Developing Process for Mobile Device Forensics

Det. Cynthia A. Murphy

Abstract –
With the growing demand for examination of cellular phones and other mobile devices, a need has also developed for the development of process guidelines for the examination of these devices. While the specific details of the examination of each device may differ, the adoption of consistent examination processes will assist the examiner in ensuring that the evidence extracted from each phone is well documented and that the results are repeatable and defensible.

I. INTRODUCTION

Over the past several years, digital forensic examiners have seen a remarkable increase in requests to examine data from cellular phones and other mobile devices. The examination and extraction of data from these devices presents numerous unique challenges for forensic examiners. With smart phones and tablets representing an increasing proportion of mobile devices submitted for examination, the number unique challenges continue to grow. Some of those challenges include the following:

Not only are there a large variety of mobile devices available commercially, those devices use a variety of proprietary operating systems, embedded file systems, applications, services, and peripherals. Each of these unique devices may be supported to different extents by the available forensic software tools, or may not be supported at all. There is also generally significant lag time before newer smart phone devices are supported sufficiently by mobile forensic tools.

The types of data contained within mobile devices and the way they are being used are constantly evolving. With the popularity of smart phones, it is no longer sufficient to document only the phonebook, call history, text messages, photos, calendar entries, notes and media storage areas because these devices are fully functioning mini-computers and potentially contain much more relevant data. The data from an ever-growing number of installed applications can contain a wealth of relevant information that may not be automatically parsed by available forensic software solutions. Traditional digital forensic skills are becoming more and more necessary for mobile device examinations.

Cellular phones and other mobile devices are designed to communicate with cellular and other networks via radio, Bluetooth, infrared and wireless (WiFi) networking. To best preserve the data on the phone it is necessary to isolate the phone from surrounding networks. This may not always be possible, and isolation methods can be prone to failure.

Mobile devices use a variety of internal, removable and online data storage capabilities. In many cases, it is necessary to use more than one tool in order to extract and document the desired data from the mobile device and its associated data storage media. In certain cases, the tools used to process cellular phones may report conflicting or erroneous information. It is therefore critical to verify the accuracy of data obtained from mobile devices. And, while the amount of data stored by phones is still small when compared to the storage capacity of traditional computer hard drives, the storage capacity of these devices continues to grow.

The reasons for the extraction of data from cellular phones may be as varied as the techniques used to process them. Cellular phone data is often desired for intelligence purposes and the ability to process phones in the field is attractive. Sometimes only certain data is important to an investigation. In other cases full extraction of the embedded file system and/or the physical memory of the phone is desirable for a full forensic examination and potential recovery of deleted data.

Because of these factors, the development of guidelines and processes for the extraction and documentation of data from mobile devices is extremely important, and those guidelines and processes must be periodically reviewed as mobile device technology continues to evolve and change. What follows is an overview of process considerations for the extraction and documentation of data from mobile devices.
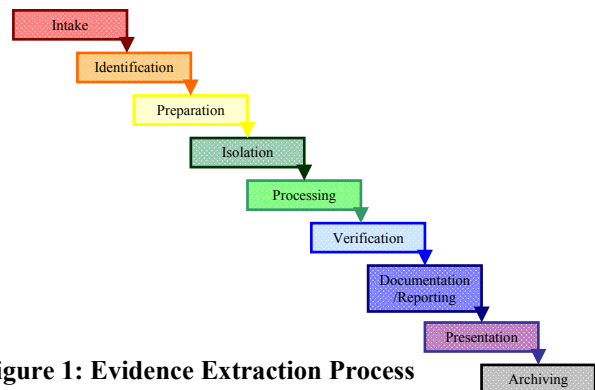
Cellular Phone Evidence Extraction Process

Figure 1: Evidence Extraction Process

Evidence Intake Phase

The evidence intake phase involves the procedure by which requests for examinations are handled. The evidence intake phase generally entails request forms and intake paperwork to document chain of custody, ownership information, and the type of incident the mobile device was involved in and outlines general information regarding the type of data or information the requester is seeking.

Critical at this phase of the examination is the development of specific objectives for each examination. This not only serves to clarify and document the examiner's goals, but also assists in the triage of examinations and begins the documentation of the examination process for each individual device examined. Many agencies and organizations use a form to document intake of mobile devices for examination.

