Mobile Device Analysis

Shafik G. Punja & Richard P. Mislan

Abstract—**The increased usage and proliferation of small scale digital devices, like celluar (mobile) phones has led to the emergence of mobile device analysis tools and techniques. This field of digital forensics has grown out of the mainstream practice of computer forensics. Practitioners are faced with various types of cellular phone generation technologies, proprietary embedded firmware systems, along with a staggering amount of unique cable connectors for different models of phones within the same manufacturer brand.**

This purpose of this paper is to provide foundational concepts for the data forensic practitioner. It will outline the common cell phone technologies, their characteristics, and device handling procedures. Further data evidence storage areas are also explained along with data types found in the various storage areas. Specific information is also noted about BlackBerry and iPhone devices.

Detailed procedures for data analysis/extraction for mobile devices and how to use the various toolkits that are available is beyond the scope of this paper; the staggering numbers of cell phones and the intricacies of the toolkits makes this impossible. However, resources for the reader to further investigate the topic are attached in the appendix.

Index Terms—**Mobile Device, Cell Phones, BlackBerry, PDA, Smart Phones, Cellular Phone Generation, CDMA, TDMA, GSM, iDen, SIM, IMEI, IMSI, ICCID, ESN, MEID, PIN, PUK, Flash Memory, Memory Cards, Mobile Device Analysis, Analysis Tools, Cell Phone Forensics**

I. Introduction

THE area of digital forensics (computer forensics), has grown rapidly in the 21st century, most notably due to the increased trend in mobile devices found at technical, non-technical, and violent crime scenes. As possible sources of evidence, these devices hold a treasure trove of helpful information. Crime scene investigators commonly require the call history, contacts, and text messages from these mobile devices, but can also benefit from other sources of evidence such as photos, videos, and ringtones. Usually these personal pieces of information take investigations to the next step or lead to more questions.

Directly correlated to this growth is the increase of cellular phone usage worldwide. Globally, mobile phone subscriptions reached 3.3 billion in November, 2007, accounting for half of the entire global population [56]. In June 2007, the United States had 243 million wireless subscribers [17]. More importantly, some of the largest growth rates for cellular phone usage and market growth are occurring in China, Africa and India [17]. The staggering numbers only forewarns of the pervasiveness of mobile devices in our society and the prevalence of these devices at crimes scenes.

This article will provide a comprehensive overview of mobile device technologies, device storage of data/information/evidence, and the techniques and tools for properly handling mobile devices.

II. Mobile Devices

Let us first clarify some terms in relation to mobile devices. For the sake of this article, the use of mobile devices is not referring to thumb drives, USB drives, memory sticks portable flash drives, or portable externally enclosed hard drives. Mobile devices specifically refer to Cellular (or Mobile) Phones, Portable Digital/Data Assistants (PDA's), and Smart Phones. Bear in mind that some of the older model PDAs's, such as the initial Palm and BlackBerry series devices do not have radio (cellular) capability and are simply used to store personal information (contacts, calendars, memos, to-do lists, etc.).

Mobile Devices Representation:

1) Cellular Phones
   a) Code Division Multiple Access (CDMA) - Typically handset only
   b) Global Systems Mobile (GSM) - Handset and SIM
   c) Integrated Digital Enhanced Network (iDEN) - Handset and SIM
2) Portable Digital/Data Assistants (PDA's)
   a) Palm Pilots (Palm OS),
   b) Pocket PC's (Windows CE, Windows Mobile),
   c) BlackBerry's (RIM OS) that contain no radio (cellular) capability.
   d) Others (Linux, Newton,)
3) Smart Phones - hybrid between 1 and 2, which have radio capability.

The cell phone and data storage organizer distinctions are now becoming so blurred with the emergence of Smart Phone devices. These devices encompass the features of cell phones (radio capability) and the ability to store personal data, surf the web, send text messages (SMS) and/or multimedia messages, (MMS), check email, instant message (IM), make audio or video calls, download/upload content to and from the Internet, take pictures as well as video. Essentially, a mobile device can do much of what a computer or laptop can do, just on a smaller scale. Those with a computer forensic background, perhaps already realize the breadth of information that can be locally stored on these small scale digital devices.

III. Cellular Phone Generations and Networks

Cellular phone technology can be classified from first generation (1G) to fourth generation (4G). The first and second generation technology devices, analog based, have been phased out to make room for newer generation devices and networks. This does not mean to say that analog no longer exists, but in fact that it is used as a secondary technology in areas where digital coverage is lacking. That said, in the United States, the analog network technology will no longer be required after February 18, 2008 [21]. Although analog drains battery life quicker on devices and the call quality is not as good as digital network technologies, it does provide a longer range between cell towers.

The breach of the 2G barrier introduced a transition from analog to digital voice. The 3G, 3.5G and 4G landmarks represent a marked increase in network bandwidth for cellular devices, simply translating to higher speed data access. This allows more functionality from a device in being able to access content from the Internet or through the network service provider (NSP) [28].

There is a cell phone network classification known as TDMA (Time Division Multiple Access). It falls under the second generation (2G) digital cellular phone technology which uses an allotted radio channel divided into time slots, allowing each time slot to handle one call. There are several variations of TDMA, of which the more common are GSM (Global System for Mobile Communication) and iDEN (Integrated Digital Enhanced Network) [38].

There are predominantly three types of cell phone networks in North America [13]:

A. *Code Division Multiple Access (CDMA)*

Originally a 2G, digital technology, it was developed by Qualcomm which uses a spread spectrum technology using a special coding scheme thereby allowing multiple digital signals on the same channel. This technology is more efficient and less costly to implement and is considered more secure than other cellular phone network technologies. CDMA has also evolved from the original 2G standard into CDMA2000 and its variants such as CDMA2000 1X (or more commonly 1X), CDMA1X EV-DO (evolution data optimized), CDMA1X EV-DV (evolution data voice), and CDMA2000 3X. These variants represent an increase in data bandwidth from 140 kbps (kilo bits per second) up to 5 Mbps (Megabits per second). The CDMA network technology competes with the GSM standard for cellular dominance [38], [16].

