course is endorsed by NIJ or NLECTC.**

http://www.cellebritelearningcenter.com/ (Cellebrite)

https://www.msab.com
(Micro Systemation XRY)

http://mobileforensicsinc.com/ (Mobile Forensics)

http://www.bkforensics.com/training-1.html
(BKForensics)

http://www.nw3c.org/training
(National White Collar Crime Center - free courses – law enforcement only)

http://teeltech.com/tt3/training.asp (Teel Technologies - advanced training courses)

Some other useful websites that offer excellent resources are listed below. Note that some of these sites require registration. These sites allow users to post questions to the forensic expert community.

http://www.mobileforensicscentral.com/mfc/

http://www.phonenews.com/phone-encyclopedia/

http://www.numberingplans.com/

http://mobileforensics.wordpress.com/

http://www.phonescoop.com/

Joining technology listserv groups is also recommended as they give forensic analysts access to numerous helpful examiners. See the listservs group websites below:

http://forum.mobileforensicsinc.com/

Organizations such as the High Technology Crime Investigation Association (HTCIA) and the Scientific

Working Group on Digital Evidence (SWGDE) provide important resources to members. These organizations help promote collaboration and education for members of the forensics investigation community. See the websites below for membership information.

http://www.htcia.org

https://www.swgde.org/

Physical Site Requirements

It is important to have a secure location of sufficient size to accommodate the number of assigned personnel, as well as to store and catalog confiscated devices. The storage site must have controlled access and be sufficient to maintain appropriate chain-of-custody controls and evidence retention requirements. Typical start-up costs for the hardware, software, furnishings and equipment for a basic forensic workstation can run in the $20,000 to $30,000 range.

More sophisticated workstations, capable of performing all five levels of analysis described above (see Exhibit 5), obviously require more space and more money. Exhibit 12 features a photograph of a more sophisticated forensic examination work station. Typical start-up costs for the hardware, software, furnishings and equipment for a more sophisticated forensic workstation can run in the $35,000 to $50,000 range.

Faraday shielding is designed to block all incoming and outgoing radio frequency (RF) signals so that potential evidence stored on a device cannot be altered while it is in the possession of the authorities. It is generally not required to retrofit a room with Faraday shielding to prevent a seized cellular device from communicating with its network. Instead, most agencies use phone evidence RF bags. Exhibit 13 features a photograph of typical RF bags (cost: approximately $15 each).

There are portable RF blocking tents on the market. Exhibit 14 shows a photograph of a typical portable RF Blocking Tent (cost: approximately $3,500 each).

This link to a YouTube video illustrates how the portable RF Blocking Tent is assembled (39 sec.): http://www.youtube.com/watch?v=iCtXZLOjpo4

Exhibit 12. Sophisticated Forensic Examination Workstation

Photo courtesy of Sterling Bryan, Teel Technologies, 2013

Exhibit 13. Photograph of Typical RF Bags

Source: BK Forensics, 2013. http://www.bkforensics.com/rfsolutions.html

Exhibit 14. Photograph of Typical Portable RF Blocking Tent

Source: BK Forensics, 2013. http://www.bkforensics.com/rfsolutions.html

Exhibit 15 features a photograph of a typical tabletop RF blocking tent.

The Ramsey STE3000FAV is a new forensics shield enclosure (http://www.ramseytest.com/product.php?pid=22). It is also possible to construct an entire room capable of blocking RF signals with readily available Faraday shielding materials, but it is generally not necessary to do so.

Once the decision is made to establish an in-house cellular device forensics lab, and the required funding is in place based on the considerations set forth above, the agency is ready to enter the implementation phase outlined in the next chapter.

Exhibit 15. Tabletop RF Blocking Tent

Source: Paraben, 2013. http://www.paraben.com/tabletop-stronghold.html

CHAPTER 5
IMPLEMENTATION

This section provides an overview of how agencies currently use cell phone forensics and offers relevant case examples. It includes legal issues and case law that has emerged, issues relating to law enforcement coordination, how agencies prioritize evidence to prevent backlogs, evidence collection and retention issues, the importance of policies and procedures, and lessons learned and success stories.