Identification Phase

For every examination of a mobile device, the examiner should identify the following:

- Legal authority for examination of the device
- The goals of the examination
- The make, model and identifying information for the device(s)
- Removable & external data storage
- Other sources of potential evidence

Legal Authority:
Case law surrounding the search of data contained from mobile devices is in a nearly constant state of flux. It is imperative that the examiner determines and documents what legal authority exists for the search of the device, as well as any limitations placed on the search, prior to the examination of the device:
- If the cellular phone is being searched pursuant to a warrant, the examiner should be mindful of confining the search to the limitations of the warrant.
- If the cellular phone is being searched pursuant to consent, any possible limitations of the consent (such as consent to examine the call history only) and should determine whether consent is still valid prior to examining the phone.
- In cases where the phone is being searched incident to arrest, the examiner needs to be particularly cautious, as current case law in this area is particularly problematic and in a state of constant change.

Particular questions as to the legal authority to search a cellular phone should be directed to a knowledgeable prosecutor or legal advisor in the examiner's local area (Mislan, Casey & Kessler 2010).

In some situations, you may find that the stated requirements for the particularity of a search articulated in a search warrant or consent go beyond the abilities of available forensic tool capabilities. For example, if a search warrant limits search of a cell phone or other mobile device for call history and messages within a particular date range, most forensic tools do not allow the examiner to limit data extraction to just that data within a date range. Obtaining all of the data from a phone and winnowing that data down to that which is articulated in the warrant may be seen as an overbroad search. It is therefore important to articulate these kinds of limitations when drafting search warrants or obtaining consent to search a device.

The Goal of the Examination:
While the general process used to examine any given cellular phone should be as consistent as possible, the goal of the examination for each phone may be significantly different. It is unlikely that any given forensics lab has the resources, capability or the capacity to examine every cellular phone that contains data of evidentiary value in every kind of case. For this reason, it can be useful to identify what level of examination is appropriate for any given cellular phone.

The first of two main considerations is who will be responsible for the process of documenting the data. The second main consideration is how in depth the examination needs to be. Of those phones that are submitted to the lab for examination, there will be differences in the goals of each examination based upon the facts and circumstances of the particular case.

In some cases evidence from cellular phones may be documented in the field either by hand or photographically. For example, in the interest of returning a victim's main communication lifeline while still documenting information of evidentiary value, or in the case of documenting evidence in a misdemeanor or minor offense, field documentation would be a reasonable alternative to seizing the device. In other cases, it may be sufficient to have an officer or analyst with basic training in the examination of cellular phones perform a quick dump of cellular phone data in the field, specifically for intelligence purposes using commercially available tools designed for this purpose.

A smaller subset of cellular phones may be submitted for examination with the goal of targeted data extraction of data that has evidentiary value. Specifically targeted data, such as pictures, videos, call history, text messages, or other specific data may be significant to the investigation while other stored data is irrelevant. It also might be the case that only a certain subset of the data can be examined due to

legal restrictions. In any event, limiting the scope of the exam will likely make extraction and documentation of the data less time consuming.

The goal of the exam may alternatively include an attempt to recover deleted data from the memory of the phone. This is usually only possible if a tool is available for a particular phone that can extract data at a physical or file system level (See levels detailed at the end of this section). If such a tool is available, then the examination will involve traditional computer forensic methods such as data carving, hex decoding, and examination of SQLite databases and therefore the examination process may be a time consuming and technically involved endeavor, as deeper levels of examination necessitate a more technically complex and time consuming process.
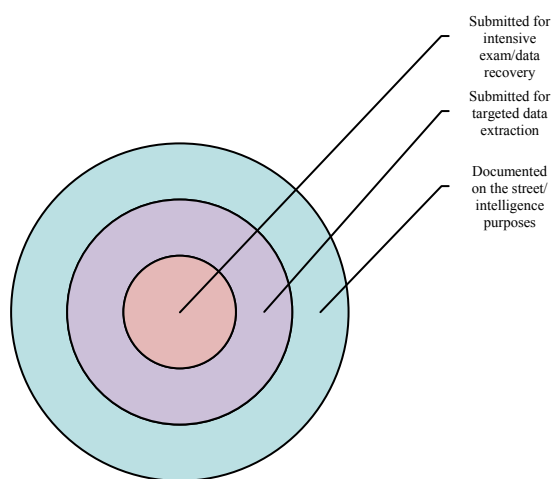

Submitted for intensive exam/data recovery

Submitted for targeted data extraction

Documented on the street/ intelligence purposes

Figure 2: Goal of the Exam 1

The goal of the exam can make a significant difference in what tools and techniques are used to examine the phone. Time and effort spent initially on identification of the goal of the exam can lead to increased efficiency in the examination process. These types of realities should be addressed in training, and the triage process related to the initial submission of cellular phones for examination should based upon the individual circumstances and severity of the case.