CDMA devices have the following characteristics:

- Electronic Serial Number (ESN): This number is found on the compliance plate located under the phone battery and can be displayed as ESN DEC, ESN HEX, ESN or D. The ESN is a unique 32 bit number assigned to each mobile phone on a network. You will note that the ESN in its decimal format contains only decimal numbers, distinguishing it from its ESN HEX equivalent which will contain both decimal and alpha characters.
- Mobile Equipment ID (MEID): This number is 56 bits long, replacing the originally used ESN, because of the limited availability of the 32 bit ESN numbers.
- While CDMA phones do not normally utilize a Subscriber Identity Module (SIM), there are newer hybrid phones that can operate as both CDMA and GSM. Notably, there will be a slot for the SIM and the compliance plate may also contain an IMEI number in addition to the ESN/MEID number.
- Re-Useable Identification Module (RUIM): This card has been developed for CDMA networks similar to the SIM in GSM networks [13].

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

Globally, GSM is the most dominant mobile phone network. As mentioned earlier it is originally a 2G digital technology based on TDMA. In the United States it operates on 1.9 GHz and 850 MHz bands. While in Europe it uses the 900 MHz and 1.8GHz bands. In Canada, Australia and most South American countries the 850Mhz band is utilized. GSM was first deployed in Europe in the early 1990's and was the first 2G technology to allow limited text messaging (SMS - short message service). Like CDMA, GSM has evolved into third generation (3G) extensions which allow for higher data rates. These extensions can be commercially recognized as GPRS (General Packet Radio Service), EDGE (Enhanced Data Rates for GSM Evolution), 3GSM and HSPA (High Speed Packet Access) [38], [24].

GSM Devices have the following characteristics:

- International Mobile Equipment Identifier (IMEI) - this is a unique 15 digit code and used to identify a GSM cell phone to its network and is found on the compliance plate. This code also code identifies manufacturer, model type, and country of approval of a handset. On most GSM based handsets typing in *#06# will display the IMEI. It can also be accessed through NANPA: http://www.numberingplans.com/?page=analysis &sub=imeinr
- Subscriber Identity Module (SIM): There will be *at least one* slot for this card usually found under the battery panel. The face of this card may also contain the name of the network to which the SIM is registered to. (More information on the SIM is presented later in this article).
- Integrated Circuit Card Identification (ICCID): This is a 18 - 20 digit number (10 bytes) imprinted on the face of the SIM. This number uniquely identifies each SIM. This number is tied to the IMSI which is associated to the IMEI when a handset is registered to a GSM network.
- International Mobile Subscriber Identity (IMSI): This number is typically a 15 digit number (56 bits) that consists of three parts, stored electronically in the SIM:
  - Mobile Country Code (MCC)
  - Mobile Network Code (MNC)
  - Mobile Station Identification Number (MSIN)

  The IMSI can only be obtained either through analysis of the SIM or from the NSP (Network Service Provider). The IMSI can be analyzed through NANPA: http://www.numberingplans.com/?page=analysis &sub=imsinr
- Dual SIMs: Newer generation mobile phones, particularly outside of North America may contain dual SIMs. This allows for multiple phone numbers being assigned to one device, which are both simultaneously active. For more information: http://www.fonefunshop.co.uk/dualsim/dualsimcovers.htm

C. Integrated Digital Enhanced Network (iDEN)

In North America, the Integrated Digital Enhanced Network (iDEN) is a Motorola proprietary variant of TDMA and GSM that operates in the 800 MHz, 900MHz, and 1.5 GHz bands. Also using a variant of SIM technology, iDEN adds a unique two-way radio system known as push-to-talk (PTT), or more accurately MotoTalk.

iDEN devices have the following characteristics:

- International Mobile Equipment Identity (IMEI): This is a unique 15 digit number and is used to identify an iDEN cell phone to its network and is found on the compliance plate. This code also code identifies manufacturer, model type, and country of approval of a handset.
- IMSI can only be obtained either through analysis of the SIM or from the NSP (Network Service Provider). The IMSI can be also analyzed through NANPA: http://www.numberingplans.com/?page=analysis&sub=imsinr
- Subscriber Identity Module (SIM): iDEN uses a different implementation of SIMs and are not compatible with GSM phones. Four different sized SIMs exist, ”Endeavor” SIMs contain no data, ”Condor” SIMs are used with two-digit models using a SIM with less memory than the three-digit models, ”Falcon” SIMS are used in the three-digit phones, and will read the smaller SIM for backward compatibility, but some advanced features such as extra contact information and possibly GPS reception is disabled. There is also the ”Falcon 128” SIM, which is the same as the original ”Falcon”, but doubled in memory size, which is used on newer three-digit phones.
- Direct Connect Number /Radio-Private ID/MOTOTalk ID/iDEN Number: iDEN use a number based on the following format for communicating device-to-device: 012*345*67890. The first three digits (012) make up the Area ID (region of your home carrier’s network). The next three digits (345) define the Network ID (specific iDEN Carrier such as Nextel, SouthernLink, Nii, MIKE/Telus, etc.) and the last five digits determine the Subscriber’s ID (personal number from home carrier’s network, sometimes the last five of the phone number). The asterisk (*) is also part of this Direct Connect Number used as a separator to divide each of the aforementioned parts.

INVESTIGATIVE TIP: The hardware information discussed above can be associated back to customer identifying data. In other words who is owner of this device? This can be especially useful if the handset is locked and all you have is the information from the compliance plate and/or SIM. You will need to provide the NSP (Network Service Provider) with the hardware information to obtain the ownership records. The NSP may require a judicial authorization (i.e.: search warrant, subpoena) prior to releasing such records.

IV. Data/Information/Evidence in Mobile Devices:

A. Handset Memory

Various types of data (digital evidence) can be obtained from the handset memory. The following is a list that describes the various types and data storage implementations:

- Audio Files (Music and Voice)
- Calendar Entries
- Call History (Inbound and Outbound)
- Contacts/Phonebook
- Email
- Internet History
- Instant Messaging (IM) chat
- Memos
- Multimedia Messages (MMS)
- Pictures
- Short Message Service (SMS) or Text Messages
- System Firmware Information
- T9 Dictionaries
- Telecommunication Settings
- Videos
- Voice Mail

Recovery of deleted content is currently, is very challenging and is influenced by a number of factors such as:

- Analysis tool
- Proprietary file systems
- Vendor installed files and configuration of the device
- Technical skill of the examiner

1) 1.1 Internal/Embedded Memory: The term ”embedded memory” refers to on board flash memory capacity built into the handset. Older generation devices had a small capacity to store data as compared to the newer generation devices.