Legal Issues and Case Law

Each jurisdiction has its own laws governing prison contraband and whether or not a court order is required to conduct a forensic analysis on a confiscated wireless device. These laws are evolving; please consult with the appropriate legal counsel for your agency or jurisdiction for specific legal advice.

Exhibit 16 highlights some frequently asked questions about the legalities of confiscating cell phones and analyzing the data that resides on the device. **Nothing contained herein should be construed as legal advice that is sanctioned by NIJ or NLECTC.**

Law Enforcement Coordination

A close working relationship with local law enforcement and the District Attorney (DA) is required in order to successfully prosecute cases involving information extracted from confiscated wireless devices. The DA must be assured that the data was properly extracted and that there is sufficient evidence to support a successful prosecution.

Exhibit 16. Frequently Asked Questions

1. **When is a court order required to confiscate a cell phone?**

- A court order is **not** required to confiscate a cell phone in the possession of an inmate. It is a violation of prison regulations (and in some jurisdictions, a violation of law) for an inmate to have a cell phone, and it can be confiscated as contraband.
- Generally, a court order **is** required to confiscate a cell phone from a non-inmate if the individual doesn't voluntarily surrender it. Use of force is **not** authorized to take a cell phone from a non-inmate.

2. **Can staff legally extract information stored on a confiscated cell phone?**

- Generally, if the cell phone was confiscated from an inmate, or if it was found without an owner in an unauthorized area, a forensic examination may be conducted without a court order.
- Staff can legally extract information if it is reasonably needed to perform a security investigation (*Hudson* v. *Palmer,* 468 U.S. 517, 525-26. 1984).
- In most jurisdictions, a court order **is** required to extract information from a non-inmate cell phone that is confiscated.

It is advisable to include the DA in the process as a cell phone forensics lab is established, so that he/she may weigh in on the appropriate chain-of-custody and evidence collection/retention procedures. The DA should have an opportunity to review and comment on agency policies and procedures so that he/she may properly respond to potential defense counsel challenges to the process.

Prioritizing Evidence to Prevent Backlogs

It is quite likely that the number of cell phones found will initially overwhelm the capacity of the cell phone forensic resources available. Therefore, it is important to establish appropriate criteria for prioritizing evidence to prevent backlogs. Although each circumstance will be unique, in general those cases with the potential to adversely affect public safety and/or institutional security should be afforded the highest priority. Close consultation with legal counsel, internal security staff and local law enforcement will enable forensic examiners to better prioritize the workload to maximize efficiency and to prevent backlogs.

Evidence Collection and Retention Issues

It is vitally important to establish appropriate evidence collection, cataloging, chain-of-custody, retention and disposition procedures. Access to the forensic lab should be controlled and logged. Unauthorized individuals should be prohibited from entering. Evidence should be kept under lock and key.

Generally, confiscated cell phones not being used as evidence in a criminal prosecution can be disposed of after one year. Cell phones that are being used as evidence in a criminal prosecution must be retained until all appeals have been exhausted.

Disposal methods vary. Some agencies erase the personal data from the phones and sell them at auction. Others donate confiscated cell phones to charities, while still others simply destroy them. Regardless of the disposition method, records must be maintained and monitored for integrity and trends. Disposal methods (if scheduled for destruction) should be environmentally appropriate (i.e., recycle vs. discard).

Importance of Policies and Procedures

Policies and procedures are required to ensure that forensic examiners follow established process for extracting and recording evidence that will stand up under legal scrutiny. MD DPSCS has developed a policy for handling contraband cell phones (MD DPSCS Policy 110.0008, Oct. 14, 2011). Exhibit 17 features an excerpt.

Exhibit 17. Maryland Department of Public Safety and Correctional Services Policy DPSCS.110.0008, Contraband – Cellular Telephones, (10/14/11) (excerpt)

§ .03 Policy.

A. The Department shall establish uniform procedures for documenting, processing, tracking and disposing of contraband cellular telephones found in a Department facility.

B. The Department shall establish uniform procedures to preserve the evidentiary value of contraband cellular telephones found in a Department facility and information extracted from a contraband cellular telephone.

C. The Department shall establish procedures for communicating results of analysis of information extracted from a contraband cellular telephone to other public safety agencies.