Make, Model and Identifying Information
As part of the examination of any cellular phone, the identifying information for the phone itself should be documented. This enables the examiner not only to identify a particular phone at a later time, but also assists in the determination about what tools might work with the phone as most cellular phone forensic tools provide lists of supported phones based on the make and model of the phone. For all phones, the manufacturer, model number,

carrier and the current phone number associated with the cellular phone should be identified and documented.

Depending upon the cellular phone technology involved, additional identifying information should be documented, if available, as follows:

CDMA cellular phones:
The **Electronic Serial Number** (ESN) is located under the battery of the cellular phone. This is a unique 32 bit number assigned to each mobile phone on the network. The ESN may be listed in decimal (11 digits) and/or hexadecimal (8 hex digits). The examiner should be aware that the hex version of the ESN is not a direct numeric conversion of the decimal value. An ESN converter can be found at *http://www.elfqrin.com/esndhconv.html.*

The **Mobile Equipment ID** (MEID), also found under the battery cover, is a 56 bit number which replaced the ESN due to the limited number of 32 bit ESN numbers. The MEID is listed in hex, where the first byte is a regional code, next three bytes are a manufacturer code, and remaining three bytes are a manufacturer-assigned serial number. CDMA phones do not generally contain a Subscriber Identity Module (SIM) card, but some newer hybrid phones contain dual CDMA and GSM technology and can be used on either CDMA or GSM networks. Inside these dual technology phones is located a slot for a SIM card. The identifying information under the battery of these phones may list an IMEI number in addition to the ESN/MEID number.

CDMA phones also have two other identifying numbers, namely, the **Mobile Identification Number (MIN)** and **Mobile Directory Number (MDN).** The MIN is a carrier-assigned, carrier-unique 24-bit (10-digit) telephone number. When a call is placed, the phone sends the ESN and MIN to the local tower. The MDN is the globally-unique telephone number of the phone. Prior to Wireless Number Portability, the MIN and MDN were the same but in today's environment, the customer can keep their phone number (MDN) even if they change carriers.

GSM cellular phones:
The International Mobile Equipment Identifier (IMEI) is a unique 15-digit number that identifies a GSM cellular phone handset on its network. This number is generally found under the battery of the cellular phone. The first 8 digits are a Type Allocation Code (TAC) and the next 6 digits are the Device Serial Number (DSN). The final digit is a check digit, usually set to 0.

On a GSM phone, there will be at least a Subscriber Identity Module (SIM) card slot which is also generally

located under the battery. The SIM card may be branded with the name of the network to which the SIM is registered. Also located on the SIM card is the Integrated Circuit Card Identification (ICCID), which is an 18 to 20 digit number (10 bytes) that uniquely identifies each SIM card. The ICCID number is tied to the International Mobile Subscriber Identity (IMSI) which is typically a 15-digit number (56 bits) consisting of three parts including the Mobile Country Code (MCC; 3 digits), Mobile Network Code (MNC; 3 digits in the U.S. and Canada, and 2 digits elsewhere), and Mobile Station Identification Number (MSIN; 9 digits in the U.S. and Canada, and 10 digits elsewhere) which are stored electronically within the SIM. The IMSI can be obtained either through analysis of the SIM or from the carrier.

The Mobile Station International Subscriber Directory Number (MSISDN) is the phone's 15-digit, globally unique number. The MSISDN follows the International Telecommunication Union (ITU) Recommendation E.164 telephone numbering plan, composed of a 1-3 digit country code, followed by a country-specific number. In North America, the first digit is a 1, followed by a 3-digit area code.

iDen cellular phones:
Though less popular in recent years, iDen phones provide the ability for users to communicate directly to one or more other iDen phones by radio. iDen cellular phones contain an International Mobile Equipment Identity (IMEI) that identifies an iDen cellular phone on its network. This number is generally found under the battery of the cellular phone. iDen cellular phones also contain SIM cards, with the identifying information described above, though they are based on different technology than GSM SIM cards and are not compatible with GSM cellular phones.