Flash memory consists of two types (Kim, Hong, Chung and Ryou, 2008; McCullough 2004; Flash Memory, Wikipedia):

1) NAND (Not AND): Stores data but not execute programs. Software stored in this area must be copied to NOR flash memory or RAM for execution. This memory works faster and is more durable than NOR. You can find NAND memory in USB flash drives, and most memory card formats.
2) NOR (Not OR) - can store and execute software and is found in PDA’s, cell phones and digital cameras.

Certain models of devices have flash memory that when the battery fails or is exhausted, all user data is lost [35]. This behavior has been encountered specifically with older models of Palm Pilots and HP iPaq. If a device is recognized that is susceptible to this, prudent steps should be taken to acquire the data from this device prior to battery failure. Or at the very least keep the device charged if the charging cable or cradle is available.

2) 1.2 Hard Drive Memory: As surprising as it may be, technological advancements have enabled cell phone manufacturers to now use 1 inch compact drives, similar to the ones found in portable music players (like Apple’s iPod). Storage capacity can range from 3 gigabytes (GB) to 12 GB and upwards. Traditional forensic tools (EnCase, Forensic Toolkit (FTK), Pro Discover, iLook, Win Hex) could be used to analyze this type of memory. However, because these devices could contain proprietary files systems, it may be difficult to interpret.

B. 2. SIM

What types of data (digital evidence) can be found on a SIM?

- Last Number Dialed (LDN)
- Phonebook/Contacts (ADN)
- Text Messages (SMS), including deleted text messages
- Location information (LOCI) from position of last usage
- Service Related Information

The SIM is essentially a type of smart card that contains a 16 - 128 kb EEPROM (Electronically Erasable Programmable Read Only Memory) [35]. The SIM is assigned the cell phone number from the network which is tied to its ICCID, IMSI number as well as the IMEI number of the handset.

The SIM file system is hierarchical in nature consisting of 3 parts:

1) Master File (MF) - root of the file system that contains DF's and EF's
2) Dedicated File (DF)
3) Elementary Files (EF)

A SIM could potentially be moved between various types of GSM cell phones. The implication here is that a suspect can store specific information such as text messages and contacts only on the SIM. The cell phone then only acts as a shell, and the SIM can be then be moved to another ”network unlocked” cell phone. In most GSM devices the SIM is required to successfully boot the phone.

C. 2.1 USIM (Universal Subscriber Identity Module)

This is the evolution of the SIM for 3G devices. It can allow for multiple phone numbers to be assigned to the USIM, thus giving more than one phone number to a device [45].

1) 2.2 SIM PIN1, PIN2 and PUK1, PUK2 codes [35], [58]:

a) 2.2.1. PIN (Personal Identification Number):

- PIN1 code allows access to the handset
- user generated, 4-8 digits in length
- 3 incorrect attempts allowed before the SIM becomes locked
- Correct PIN will reset the counter for attempts
- Lock out requires PUK

b) 2.2.2. PIN2:

- Minimum of 4 digits
- protects network settings
- is used for billing and fixed dialing purposes
- since PIN2 code manages restriction of a small set of features, the PIN2 lock will not affect access to those handset features controlled by PIN1

c) 2.2.3 PUK (Personal Unlocking Key):

- PUK1 code typically can only be obtained from NSP
- 8 digits in length
- 10 incorrect attempts to enter this code correctly before the SIM is permanently locked out, which then must be returned to the NPS for reactivation
- With some service providers the PUK is provided with the SIM when you purchase the SIM with airtime
- Some NSP's may provide an online way to access the PUK for a registered subscriber

d) 2.2.4. PUK2 is used to unblock PIN2 and is obtained from the NSP.: No hardware/software tool currently exists that will allow an examiner to crack, bypass, or determine the PIN/PUK codes. An examiner will not be able to read the file system of a PIN or PUK locked SIM without the appropriate unlock code.

D. 3. Memory Cards (micro SD or TransFlash)

What types of data (digital evidence) can be found on a memory cards?

- Pictures
- Movies
- Audio Files
- Documents

These removable flash memory cards can be found mainly in cellular phones. But can also be used in GPS devices, portable audio players, video game consoles and expandable USB flash drives. The capacity of micro SD/TransFlash memory cards currently range in storage size from 64 MB (megabytes) to 8 GB (gigabytes) and upward. They are very small in physical size, about the size of a fingernail, making them much smaller than their digital camera memory card counterparts [39].

The location on a mobile device, as to where a memory card can be found varies depending upon the manufacturer. It is strongly recommended to check each device thoroughly to determine whether it contains a memory card. If unsure, then consult the device's user guide. On the outside of a device, there is usually a small port cover that will have an inscription of ”micro SD” or ”TransFlash”. Opening the port cover will reveal a slot for the memory card. If the memory card is inside this slot simply push on the card and it will eject from the slot. The other location, for a memory card slot on a mobile device, is under the battery cover. Remove the cover and the battery, and near the compliance plate there should be a small metal hinged door that covers the memory card, or the card may be inserted into the body of the device that borders the inside edge of the battery cavity, away from the compliance plate.

Typically these cards contain a FAT16 file system (although FAT12 has been observed). The cards listed at or exceeding the 4GB capacity are categorized as Secure Digital High Capacity (SDHC) and may use a FAT 32 file system to support partition sizes greater than 2GB [39]. A memory card with a unique proprietary file system, may be encountered, that is used by the device, in which a traditional forensic data analysis approach will not work. In one example an examination of a micro SD card from a Nokia (Symbian based) contained a proprietary file system. With the card write-protected and not write-protected it was not able to be read, nor was the file system interpreted. When the card was re-inserted into the device it showed that there were files on it. There are no known tools that have been encountered which are able to interpret all the proprietary file systems of the mobile devices that are currently on the market.