Source: MD DPSCS, 2013

The MD DPSCS policy also provides specific instructions for staff who find contraband cellular devices. Staff must secure the device, notify the shift supervisor, complete a Cell Phone Chain of Custody form, secure the phone and the form in a sealed evidence envelope, and file reports as directed. Supervisors log the contraband into the Facility Incident Reporting Manager (FIRM) system, an automated security reporting system. The policy requires proper chain-of-custody, secure storage and referral to the cell phone forensic lab technician (see Section .05., B. Responsibility, pp. 3-7, of the MD DPSCS policy DPSCS.110.0008.)

NIJ's flipbook titled *Electronic Crime Scene Investigation: An On-the-Scene Reference for First Responders* provides a pocket-sized resource that assists officers in recognizing and identifying potential digital evidence and properly secure the evidence for later analysis. https://www.ncjrs.gov/pdffiles1/nij/227050.pdf.

In Maryland, cell phone forensic lab technicians are required to retrieve the confiscated cellular devices from the facilities where they were seized. They extract whatever information they can from the devices and inform appropriate internal personnel and other concerned criminal justice agencies of any significant intelligence gained from the forensic examinations (see Section .05., H. Responsibility, pp. 7-8, of the MD DPSCS policy DPSCS.110.0008.)

The MD DPSCS policy also provides specifics on the required retention period (minimum of one year in cases that are not prosecuted, or until all appeals are exhausted in a criminal prosecution) and delineates the disposition procedures when the devices become eligible for disposal (see Sections .05., J. and K. Responsibility, p. 9, of the MD DPSCS policy DPSCS 110.0008.)

The Scientific Working Group on Digital Evidence (SWGDE) also provides policies and procedures that may be helpful to practitioners. Of note is SWGDE Best Practices for Mobile Phone Forensics - version 2.0 and SWGDE Model Operating Procedures for Computer Forensics - version 3.

These documents are available on the SWGDE website and can be located by using the site's search function.

https://www.swgde.org/

Lessons Learned and Success Stories

The forensic examination of confiscated cell phones has resulted in successful prosecutions by law enforcement. A well-publicized case from the New Jersey Department of Corrections (NJ DOC) in 2009 resulted in the indictment of 35 inmates (see Exhibit 18).

Forensic analysts used the data collected from the confiscated cell phones to link inmates with known STGs. The call detail records helped prosecutors establish the communication connections that proved criminal conspiracy. To date, this prosecution represents the largest criminal enterprise operating from behind bars to be disrupted through the use of cell phone forensics (Jeffrey Poling, NJ DOC, 2013).

Exhibit 18. New Jersey Department of Corrections Successful Prosecution

TRENTON – Attorney General Anne Milgram announced that the Division of Criminal Justice has obtained state grand jury indictments charging 35 inmates with the illegal possession of cell phones in state prisons as a result of a collaborative effort with the Department of Corrections. Twenty-five of the indicted inmates are members or associates of criminal street gangs, including various sets of the Bloods, as well as the Crips, Latin Kings, and Netas.

In another NJ DOC case, *State* v. *Calvin Alexander,* staff found a cell phone in a ceiling light fixture in a dormitory housing unit. The inmate whose bed was directly under the light was charged. A subsequent forensic examination recovered several text messages. A cross check against the phone system used by inmates for collect calls found several of the numbers in the cell phone matched the numbers on another inmate's calling list. None of the numbers matched the calling list of the inmate originally charged. The second inmate lived in the dormitory and his bed was near the light fixture. He pled not guilty, but was ultimately found guilty in trial court. The case would not have proceeded in this manner without the use of cell phone forensics (Jeffrey Poling, NJ DOC, 2013).

BOP reports that, as of 2013, the bureau has prosecuted more than 100 inmates for various crimes as a result of forensic examinations performed on confiscated cell phones. These crimes include child pornography, drug trafficking and contraband smuggling.