Unique to iDen cellular phones is the Direct Connect Number (DCN) which is also known as the MOTOTalk ID, Radio-Private ID or iDen Number. The DCN is the identifying number used to communicate directly device-to-device with other iDen cellular phones. This number consists of a series of numbers formatted as ###*###*##### where the first three digits are the Area ID (region of the home carrier's network), the next three digits are the Network ID (specific iDen carrier) and the last five digits are a subscriber identification number which sometimes corresponds to the last five of the cellular phone number. (Punja, & Mislan, 2008)

Removable /External Data Storage:
Many cellular phones currently on the market include the ability to store data to a removable storage device such as a Trans Flash Micro SD memory expansion card. In the event that such a card is installed in a cellular phone that is submitted for examination, the card should be removed by the examiner and processed using traditional digital forensics techniques. The processing of data storage cards using cellular phone forensic tools while the card remains installed within the phone may result in the alteration of date and time stamp data for files located on the data card.

Additionally, cellular phones may allow for the external storage of data within network based storage areas accessible to the phone's user by computer or data on the phone may be synced with an internet based account such as iCloud account for iOS devices or a Google account for Android based devices. Accessing this data, which is stored on the service provider's network, may require further legal authority and is generally beyond the scope of the examination of a cellular phone handset. However, the potential existence of network based data storage should be taken into account by the examiner.

Many feature phones and smart phones are also designed to sync with a user's computer to facilitate access to and transfer of data to and from the cellular phone. Full or partial backups of the data from a phone may be found on the phone owner's computer or any computer the phone has been synced with. The potential for the existence of these alternative storage areas should be considered by the examiner as additional sources of data originating from cellular phones.

Other Potential Evidence Collection:
Prior to beginning examination of a cellular phone, consideration should be given to whether or not other evidence collection issues exist. Cellular phones may be good sources of DNA, fingerprint or other biological evidence. Collection of DNA, biological and fingerprint evidence should be accomplished prior to the examination of the cellular phone to avoid contamination issues.

Preparation PHASE
Within the Identification phase of the process, the examiner has already engaged in significant preparation for the examination of the phone. However, the preparation phase involves specific research the regarding the particular mobile device to be examined, the appropriate tools to be used during the examination and preparation of the examination machine to ensure that all of the necessary equipment, cables, software and drivers are in place for the examination.

Once the make and model of the mobile device have been identified, the examiner can then research the specific

device to determine what available tools are capable of extracting the desired data from the phone. Resources such as phonescoop.com and mobileforensicscentral.com can be invaluable in identifying information about cellular phones and what tools will work to extract and document the data from specific phones. The SEARCH toolbar (available as a free download from *www.search.org*) contains additional and regularly updated resources for cellular phone examinations.

Choosing Appropriate Tools:
The tools that are appropriate for the examination of a mobile device will be determined by factors such as the goal of the examination, resources available to the organization responsible for the examination, the type of cellular phone to be examined and the presence of any external storage capabilities.

A matrix, such as the example shown below, of the tools available to the examiner, and what general technology of phones (GSM, CDMA, iDEN, SIM Card) they are compatible with in an examination may also be helpful.

	CDMA	GSM	iDen	SIM	Logical Dump	Physical Dump
BitPim	X				X	
Data Pilot Secure View 3	X	X				
Paraben Device Seizure	X	X	X	X	X	X
SIMCon				X		
iDen Media Manager			X			
Manufacturer / Other	X	X	X	X		
Cellebrite	X	X	X	X	X	X
CellDEK	X	X	X	X	X	X
Oxygen Forensic Suite	X	X		X	X	X
XRY / XACT	X	X	X	X	X	X

Figure 3: Cellular Phone tool matrix (Kessler, 2010)

Tool Capabilities:
Notably, there is no one tool available on the market that will be sufficient to retrieve all data from all makes and models of cellular phones and other mobile devices that the examiner will encounter and need to process. Conversely, there are still many phones on the market for which only manual extraction and documentation of the information contained in the phone will be successful. Various cell phone data extraction tools on the market have different capabilities for processing different phones due to the vast and ever changing variety of devices available.