The most commonly found data types on microSD/TransFlash cards are: Video, Pictures and Music. Because of the native Windows based FAT file systems typically used on these memory cards, the recovery of deleted content is much more viable using tools like EnCase or FTK.

Video files can be stored on either the device's internal memory or the memory card. It is much easier to recover a data file stored on the memory card as opposed to the device's embedded memory.

Video taken with a mobile device is stored in a 3GP multimedia container format. There are two types of 3GP formats: .3G2 (CDMA based devices) or .3GP (GSM based devices). The file name is followed by a dot "." and then the file extension of either 3g2 or 3gp based on the device network type. These video formats are a simplified version of the MPEG-4 or mp4 and were designed specifically for mobile phones [2]. 3GP video files can be viewed in their native file format on a computer using RealPlayer, QuickTime Media Player Classic, or VLC media player.

At the binary level 3GP data is stored *big-endian* first, meaning that the most significant bytes are stored first. Both EnCase and FTK (Forensic Toolkit) can be used to analyze these flash cards. Both tools have will observe these files as an unknown file type from a file signature perspective. Although FTK 1.7x did attempt to resolve this partially in that it does recognize .3gp but not .3g2. Based on the file header, the video file can be carved from unallocated clusters.

E. 4. Network Service Provider (NSP) [58]

What type of information may be available from a NSP, given proper consent from the NSP or judicial authorization?

- Subscriber Information
- Call Data Records - related to phone calls and text messages
- Subscriber Location - this relates to geo location of the physical device, in an effort to track the subscriber

INVESTIGATIVE TIP: Remember the handset memory can only retain a limited amount of information. For example you may only find 10 to 30 numbers in the call history. If you are looking for call history beyond what the device contains or realize the handset's call history has been purged then you will have to seek assistance from the NSP. Each NSP will have their own policy with respect to how much information they may store and what type (call history, text messages, uploaded content from the device) and the length of time they will store it. Contact the NSP and ask them to preserve the data, and advise them that you will be seeking release of this information and then find out what type of judicial authorization is required.

V. Device Handling & Procedures

The following are suggested best practice guidelines for handling mobile devices and subsequent analysis:

A. 1. Documentation/Notes

- Specific location where device is found at the scene, and/or the chain of custody as evidence transferred from the investigator to the forensic examiner.
- Note any physical issues with the device (boot failure, damage, broken display etc.).
- Photograph all external aspects of the device.
- Seize any manuals, chargers, batteries associated to the device.
- If the device keypad is manipulated to view information, document or photograph what was done and the information gained through user action.

B. 2. Device Shielding/Isolation (Protection and Preservation of Evidence)

The Mobile Phone Forensics Sub-Group of the Interpol European Working Party on IT Crime (2006) has identified that mobile devices should be isolated from other devices they may be connected to and also from the radio network. If a device is found connected to a computer, pull the plug from the back of the computer to prevent data synchronization or overwrites. Similarly isolating the device from the NSP will also prevent new data traffic from affecting the current data stored on the device. An example of this would be call history logs being affected by an incoming call, which can overwrite the oldest incoming call log, depending upon the storage capacity of the device [35].

A device can be isolated from its network in several ways:

1) Jammer or spoofing device
   - Will create a temporary dead zone to all cell phone traffic in the immediate proximity depending on the source power of the jammer.
   - Considered a violation of the Communications Act of 1934 in the United States [20].
2) Radio shielded bag or container
   - Will cause device to increase its signal strength causing the battery to drain faster and eventually exhaust.
   - Will eventually lead to battery exhaustion. This can activate the handset lock for the device and/or the PIN for the SIM, thus preventing data analysis. It will cause data loss on devices whose volatile memory is dependant on battery power.
   - Either way the device needs to be charging while inside the shielded environment.
3) Airplane mode
   - Requires user input on keypad; it severs radio connection with the network and is not always in the same location on every device.
4) Turning the device off
   - This will activate handset lock codes for the device and/or the PIN for the SIM, if they have been user enabled. This could likely render the device and/or SIM memory inaccessible for analysis.
5) Network Service Provider
   - NSP could disable device from the network. This depends on obtaining cooperation from the NSP and may not be practical for every case.

Radio isolation will prevent remote locking or wiping of a device. It also prevents the device from receiving new data from the NSP thereby overwriting possible evidence. The device when seized should be placed into an antistatic radio isolation bag/container. Ideally the device should also be analyzed in a radio isolated environment.

C. 3. Device State - On or Off

If the device has been brought in for analysis or it is found on scene, note its state - on or off. If the device is on, note its date and time, and note any inconsistencies by comparing it to actual date and time. The time on a device may be set independent of the NSP and may be affected by the radio isolation. Also a device that is no longer registered with the NSP regardless of network type may not have date/time values that match actual on comparison.

If the device is off, the time and date comparisons can be completed once the device is turned on. Turning the device on will affect its position regarding location. ***If the location or position of last usage is critical the investigator, this data should be secured first through collaboration with the NSP, prior to analysis of the device.***

D. 4. Device Identification

Attempt to document the following about the device first without affecting its state:

- Make, Model
- Vendor Logo
- Style (flip/clam or slide)
- External Memory card slot (miniSD or TransFlash)
- Digital Camera (location - front or back of device)
- Compliance Plate (ESN/MEID or IMEI) and SIM (ICCID) information only if device is in an off state. On some devices, like PDA's or Palm Pilots you will not be able to remove the back cover and the compliance information will be on the back of the device.
- Download the user manual for the device to understand the device's features

Turning a device off that is already on, to examine the compliance plate located in the battery cavity will initiate security/authentication mechanisms if they have been enabled, rendering the device inaccessible. A secondary effect that may be observed, by removing the battery from a powered off device, is the system date and time being reset to default values.

E. 5. Device Analysis Procedure and Data Extraction/Capture

If the device is not recognized or a similar one has never been analyzed, obtain an e-copy of the user manual to familiarize yourself with the device's features and navigation. Next, check forensic examiner web forums to see if another examiner has already analyzed the device. There are several web-based resources (which are listed further below under Resources) that keep a database of devices and what tools have worked successfully. Ensure that the device's battery contains at least 50% charge prior to analysis.