Clearly there is a wealth of law enforcement and corrections intelligence contained within confiscated cellular devices. Most of this information exists without ever being extracted by trained forensic analysts. It is well documented that some inmates maintain strong organizational control of their co-conspirators in the

community. They operate criminal enterprises, they orchestrate intra- and inter-institutional disruptions, and they coordinate escapes. They threaten public officials, they harass witnesses and they intimidate victims. Much of this criminal activity could be interrupted, prosecuted and deterred if agencies develop the internal capacity to perform forensic analyses of confiscated cell phone devices.

CHAPTER 6
CONCLUSIONS

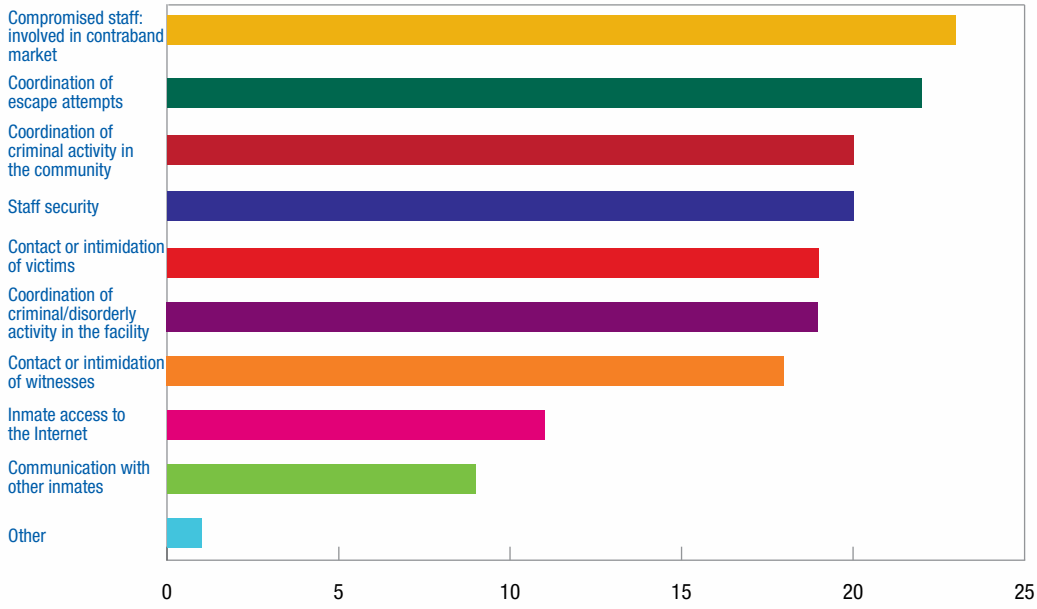
According to a recent survey of state correctional administrators, there is a great deal of concern related to the security threats that cell phones pose (see Exhibit 19).

There are ongoing initiatives to address the problems that contraband cell phones pose, including implementation of managed access systems, detection/location systems, hand-held detection devices, K9 training,

Exhibit 19. Summary of Cell Phone Threats and Concerns

Association of State Correctional Administrators
Contraband Cell Phones Survey Results

Greatest Level of Concern for Security Threats That Cell Phones Pose for Agencies



Other: Security Threat Groups communicate to outside gangs to maintain understanding of the activity and make profit from illegal acts

Source: Association of State Correctional Administrators, 2013

enhanced portal security and legislation designed to deter and prosecute attempts to introduce wireless devices into prisons. Each of these initiatives has strengths and weaknesses. Used in conjunction, they can complement each other. But realistically, contraband will find its way into the hands of inmates in spite of all the best efforts of correctional administrators.

In July 2013, the Corrections Technology CoE, in coordination with the Association of State Correctional Administrators (ASCA), presented a webinar on the issue of contraband cell phones in prisons. A poll of practitioner participants yielded responses to the question: "If technology such as managed access was used to defeat inmate calls would there still be a need to recover the phones?" (see Exhibit 20). More than 95 percent of the respondents said that they believed that it would be beneficial to recover the hardware. It is likely that the remaining five percent do not understand that the hardware, in the hands of an inmate, can still be used as a camera, a video recorder, a word processor and/or a local text messaging hotspot even when the signal to the cell phone tower is interrupted. Clearly, those who subscribe to the "paperweight theory" (i.e., terminate the calling feature and render the cell phone into a useless "paperweight") do not understand the capabilities of the technology or the continuing threat to security that cell phones pose if they are not confiscated.