There is also some difference in semantics in the way data extraction from phones is defined from software vendor to software vendor. Therefore, it is important to know how the vendor is using definitions in regards to the capabilities of a particular tool. The following terms are often used to define what types of data extraction of which a particular cell phone data extraction tool is capable:

Object Extraction or Container Extraction:
The terms "Object Extraction" or "Container Extraction" generally refer to the extraction of a particular data type or types from a cellular phone such as text messages, call history, pictures, video, ringtones, calendar, etc. A tool may support the extraction of one or more than one data container(s) from any given make or model of phone. Object or Container extraction is a logical extraction function in that the software is accessing data stored in a particular area of the file system of the phone.

Logical Extraction or Logical Acquisition:
The terms "Logical Extraction" or "Logical Acquisition" generally refer to the extraction of the full file system from a cellular phone. Some vendors, however, more narrowly define logical acquisition as the ability to obtain a particular data type or container (text messages, call history, pictures, video, ringtones, calendar, etc…) from a phone.

File System Extraction:
The term "File System Extraction generally refers to the extraction of the full file system from a cellular phone, though it can also refer to extraction of the file system from removable media cards within the device itself.

Physical Extraction, Physical Acquisition or Physical Memory Dump:
The terms "Physical Extraction," "Physical Acquisition" or "Physical Memory Dump" are generally used to refer to the extraction of the full contents of one or more flash memory chip or chips on the cellular phone. The data from a Physical Extraction, Physical Acquisition, or Physical Memory Dump comes in the form of raw data as a hexadecimal dump which can then be further parsed to obtain file system information and/or human readable data.

Device Profile:
The term "Device Profile" has emerged within the recent past to describe what capabilities a particular cell phone forensics or data extraction tool has related to a particular make and model of cellular phone or mobile device.

Cellular Phone Tool Leveling System:

When identifying the appropriate tools for the analysis of cellular phones, a useful paradigm is the Cell Phone Tool Leveling System (Brothers, 2009). The tool leveling system is designed to categorize mobile phone and GPS forensic analysis tools by the depth to which they are capable of accessing data on a given device. As you move up the pyramid (generally):

- Methods get more "forensically sound"
- Tools get more expensive
- Methods get more technical
- Longer Analysis times
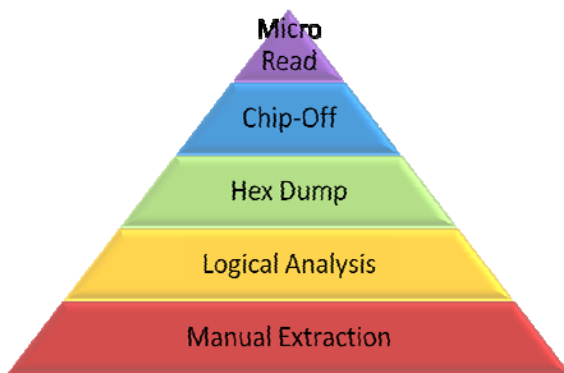- More training required
- More invasive

Figure 4: Cellular Phone Tool Leveling Pyramid – (Brothers 2009)

1. Manual Analysis – physical analysis of the phone involving manual manipulation of the keyboard and photographic documentation of data displayed on the screen.
2. Logical Analysis - Connect data cable to the handset and extract data using AT, BREW, etc. commands in client/server architecture.
3. Physical Analysis (Hex Dump) - Push a boot loader into phone, dump the memory from phone and analyze the resulting memory dump.
4. Physical Analysis (Chip-Off) - Remove memory from the device and read in either second phone or EEprom reader.
5. Physical Analysis (Micro Read) - Use an electron microscope to view state of memory.

In general, examinations gather more detailed information and take more time as one advances through the levels from manual extraction to micro read.

Other resources that should not be overlooked are cellular phone manufacturer's and cellular phone carrier's websites. They can contain links to electronic versions of manuals for almost every make and model of phone as well as cable and phone driver downloads. Manufacturers will also sometimes provide free software designed for users to access and synchronize the data on their phones with their computers. While these tools are not designed specifically for extraction and documentation of evidence, they may be useful when other tools do not work, though caution should be used when utilizing these tools, as they are generally designed to access and write data back to a cellular phone.