You will very likely need multiple toolkits as no one toolkit can currently extract everything from a device. Remember to look up the toolkit's specific device supported section to see if the device is supported for data extraction.

1) 5.1. Device in Off state: Proceed with external examination/documentation of device. If the device contains any SIM or memory cards, analyze these first. Ideally these should not be placed back into the device, as data could be written to either on power up.

SIM analysis first will preserve the position of last usage information, and allow extraction of any deleted text messages from the SIM. Deleted text messages on a SIM cannot be extracted through the device (while the SIM is inside the device).

To preserve the original SIM, an examiner *should ideally* also clone the SIM and use the cloned card inside the device during device memory analysis. A cloned SIM will mimic the identity of the original SIM and will not allow network access.

If a memory card is found, take the appropriate steps to write protect the card, and then image/analyze with traditional forensic tools (EnCase, FTK, WinHex, ProDiscover, iLook). There are USB card readers that can accept miniSD and TransFlash cards, or using a card reader adapter, you can attach the USB card reader to a USB write blocker (Tableau USB Bridge) and make a forensic image.

Internal memory analysis of the device (in an off state) should occur last. Ensure the device is radio isolated during analysis.

2) 5.2. Device in On state: Proceed with data extraction or capture of the device. As mentioned earlier, power cycling the device, can cause the device to initiate authentication mechanisms. Once data extraction from handset is completed then check the device for SIM and/or memory cards. Complete data extraction on these cards as described in 5.1 above.

3) 5.3. Battery Exhaustion Leading to Data Loss: If the device is of a type where battery exhaustion will cause data loss, either extract data immediately or keep the battery under charge until the device can be analyzed (in a radio isolated environment).

4) 5.4 GSM Devices without a SIM: Upon powering up a GSM device that does not contain a SIM, the LCD display will usually prompt ”Insert SIM”. Without the last used SIM from the specific device, an examiner will not be able to successfully power on the device. However, not all GSM devices require a SIM to properly power up.

In this case, there are two options that an examiner can explore:

5.4.1. It is strongly recommended to make a forensic clone of the SIM that was last used in the device [48]. This can be determined by taking the IMEI of the GSM device, and requesting the NSP to provide the last known ICCID and IMSI that was used for that device, provided the appropriate documents are served on the NSP. The ICCID and IMEI numbers are then used to make a forensic clone on a SIM, using software such as Smart Card Pro (http://www.scardsoft.com/). With the forensically cloned SIM inserted into the device, the GSM handset is then successfully powered up without causing data loss on the device.

5.4.2. In the absence of a tool that can create a forensically cloned SIM, an examiner can try and use a ”blank” SIM that has never been activated, in order to successfully boot the device. *This should be used only as a last resort method.*

According to Reiber (2008) inserting a foreign SIM into the GSM device will cause the loss of handset data, as the GSM device will search for the last known ICCID and IMSI numbers.

5) 5.5 Device Connection: According to the Good Practice Guide for Mobile Phone Seizure & Examination [33] there are currently three possible connection options (listed in order of preference), that can allow data extraction:

5.5.1 *Cable* - the most secure, and reliable with the least amount of impact with respect to data change relative to IR or BT.

5.5.2 *InfraRed (IrDA)* - less secure and less reliable; will require the examiner interact the device to enable/activate *IrDA*

5.5.3 *BlueTooth (BT)* - least secure of all; will require interaction with device interface to activate, and data will be written to the handset during the BT authentication process

Most 3G and above devices contain all three; however analysis software suites may not take advantage of all three options of data extraction and will often recommend a preferred method of connection depending on the tool supplier.

6) 5.6 Screen Display Capture (last resort):: Should no toolkits acquire or extract the data, an examiner will have to rely on taking a digital photograph of the LCD display, showing the information that is of interest. An examiner can do this by using either a professional quality digital camera with a macro lens or tools such as Fernico ZRT or Project-a-Phone.

VI. TEXT MESSAGES (SHORT MESSAGE SERVICE - SMS)

Text messages (SMS) can be a great source of evidence, considering that the CTIA (Cellular Telecommunications & International Association) reports that, by June 2007, over 28.8 billion text messages were sent per month in North America.

SMS deleted from a handset may be recoverable, to a far lesser degree than those deleted from a SIM. The examiner will need to access the file system, at least from the logical level in order to examine the folder/file structure where the messages are stored.

SMS can be sent in one of three ways:

1) Device to Device - using the Text Message or Messaging Feature on the handset to create the message. A copy of the message could be saved in the Sent folder on the handset.
2) Web Interface to Device - using the NSP provided or third party provided website to send SMS to a device from an Internet connected computer.
3) Email Client or Webmail Client - this is like sending a regular email except in the ”To” field the sender's address is formatted as a syntax which includes the area code and cellular phone number (10 digit phone number) as part of the prefix before the ”@” symbol and the domain of the NSP as part of the suffix after the ”@”. This message would be sent as an email from the computer and received by the mobile device as a text message. Depending on the email client or web mail client, a copy of this message may be stored in the ”Sent Items” folder.

When sending a text message to a cell phone using Outlook the following information can be viewed in ”To” field: To:4031234567@msg.telus.com

4031234567 = 10digitphonenumber msg.telus.com = the domain naming convention that Telus uses; this will vary from NSP to NSP.

Rogers for example uses this convention, 10digitphonenumber @pcs.rogers.com

An examiner could also examine the text message headers, if available, like email headers, looking for IP addresses, in an attempt to determine the origin of the message. The header information may be retained on the device and/or at the NSP. Remember with the amount of SMS traffic that goes across the ”wire”, the header data may not be retained for too long. Obtaining assistance from the NSP and requesting the preservation of the data in question is strongly recommended.

VII. PIN PROTECTED DEVICES

It is important to note that on CDMA handsets there is only the handset PIN to contend with. But on GSM devices, there may also be a handset PIN in addition to the SIM PIN that can be set by the user.