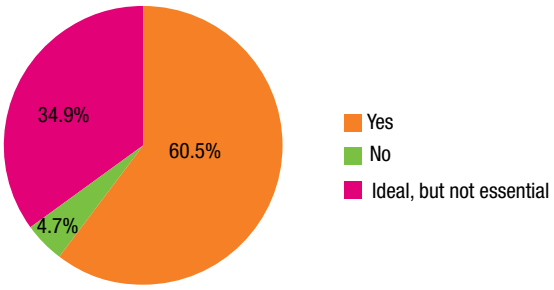
Recovered contraband wireless devices contain potentially valuable intelligence that can assist in the investigation of criminal activity and the prosecution of the perpetrator(s). Due to the number of devices confiscated, the FBI and state police forensic labs are overwhelmed with a large backlog of requests for analysis. Therefore, it is becoming increasingly important for correctional agencies to develop their own internal capacity to perform forensic analyses.

Only about 29 percent of the practitioner respondents polled during the July 2013 cell phone webinar indicated that their agency has the internal capability to perform forensics on recovered cell phones. Fifty-five percent said "No," and about 16 percent didn't know (see Exhibit 21). (Note that the webinar participants did not identify the agency that they represent, and it is quite likely that some agencies had multiple participants. Therefore, one cannot assume that these results represent all states or all agencies.)

It appears that less than one-third of the participants polled in the July 2013 ASCA survey represent agencies that have the internal capacity to perform forensic analyses on confiscated cell phones. The agencies that have this capacity have been able to investigate and prosecute crimes that would have otherwise gone undetected. Exhibit 22 reflects the number of cell phone

Exhibit 20. Practitioner Response to the Poll Question:

"If technology such as managed access was used to defeat inmate calls would there still be a need to recover the phone?"

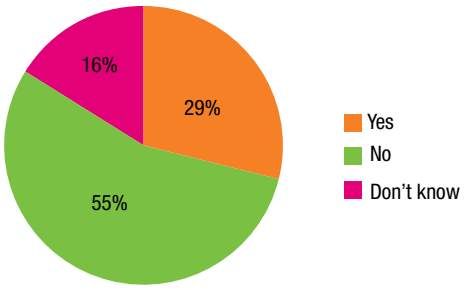


Source: ASCA Webinar Poll, July 2013

Yes	26
No	2
Ideal, but not essential	15
Total responses	43

Exhibit 21. Practitioner Response to the Poll Question:

"Does your agency have the internal capability to perform forensics on recovered cell phones?"



Source: ASCA Webinar Poll, July 2013

Yes	11
No	21
Don't know	6
Total responses	38

cases that have been referred for prosecution by the agencies that responded to a recent ASCA survey. With the capacity to conduct more forensic analyses, the percentage of cases referred for prosecution will likely increase. As more cases are successfully prosecuted, a deterrent effect could result in fewer cell phones being smuggled inside the nation's prisons.

In order to develop the internal capacity to conduct forensic analyses on wireless devices, an agency must have strong executive support. There must be a commitment to fund the initial lab, including staffing, training, equipment, and computer hardware and software. Beyond the initial stand-up costs, there must be a financial commitment to ongoing training and hardware/software upgrades due to the dynamic, ever-changing advances in wireless technology.

Agencies that take the initiative to establish a cell phone forensics lab will be able to analyze the data on confiscated phones. Mining the data from the phones and conducting link analyses with other data sources (e.g., inmate visiting lists, employee/volunteer telephone numbers) will yield a wealth of potentially actionable intelligence that will enable investigators to develop a case for the successful prosecution of criminal activity. In some cases, the data gathered may be sufficient to prevent an escape, intercept the smuggling of contraband or interrupt a conspiracy to commit some other planned criminal activity. See Appendix A for a list of agencies and contacts that have established forensic labs.