Isolation Phase

Cellular phones and other mobile devices are by design intended to communicate via cellular phone networks, and other and to other networks via Bluetooth, infrared and wireless (WiFi) network capabilities. For this reason, isolation of the device from these communication sources is important prior to examination. Isolation of the phone prevents the addition of new data to the phone through incoming calls and text messages as well as the potential destruction of data through remote access or remote wiping via a "kill signal" as well as the possibility of accidental overwriting of existing data as new calls and text messages come in.

Isolation also prevents overreaching of the legal authority such as warrant or consent that covers search of the data on the device. If the phone is isolated from the network, the examiner cannot accidently access voicemail, email, Internet browsing history or other data that may be stored on the service provider's network rather than on the device itself.

Isolation of a cellular phone can be accomplished through the use of Faraday bags or radio frequency shielding cloths which are specifically designed for this purpose. Other available items such as arson cans or several layers of tinfoil may also be used to isolate some cellular phones. Both formal and informal faraday methods and devices however, may be prone to failure (Katz, 2010). Another problem with these isolation methods however is that once they're employed, it is difficult or impossible to work with the phone because you can't see through them or work with the phone's keypad through them. Faraday tents, rooms, and enclosures exist, but are cost prohibitive.

Additionally, some laboratories within the US federal government may use signal jamming devices to curtail radio signals from being sent or received for a given area. The use of such devices is illegal for many organizations and their use should only be implemented after verifying the legality of the use of such devices for a given organization. Additional information about the FCC exceptions can be found at *www.fcc.org*.

Another viable option is to wrap the cellular phone in radio frequency shielding cloth and to then place the phone into Airplane mode (Also known as Standalone, Radio Off,

Standby or Phone Off Mode). Instructions for how to place a phone into Airplane mode can be found in the manufacturer's user manual for the particular make and model of cellular phone.

For GSM cellular phones, isolation can be accomplished by creating and using a SIM ID Clone (also known as a Forensic SIM Clone). A SIM ID Clone is not a fully cloned copy of the cell phone's SIM Card, but rather is an examiner-created SIM Card that contains only the ICCID and IMSI from the original SIM. This allows examination of the contents of the cellular phone without allowing the phone to connect to or be recognized by the surrounding cell phone networks. There are a variety of commercial tools available to create SIM ID Clones including Cellebrite UFED, XRY/XACT, and Forensic SIM Cloner. It may also be possible with some phones to use a SIM ID Clone to access data on a GSM phone with a missing SIM Card even to successfully bypass PIN-locked SIM Cards.

Unfortunately, not all phones have an Airplane mode or its equivalent, and sometimes even the most seemingly foolproof isolation methods can fail. Additionally, some devices obtain their date and time from the cell phone network, and isolation can result in erroneous date and time information. Even if a cellular phone is successfully isolated from all networks, user data can still be affected if automatic functions are set to occur, such as alarms or appointment announcements. If these situations arise the examiner should document their attempts to isolate the phone and whether any incoming calls, text messages or other data transmissions occur during the course of the examination.

Processing Phase

Once the phone has been isolated from the cell phone and other communication networks, the actual processing of the phone may begin. The appropriate tools to achieve the goal of the examination have been identified in the steps described previously, and they can now ideally be used to extract the desired data from the phone.

Removable data storage cards should be processed separately from the phone when possible, as accessing data stored on these cards during the process of examining the cellular phone may alter data on the data storage card. Any installed data storage/memory cards should be removed from the cellular phone prior to examination of the phone, and processed separately using traditional computer forensics methods to ensure that date and time information for files stored on the data storage/memory card are not altered during the examination. There are situations when it may not be possible to process a removable data storage card separately from the phone, such as when the examiner lacks tools to do so, or if the data card is locked to the

phone or encrypted and cannot be accessed except through the phone. In these situations documentation of the time the phone and card were processed is especially important.

Consideration should be given to the order of the software and hardware tools used during the examination of the cellular phone. There are advantages to consistency in order of tools used during examination of a cellular phone. This consistency may help the examiner to remember the order of tools used in the examination at a later time. Also, depending on the circumstances, it may make sense to use more intrusive tools first or last during the course of the examination depending upon the goals of the exam. For example, if the goal is to extract deleted information from the physical memory of the phone, starting the examination with a physical dump of the memory (if tools for this function are available) would make more sense than extracting individual files or the file system of the phone. Performing multiple kinds of extractions from the same device may be helpful in decoding the data obtained from the phone, as well.