1) Try the default codes that are found in the user manual, bearing in mind that on SIMs and BlackBerry's and iPhone's there are a limited number of attempts.
2) The last 4 digits of the phone number assigned to the device are commonly used as the PIN for the handset.
3) Obtain the PIN from the owner of the device, if possible.
4) Contact NSP or device manufacturer to exploit vulnerabilities.
5) Brute force, through automated key stroke entry of devices that have no password attempt restrictions. This approach has been employed by the Netherlands Forensic Institute [35].
6) Last option could be to search hacker, and developer web sites for device exploits.

VIII. BLACKBERRY (BB)

This device is produced by Research In Motion (RIM) and has its own proprietary operating system. There are CDMA, GSM, and iDEN versions of BlackBerry's. In addition to the either an ESN/MEID or IMEI number on the compliance plate, a PIN will also be observed on each BB device. The PIN is unique to each BlackBerry and consists of 8 alpha numeric characters. Message pathways for all BB devices are set up as follows: first through the NSP where the device is hosted and then through a RIM Relay maintained by RIM in Waterloo, Ontario, Canada, their worldwide corporate headquarters.

A. BlackBerry Messaging

There are several messaging options with a BlackBerry device.

1) PIN to PIN
2) SMS
3) MMS (Multimedia Messaging Service)
4) Email

According to BlackBerry Enterprise Solution Security Version 4.0.x Technical Overview paper, the following is stated on PIN, SMS and MMS messaging with respect to BlackBerry devices:

> ”A PIN uniquely identifies each BlackBerry device on the wireless network. If a user knows the PIN of another BlackBerry device, they can send a PIN message to that BlackBerry device. Unlike an email message that the user sends to an email address, a PIN message bypasses the BlackBerry Enterprise Server and the corporate network.
>
> During the manufacturing process, RIM loads a common peer-to-peer encryption key onto BlackBerry devices. Although the BlackBerry device uses the peer-to-peer encryption key with Triple DES to encrypt PIN messages, every BlackBerry device can decrypt every PIN message that it receives because every BlackBerry device stores the same peer-to-peer encryption key. PIN message encryption does not prevent a BlackBerry device other than the intended recipient from decrypting the PIN message. Therefore, consider PIN messages as scrambled-but not encrypted-messages.
>
> You can limit the number of BlackBerry devices that can decrypt your organization’s PIN messages by generating a new peer-to-peer encryption key known only to BlackBerry devices in your corporation. A BlackBerry device with a corporate peer-to-peer encryption key can send and receive PIN messages with other BlackBerry devices on your corporate network with the same peer-to-peer encryption key. These PIN messages use corporate scrambling instead of the original global scrambling. You should generate a new corporate peer-to-peer encryption key if you know the current key is compromised. You can update and resend the peer-to-peer encryption key for users in the BlackBerry Manager.
>
> SMS and MMS messaging are available on some BlackBerry devices. Supported BlackBerry devices can send SMS and MMS messages over the wireless TCP/IP connection between them. The BlackBerry device does not encrypt SMS and MMS messages.”

This being stated, the forensic examiner/analyst should keep in mind that access to the Blackberry Enterprise Server (BES) is equally as important as access to the device as a backup of the BlackBerry data can be stored upon the server, including PIN messages. PIN messages are routed using the PIN number of the BlackBerry and are not associated to the recipient’s or sender’s email address. PIN messages can also be sent via the Web [57].

B. BlackBerry Security Mechanisms

Password protection can be applied to a BB device. The password length can vary depending upon the content protection strength, which is level 0 by default. It can be either user or administrator configured. There are a maximum of 10 attempts allowed. Password tampering, in attempt to unlock the device, can reduce the number of attempts by half, if Duress Notification IT policy is enabled. Or worse, initiate a device wipe that completely overwrites the data if the incorrect password is typed 10 times, if the Set Maximum Passwords Attempts Policy rule allows. According to RIM there is no back-door to unlock a password protected device [15].

A BlackBerry (Java based version 4.2 and higher) attached to a BES, version 3.6 and higher, can be remotely wiped from the BES server through the Erase Data and Disable Handheld command, if the device can receive a signal. Radio isolation in this instance is critical to preserving the data.

The device wipe function deletes all data in memory and overwrites the memory area with zeroes. Additionally if content protection is enabled, this will further cause a memory scrub which will overwrite the flash memory file system. The memory scrub process is compliant with Department of Defense directive 5220.2-M and National Institute of Standards and Technology Special Publication 800-88 [49].

Content protection can be enabled by either the user or administrator. This is designed to protect user data such as Email, Calendar, BlackBerry Browser, Memopad, Tasks, Contacts, Auto Text. Third party security applications like PGP can be added for further content encryption.

Memory cleaning can also be initiated by the user which will cause the memory cleaner program to run. This program can be configured to run automatically according to RIM when the:

1) user synchronizes the BlackBerry device with the desktop computer
2) user locks the BlackBerry device
3) BlackBerry device locks after a specified amount of idle time
4) device is holstered
5) user changes the time or time zone on the BlackBerry device

There is no information, at present, to suggest an SD card inside the device is affected by either the remote wipe or the memory cleaner.

The memory cleaning behaviour can be observed within a virtual environment. An examiner would need to create a IPD file from a device that has been configured for memory cleaning and then load the IPD (Inter@ctive Pager Backup) file into a BlackBerry simulator specific to the actual model. The IPD file is a database file that contains the user settings and data of a BlackBerry.

BlackBerry devices have an auto power-on feature. When the battery reaches a certain level of charge it will cause the device to power on automatically. At this point the battery is still in a weak enough state that the radio feature is disabled. The date/time stamp will likely not match to actual date/time in this instance. When the battery level is strong enough (approximately 25 percent charge), the radio feature will enable itself and connect to the NSP, which may cause the date/time to update from the network if this feature is enabled on the device.

C. BlackBerry Examinations

Examination of BB devices is treated no differently than the steps described in Device Handling & Procedures explained earlier. The acquisition of data from a BB device requires that an examiner make an IPD file. The .IPD (Inter@ctive Pager Backup) file contains a backup of the BB device database. Using the BlackBerry Desktop Manager software, selected or all databases can be backed up while the BB device is connected through a USB cable to the acquisition computer.