Exhibit 22. Cell Phone Cases Referred for Prosecution

Association of State Correctional Administrators
Contraband Cell Phones Survey Results

	Referred for Prosecution	Number of Cell Phones Confiscated	Percent Referred for Prosecution
Agency 1	1	367	0.3%
Agency 2	1	67	1.5%
Agency 3	1	170	0.6%
Agency 4	2	110	1.8%
Agency 5	5	68	7.4%
Agency 6	10	650	1.5%
Agency 7	12	2,106	0.6%
Agency 8	18	63	28.6%
Agency 9	21	36	58.3%
Agency 10	57	2,107	2.7%
Agency 11	61	312	19.6%
Agency 12	68	1,166	5.8%
Agency 13	82	630	13.0%
Agency 14	100	3,000	3.3%
Agency 15	164	411	39.9%
Agency 16	336	1,516	22.2%
Agency 17	567	3,830	14.8%
Total	1,506	16,609	9.1%

APPENDIX A
SAMPLE POLICIES AND PROCEDURES AND FORENSIC LAB CONTACT INFORMATION

Sample Policies and Procedures

1. Maryland Department of Public Safety and Correctional Services (MD DPSCS) Policy 110.0008, *Contraband – Cellular Telephones,* 10/14/11.

2. Scientific Working Group on Digital Evidence (SWGDE) Quality Assurance Manual (QAM) and Standard Operating Procedures (SOP) Manual https://www.swgde.org/

3. Scientific Working Group on Digital Evidence (SWGDE) Best Practices for Mobile Phone Forensics https://www.swgde.org/

4. U.S. Department of Homeland Security and U.S. Secret Service, *Best Practices for Seizing Electronic Evidence (v.3) A Pocket Guide for First Responders.*

5. *Electronic Crime Scene Investigation: An On-the-Scene Reference for First Responders.* https://www.ncjrs.gov/pdffiles1/nij/227050.pdf

Forensic Lab Contact Information: State and Federal Government

(Note that this list is not necessarily all-inclusive and no specific lab is endorsed by NIJ or NLECTC.)

1. Federal Bureau of Prisons, Darnell Stewart, Forensic Examiner, (202) 616-2152.

2. U.S. Department of Homeland Security, Sam Brothers, Forensic Analyst, (703) 921-7149, sam.brothers@dhs.gov

3. Maryland Department of Public Safety and Correctional Services, Jay Miller, DOC IT Manager, (410) 585-3489, JEMiller@dpscs.state.md.us

4. Nebraska Department of Corrections, Jeff Peterson, Intelligence Coordinator, (402) 479-5912, Jeff.A.Peterson@nebraska.gov

5. New Jersey Department of Corrections, Jeff Poling, Senior Investigator, (609) 292-4036 ext. 5190, Jeffrey.Poling@doc.state.nj.us

Forensic Lab Contact Information: Private Sector

(Note that this list is not necessarily all-inclusive, and no specific lab is endorsed by NIJ or NLECTC.)

1. AccessData, (800) 574-5199, http://www.accessdata.com

2. Computer Forensics Labs, Inc., (303) 500-7200, http://www.computerforensiclabsinc.com/

3. DisputeSoft, (646) 416-7990 (N.Y.) (301) 765-9506 (Md.), http://www.disputesoft.com

4. Optimo Digital Forensics, (877) 564-8552, http://www.optimo-it.com/landing/digital-forensics/?gclid=CJLu2snVv7wCFTHNOgodsUEA5A

5. Southern Vermont Digital Forensics Laboratory, Inc., (802) 451-1098 (Vt.) 603-513-7833 (N.H.), http://www.svdfl.com/

6. Teel Technologies, (203) 855-5387, http://www.teel-tech.com

APPENDIX B
REFERENCES

1. Brothers, Samuel. May 8, 2008. *Cell Phone Forensic Tool Classification Pyramid,* Mobile Forensics World 2008, Breakout Presentation, Chicago, Ill.

2. BKForensics.com. http://www.bkforensics.com/rfsolutions.html

3. Maryland Department of Public Safety and Correctional Services (MD DPSCS). Oct. 14, 2011. *Policy 110.0008, Contraband – Cellular Telephones*.