Verification Phase

After processing the phone, it is imperative that the examiner engages in some sort of verification of the accuracy of the data extracted from the phone. Unfortunately, it is not unusual for cellular phone tools to erroneously or incompletely report data or to report conflicting information from tool to tool. Verification of extracted data can be accomplished in several ways.

Comparison of Extracted Data to the Handset

Comparison of the extracted data to the handset simply means checking to be sure the data which was extracted from the mobile device matches the data displayed by the device itself. This is the only authoritative way to ensure that the tools are reporting the phone information correctly.

Check the Underlying Hex

If physical or file system extraction is supported, traditional forensic tools can be used for verification of extracted data by manually examining the hex and decoding the data to ensure that the results are consistent with what is being reported by the tool. This method uses traditional digital forensics methods to check the data, but requires a higher level of expertise and experience. There are a large variety of file formats and encoding methods used in various mobile devices which may prove to be a challenge when using this method.

Use of More than One Tool, Compare Results

Another way to ensure the accuracy of extracted data is to use more than one tool to extract data from the cellular phone and to cross verify the results by comparing the data reported from tool to tool. If there are inconsistencies, the examiner should use other means to verify the accuracy of

the data extracted from the phone. Even if two tools report information consistently, verification via manual inspection of the handset is authoritative because it is possible that both tools used are reporting erroneously.

Use of Hash Values
If file system extraction is supported, traditional forensic tools can be used for verification of extracted data in several ways. The forensic examiner can extract the file system of the cell phone initially, and then hash the extracted files. Any individually extracted files can then be hashed and checked against the originals to verify the integrity of individual files. Alternatively, the examiner could extract the file system of the cell phone initially, perform the examination and then extract the file system of the phone a second time.

The two file system extractions can then be hashed and the hash values compared to see what data on the phone, if any, has been altered during the examination process. Any changed files should then be examined to determine if they are system files or user files to potentially determine the reason for the changes to the files. (Murphy, 2009) It should be noted that hashing only validates the data as it exists *after* it has left the phone. Cases where the data extraction process actually modifies data have been documented in other papers. (Dankar, Ayers & Mislan 2009)

In some cases, a combination of verification techniques may be used to validate the integrity of the data extracted from the phone.

Documentation & reporting Phase
Documentation of the examination should occur throughout the process in the form of contemporaneous notes regarding what was done during the examination. Examination worksheets can be helpful in the examination process to ensure that basic information is recorded.

The examiner's notes and documentation may include information such as:
- The date and time the examination was started
- The physical condition of the phone
- Pictures of the phone and individual components (e.g., SIM card and memory expansion card) and the label with identifying information
- The status of the phone when received (off or on)
- Make, model, and identifying information
- Tools were used during the examination
- What data was documented during the examination

Most cellular phone tools include reporting functions, but these may not be sufficient for documentation needs. At times, the cellular phone tools may report inaccurate information such as the wrong ESN, MIN / MDN numbers, model, or erroneous date and time data, and so care must be taken to document the correct information after the data verification phase.

The process used extract data from the phone, the kinds of data extracted and documented and any pertinent findings should be accurately documented in reports. Even if the examiner is successful in extracting the desired data using available tools, additional documentation of the information through photographs may be useful, especially for court presentation purposes.

Time Zone / Daylight Savings Time Adjustments
Particular attention should be given to date and time stamps, which may be reported in UTC or other standardized time formats by mobile forensic software tools, while the phone itself shows local time. Most tools allow the examiner to adjust time stamps to the local time zone for reporting purposes but this is not always the case. Adjustments for time zone and daylight savings or standard time should be accounted for, as these details may be missed or misunderstood by others reading the reports. This can result in relevant data being missed by investigators after the fact, or in the appearance of a date and time conflict between the evidentiary phone and reports generated by various forensic tools. Mentioning in your report that time zone adjustments have or have not been applied may save time, confusion, and explanation of relative time differences at a later point.

Presentation Phase
Consideration should be given throughout the examination as to how the information extracted and documented from the mobile device can be clearly presented to another investigator, prosecutor and to a court. In many cases, the receiver may prefer to have the extracted data in both paper and electronic format so that call history or other data can be sorted or imported into other software for further analysis.