Another alternative for an examiner is to use commercially available forensic software like Paraben Device Seizure, CellDEK, or Secure View for Forensics to make an acquisition of the data stored on the BB. These tools use their own proprietary format for data extraction. In addition, they may not support acquisitions of certain models of BB devices. It is strongly recommended that an examiner always create an IPD file, regardless of the toolkit that is used. The IPD file format provides much more flexibility for analysis. It can be imported into Paraben Device Seizure for parsing as well as dumped into either FTK or EnCase for data carving, and the IPD file can also be loaded it into a BlackBerry simulator.

An examiner should try to have the following tools at their disposal when commencing BB analysis:

1) BlackBerry Desktop Manager (free download from RIM's website) - this tool is used to create the IPD file as well as restoring the IPD file into a BlackBerry simulator.
2) BlackBerry Simulator (free download from RIM's developer website) - specific to the model you are examining; allows the evidence IPD file to be viewed in a virtual environment.
3) Process Text Group's Amber BlackBerry Converter - outstanding tool (very inexpensive to purchase) that will parse the IPD only; allows an examiner to export the information to various reporting type formats.
4) Paraben Device Seizure - is able to parse the IPD file, or allows an IPD file to be imported for analysis. Pictures can be recovered in unallocated areas by using Paraben to view the binary files of the IPD databases which can then be dumped into either EnCase or FTK for data carving.

Using at least tools 1 - 3, above, there is not a Blackberry (that is not PIN protected) which cannot be analysed. On a PIN protected BB, the data extraction tools will prompt the examiner for the PIN. The PIN needs to be typed in by the examiner for a successful extraction to occur.

Remember even if a BB device is radio isolated, its local device settings, can cause user created data to be wiped as it is being analysed.

More information regarding BlackBerry analysis is listed in the appendix. These articles provide an overview on how to create an IPD file of the BlackBerry, and then how to ”mount” or use the IPD file in a BB simulator, allowing the suspect device to be viewed within a simulated virtual environment.

IX. Personal Digital Assistants

These devices contain the following hardware components: microprocessor, ROM (Read Only Memory), RAM (Random Access Memory), LCD (Liquid Crystal Display), and a variety of hardware keys and interfaces. The device can also contain expansion slots for memory cards, and wireless network cards; in addition they can also come equipped with InfraRed, BlueTooth and built-in wireless. They are usually powered by batteries. User data is normally stored in RAM) which is kept active through powered batteries. Failure of a battery will lead to data loss. The Flash ROM is where the operating system is stored [10].

All PDA types, support PIM (Personal Information Manager) applications, such as contacts, calendar, email, tasks and notes. This data can be synchronized with a computer/laptop using synchronization protocols specific to the device: Microsoft's Active Sync or Palm's Hot Sync.

PDA's have 4 generic states [55] , [10]:

1) Nascent State - first released by manufacturer with default settings, and contains no user data.
2) Active State - device is on and performing a task.
3) Quiescent State - power preservation mode to preserve battery life.
4) Semi - Active State - in between active and quiescent, triggered by timer, dimming display, to initiate battery preservation.

PDA Analysis Issues [55]:

1) Power needs to be maintained in order to prevent user data loss. Thus, in addition to seizing the device, the docking cradle is just as critical.
2) PDA's operating systems and platforms are varied: Windows, Linux, Palm, Java
3) Integrity of forensic images is difficult to maintain; two consecutive forensic acquisitions may not be forensically identical, likely because acquisition is an active state (device is on).
4) File recovery can be difficult due to memory reorganization.

Palm Operating System [55], [10], [23]

- Various Palm OS Licensees (Palm, Handspring, Sony, IBM etc).
- Older Palm OS's (less than version 5) have no access control, memory protection. User can directly access hardware through software.
- RAM (volatile) stores user data; contents lost when power removed.
- Flash ROM stores OS; contents preserved even when power removed.
- Data is stored in databases in sequence memory chunks referred to as records.
- Database headers: creationDate, modificationDate, lastBackupDate.
- Palm File Format (PFF) consists of the following file types:
  - Palm Database (PDB) - stores application or user data
  - Palm Resource (PRC) - contains user interface elements and code; very similar in structure to PDB.
  - Palm Query Application (PQA) - contains World Wide Web content.

- Hard Reset - data in RAM lost; ROM unaffected.
- Soft Reset - records that are marked for deletion are removed.
- HotSync - records that are marked for deletion are removed.
- Battery still loses power while in off state when not charging.
- Device needs to be placed into Console Mode for acquisition by Paraben Device Seizure or EnCase. This is user initiated and allows the data to be accessed via cable connection using the toolkit of examiner's choice.
- ABC Amber Palm Converter (free software) that will convert your PDB and PRC (Palm) files to various formats (PDF, HTML, CHM, RTF, HLP, DOC, and many more).

Pocket PC [10]

- Microsoft based operating system first released as Windows CE (WinCE). This later evolved to Windows Mobile.
- PIM data resides in RAM normally.
- ROM contains OS and support applications.
- Windows CE file system stores a file with same name in both RAM and ROM; the RAM file supersedes the ROM file.
- User only has access to the RAM version until it is deleted.
- ROM file accessible when RAM file is deleted.
- Windows CE registry is a database storing system, applications and user settings; and is always stored in RAM; default registry file stored in ROM.
- User has ability to set power on password of either 4 digit numeric or 29 alphanumeric characters; if password is forgotten the only way to unlock the device is to perform a hard reset, which will erase user data in RAM and perform data resynchronization if the device is connected to a laptop/computer with a backup of the original data.
- Windows CE supports four types of memory:
  - RAM - data storage and program execution.
  - Expansion RAM
  - ROM - contains boot loader
  - Persistent Storage - external memory cards

Linux [55]

- The most popular Linux distribution for PDA's is called Familiar.
- Data on Familiar OS is stored in ROM or removable memory card, unlike the Palm OS and Pocket PC OS.
- Thus data loss does not occur when battery is depleted or if a hard or soft reset is performed on the device.
- Familiar uses a JFFS2 (Journaling Flash File System, Version 2).
- Other Linux distributions, like Zaurus use the ext2 file system.