4. MicroSystemation (XRY). http://www.msab.com/xry/

5. National Institute of Justice. April 2012. *SFP1215W Forensic Pouch Evaluation Report.* https://www.justnet.org/pdf/SFP1215W-Forensic-Pouch.pdf

6. National Institute of Justice. September 2012. *Test Results for Mobile Device Acquisition Tool: CelleBrite UFED 1.1.8.6 – Report Manager 1.8.3/UFED Physical Analyzer 2.3.0.* NCJ238993. https://ncjrs.gov/pdffiles1/nij/238993.pdf

7. National Institute of Standards and Technology. April 12, 2010. *Computer Forensics Tool Testing Program, Smart Phone Tool Test Assertions and Test Plan.* www.cftt.nist.gov/mobile_devices.htm

8. National Institute of Standards and Technology. Feb. 1, 2012. *Computer Forensics Tool Testing Handbook.* http://www.cftt.nist.gov/CFTT-Booklet-Revised-02012012.pdf

9. National Institute of Standards and Technology. 2013. *Computer Forensics Tool Test Reports.* http://www.cftt.nist.gov/mobile_devices.htm

10. Jansen, Wayne and Rick Ayers. May 2007. *NIST Special Publication 800-101, Guidelines on Cell Phone Forensics: Recommendations of the National Institute of Standards and Technology.* http://csrc.nist.gov/publications/nistpubs/800-101/SP800-101.pdf; http://csrc.nist.gov/publications/drafts/800-101-rev1/draft_sp800_101_r1.pdf (latest draft version).

11. Paraben Mobile Field Kit. https://www.paraben.com/device-seizure-field-kit.html

12. Poling, Jeffrey. Senior Investigator, NJ Department of Corrections, Special Investigations Division, Technical Services Unit, 2013.

13. RamseyTest.com. http://www.ramseytest.com/product.php?pid=22

14. Scientific Working Group on Digital Evidence, June 7, 2012. *SWGDE Core Competencies for Mobile Phone Forensics, Version: 1.0*. https://www.swgde.org/documents/Archived%20Documents/2012-06-07%20SWGDE%20Core%20Competencies%20for%20Mobile%20Phone%20Forensics-v1.0

15. Teel, Bill. Teel Technologies, 2013. http://www.teel-tech.com

APPENDIX C
LIST OF ACRONYMS

Acronym	Definition
ASCA	Association of State Correctional Administrators
BOP	Bureau of Prisons
CDCR	California Department of Corrections and Rehabilitation
CD/DVD	Compact Disk/Digital Video Disk
CoE	Center of Excellence
CPIK	Cell Phone Investigative Kiosk
DA	District Attorney
DU	Denver University
EEPROM	Electronically Erasable Programmable Read-Only Memory
FBI	Federal Bureau of Investigation
FIRM	Facility Incident Reporting Manager
iOS	Mobile Operating System developed by Apple, Inc.
IT	Information Technology
JIG	Joint Industry Guide
JTAG	Joint Test Action Group
K-9	Canine
LE	Law Enforcement
MAC	Macintosh
MDOC	Mississippi Department of Corrections
MDPSCS	Maryland Department of Public Safety and Correctional Services
NAND	Negated AND or NOT AND
NIJ	National Institute of Justice
NIST	National Institute of Standards and Technology
NJDOC	New Jersey Department of Corrections
NLECTC	National Law Enforcement and Corrections Technology Center
NOR	Negated OR
OSX	Operating System X, a Unix-based operating system developed by Apple, Inc.
PIN	Personal Identification Number

Acronym	Definition
RAM	Random Access Memory
RCFL	Regional Computer Forensics Laboratory
RF	Radio Frequency
SD	Secure Digital
SIM	Subscriber Identity Module
SME	Subject Matter Expert
STG	Security Threat Group
SWGDE	Scientific Working Group on Digital Evidence
TWG	Technology Working Groups
UFED	Universal Forensics Extraction Device
URL	Uniform Resource Locator
USB	Universal Series Bus