The investigator may also want to provide reference information regarding the source of date and time information, EXIF data extracted from images or other data formats, in order that recipients of the data are better able to understand the information.

For court purposes, pictures or video of the data as it existed on the cellular phone may be useful or compelling as exhibits. Extracted text messages may be great evidence, but pictures of the same text messages may be more familiar and visually compelling to a jury.

It is often very useful to present a series of pictures of text messages and call history logs in chronological order via a PowerPoint® presentation or timeline software so that the

progression of communications is shown clearly to the audience, whether the audience is an investigator, prosecutor, or jury. This is especially effective if there are a number of cellular phones involved in a case.

Archiving Phase

Preservation of the data extracted and documented from the cellular phone is an important part of the overall process. It is necessary to retain the data in a useable format for the ongoing court process, future reference, and for record keeping requirements. Some cases may endure for many years before a final resolution, and most jurisdictions require that data be retained for varying lengths of time for the purposes of appeals.

Due to the proprietary nature of the various tools on the market for the extraction and documentation of cell phone data, consideration should be given to the ability to access saved data at a later date. If possible, store data in both proprietary and non-proprietary formats on standard media so that the data can be accessed later even in the event that the original software tool is no longer available. It may also be a good practice to retain a copy of the tool itself to facilitate the viewing of the data at a later date.

Conclusion

With the growing demand for examination of cellular phones and other mobile devices, a need has also developed for the development of process guidelines for the examination of these devices. While the specific details of the examination of each device may differ, the adoption of consistent examination processes will assist the examiner in ensuring that the evidence extracted from each phone is well documented and that the results are repeatable and defensible in court. The information in this document is intended to be used as a guide for forensic examiners and digital investigators in the development of processes that fit the needs of their workplace.

Bibliography

Ayers, R., Dankar, A. & Mislan, R. (2009). Hashing Techniques for Mobile Device Forensics. *Small Scale Digital Device Forensics Journal* , 1-6.

Brothers, S. (2011). How Cell Phone "Forensic" Tools Actually Work - Cell Phone Tool Leveling System. *DoD Cybercrime Conferece. 2011.* Atlanta, GA

Guide for Mobile Phone Seizure and Examination. *APCO Good Practice Guide for Computer Based Electronic Evidence – Official Release Version 4.0*, 45-51.

Katz, Eric, "A Field Test of Mobile Phone Shielding Devices" (2010). *College of Technology Masters Theses.* Purdue University.

Kessler, G. (2010). Cell Phone Analysis: Technology, Tools, and Processes. *Mobile Forensics World.* Chicago: Purdue University.

Mislan, R.P., Casey, E., & Kessler, G.C. (2010). The Growing Need for On-Scene Triage of Mobile Devices. *Digital Investigation*, *6*(3-4), 112-124

Murphy, C. (2009). The Fraternal Clone Method for CDMA Cell Phones. *Small Scale Digital Device Forensics Journal* , 4-5.

Punja, S & Mislan, R. (2008). Mobile Device Analysis. *Small Scale Digital Device Forensics Journal, Vol. 2, No. 1* , 2-4.

Cynthia A. Murphy is a Detective with the City of Madison, Wisconsin Police Department and has been a law enforcement officer since 1985. She is a certified computer forensic examiner and has directly participated in the forensic examination hundreds of digital devices pursuant to criminal investigations of various types of crimes including homicides, missing persons, computer intrusions, sexual assaults, child pornography, financial crimes, and other investigations. She has successfully utilized her skills in the investigation and prosecution of numerous criminal cases involving digital evidence and has testified as an expert in both state and federal court. Det. Murphy is also a part time Digital Forensics instructor at Madison College and teaches mobile device forensics for the SANS Institute.

Author's Note: This is the third major revision of this paper, the first version of which was written and distributed in 2009. The author makes an effort to keep the information as up to date as possible, and any suggestions for revisions, additions, or for updating of its contents are appreciated and can be sent to cmurphy@cityofmadison.com.

A previous version of this paper (version 1.1.8) was cited by the U.S. 7th Circuit Court of Appeals in United States v. Flores-Lopez (http://docs.justia.com/cases/federal/appellate-courts/ca7/10-3803/10-3803-2012-02-29.pdf). If you are in need of a copy of that particular version of this paper, please contact the author for a copy.