APPENDIX D
GLOSSARY OF TERMS

Term	Definition
Boot Loader	A boot loader, also called a boot manager, is a small program that places the operating system (OS) of a computer into memory. When a computer is powered up, the basic input/output system (BIOS) performs some initial tests and then transfers control to the master boot record (MBR) where the boot loader resides. Most new computers are shipped with boot loaders for some version of Microsoft Windows™ or the MAC OS. If a computer is to be used with Linux, a special boot loader must be installed. For additional information, see: http://searchenterpriselinux.techtarget.com/definition/boot-loader. (TechTarget, 2014)
Chip Off	A technique that involves the removal of a memory chip, or any chip, from a circuit board and reading it. For additional information, see: http://www.evidencemagazine.com/index.php?option=com_content&task=view&id=922 (Evidence Technology Magazine, 2014)
EEPROM Reader	An Electronically Erasable Programmable Read-Only Memory Reader is an analytical tool used to read the programming code on computer chips. For additional information, see: http://www.wisegeek.com/what-is-an-eeprom-reader.htm (WiseGEEK, 2014)
Faraday Shielding	A device, first developed by physicist Michael Faraday (1791-1867), that is designed to block electric fields. For additional information, see: http://www.wisegeek.com/what-is-a-faraday-shield.htm (WiseGEEK, 2014)
Flasher Box	A device that permits forensic examiners access to retrieve information from digital devices, including contacts, call history, and deleted images and videos. For additional information, see: https://news.uns.purdue.edu/x/2007a/070412MislanFlash.html (Purdue University, 2014)
Flash Reader	A peripheral device that reads and writes a memory card made of flash memory chips. For additional information, see: http://www.pcmag.com/encyclopedia/term/46764/memory-card-reader (PC Magazine, 2014)
Hex Dump Tools	A Hex Dump Tool enables the user to list the contents of a file in hexadecimal and ASCII code. It is useful for seeing exactly what is in a file, byte-by-byte. For additional information, see: http://en.wikipedia.org/wiki/Hex_dump (Wikipedia, 2014)
JTAG Connection	A Joint Test Action Group connection is a universally accepted means for testing wire-line interconnects on printed circuit boards. For additional information, see: http://www.evidencemagazine.com/index.php?option=com_content&task=view&id=922
Logical Extraction	A digital forensic examination process that enables the acquisition of most of the data on a digital device in a readable format and forensically sound manner. Data types include passwords, call logs, SIM deleted call logs, phone details, phonebook entries, text messages, imaged, videos, audio files, etc. Logical extraction is not possible on locked devices. For additional information, see: http://www.cellebrite.com/mobile-forensics/capabilities/operations/logical-extraction (Cellebrite, 2014)
Manual Extraction	A digital forensic examination process that involves reviewing the data on a digital device by browsing through the various menu options to review and record data by hand. Pros: It works on every device, does not require cables or external software, and is easy to do. Cons: It will not get all data, it will not allow access to deleted files and it can be time consuming. For additional information, see: http://www.nist.gov/forensics/upload/2-Brothers-NIST-2014_Slides-23-Pages-2.pdf (Sam Brothers, 2014)

Term	Definition
Micro Reader	A device that allows users to move data between computers and small devices such as mobile phones and cameras. For additional information, see: http://www.ehow.com/facts_6919474_usb-microsd-card-reader_.html (eHow.com, 2014)
NAND Chip	Negated AND or NOT AND chips are part of the circuitry of a digital device that processes information via Boolean functions. For additional information, see: http://xlinux.nist.gov/dads//HTML/nand.html (NIST, 2014)
NOR Chip	Negated OR chips are part of the circuitry of a digital device that processes information via Boolean functions. For additional information, see: http://xlinux.nist.gov/dads///HTML/nor.html (NIST, 2014)
Physical Analysis	A digital forensic examination process that involves reviewing the data on a digital device by pushing a boot loader into the digital device and dumping the memory from it. Pros: It enables access to deleted data and data hidden from device menus. Cons: It requires data conversion and custom cables, and it can be difficult to do. For additional information, see: http://www.nist.gov/forensics/upload/2-Brothers-NIST-2014_Slides-23-Pages-2.pdf (Sam Brothers, 2014)
Unallocated Space	When files are erased or deleted from a digital device, the content of the file is not actually erased. The "erased file" remains behind in an area of the device known as unallocated storage space. As a result, the data remains behind for discovery through the use of data recovery and/or computer forensics software utilities. For additional information, see: http://www.computer-forensics.net/FAQs/what-is-unallocated-space.html (Center for Computer Forensics, 2014)