PDA Tools

- EnCase
- Paraben's Device Seizure (formerly two separate tools, Cell Seizure and PDA Seizure).
- pdd (Palm dd) - Windows based command line tool written by Joe Grand in 2002; supports only serial port connection.
- Palm OS Emulator (POSE)
- Pilot-link - open source tool for Unix.
- dd (Duplicate Disk) - creates a bit image of device; this command executes directly at the PDA and must be invoked through command line or remote connection [55].

More information regarding Palm/PDA analysis are listed in the appendix. These sources detail the structure of the various Palm, Pocket PC, PDA architectures, as well as provide information about analysis tools used on these devices.

X. Apple iPhone

This is a quadband (850, 900, 1800, 1900 MHz) device that currently only comes in a GSM version. There are several ways to find the IMEI number on an iPhone.

1) Back of the phone.
2) In the iPhone ”About” Screen.
3) On the iPhone Packaging.
4) Using iTunes 7.3 or later - iPhone Summary tab.

For more detailed instructions on locating the IMEI please refer to the Apple web site.

The internal memory consists of a flash hard drive that currently comes in either a 8GB or 16GB size. The current specifications do not indicate that it has the ability to add an SD card. This device contains an internal rechargeable battery that requires either a dock or dock cradle with USB connection (both come with the iPhone). These two hardware accessories are the only methods by which an iPhone can be charged.

The iPhone handset can be locked with a user generated 4 digit passcode. By default the passcode is not enabled on an iPhone device. A wrong passcode results in a red disabled screen that will display the message ”Wrong Passcode, try again”. If the wrong passcode is entered too many times, the screen will display the message ”iPhone is disabled, try again in 1 minute”. Subsequent repeated entries of the wrong passcode will result in the device being disabled for longer time intervals. Too many unsuccessful attempts will result in the iPhone being disabled, with no further attempts allowed, until the iPhone is connected to the computer/laptop that it normally syncs with [3] [4].

The OS is an optimised version of OS X (which is based on BSD). Updates to the iPhone OS are provided through iTunes (7.5 or greater), in a manner very similar for iPods. iTunes can also be set to sync any or of the following between the iPhone and a computer:

- Contacts
- Calendars
- Email Account Settings
- Webpage bookmarks
- Ringtones
- Music and audio books
- Photos
- Podcasts
- Videos

On the Apple iPhone, Mac OS X has three primary domains:

1) System - contains software Apple installs.
2) Local - machine specific applications and includes everything in /Library and /Applications.
3) User - contains user files; found under the /usr directory.

In one approach to analyze an iPhone, Reiber (2007), decribes key databases and storage locations for user information which are shown below (please refer to the appendix for more for reference to his article):

SMS. /var/root/Library/SMS/sms.db

Calendar. /var/root/Library/Calendar/Calendar.sqlitedb

Notes. /var/root/Library/Notes/notes.db

Call History. /var/root/Library/CallHistory/call_history.db

Address Book. /var/root/Library/AddressBook/ AddressBook.sqlitedb and /var/root/Library/AddressBook/ AddressBookImages.sqlitedb

Keychain. /var/root/Library/Keychains/keychain-#.db. *This is the area where the passwords are located (user information) and is encrypted.*

Voicemail. /var/root/Library/Voicemail/voicemail.db. *Individual voicemails are stored as 1.amr, 2.amr, etc.* custom greeting, it's stored as Greeting.amr.

Photos -*Photos taken*: /var/root/Media/DCIM/100Apple. *Photos synced from iPhoto* : /private/var/root/Media/Photos.

Safari You'll find Safari bookmarks and history files in /var/root/Library/Bookmarks.plist and History.plist.

Cookies are stored in /var/root/Library/Cookies/Cookies.plist.

Email The files are stored in: /var/root/Library/Mail attachments are mime encoded stored in: /var/root/Library/Mail/(account name)/INBOX.mbox/Messages) ”Envelope Index”

In addition, there are several other choices that an examiner could explore:

1) Mount the iPhone file system in a Linux environment [50].
2) . Disk for iPhone [44] - uses a MacFUSE based file system to read and write to the iPhone over USB connection. Must also have MacFUSE installed [52].
3) Use AFP (Apple Filing Protocol) to access iPhone file system from Finder in OS X. This is a hack in which you have to install the AFP Service on to the iPhone. Access to the file system is then gained by using Finder and connecting to a server using the following: **afp://your.iPhone.ip.** You will be prompted for username and password. For firmware versions 1.1.1 and 1.1.2, user name is root, and password is alpine. Firmware older than 1.1.1, username root and password is dottie [5].
4) Check the firmware on the iPhone [34].

The iPhone file system will be affected using any of the approaches in 1-3 above. It is strongly recommended that an examiner test out the methods and determine what is being changed before attempting it on an evidentiary iPhone.

XI. Analysis Tools

Due to the wide variety of mobile devices, currently no one tool can analyze them all. An examiner should determine what type of devices they have to analyse and strive to have multiple tools that will address their needs, given budgetary factors.

Regardless of toolkit, an examiner will need full access to the device. Should the device be protected by authentication, the toolkit will not extract the data, unless the authentication mechanism can be satisfied. Toolkits may or may not come with a host of cables to support various models of devices. They also have supported connection methods (cable, IR, BT).

Device extraction toolkits can be divided into three areas:

1) Integrated - data extraction form handset memory and SIM.
2) Handset Only
3) SIM Only

Most toolkits currently fall into the category of integrated. And they only do a logical acquisition of the device. Refer to the appendix for alphabetically listed tools that are currently available.

There are toolkits in development that are now going to target a physical dump of the device's internal memory in an attempt to recover all data including deleted data. Based on research this will require a flasher box, which will connect to the device through a cable interface, and create a memory dump. This dump file is then interpreted by a software application that will understand the device's file system and encoding. These are also listed in Table 3.

Finally as a last result, when all digitally connected acquisitions fail, there is the use of screen capturing tools. These devices are built specifically to photograph the device or the screen on the device for preservation purposes. These tools can also be found in Table 4.

Manufacturer Specific Tools:

Cell phone manufacturers do release their own software, which may be device specific or support a number of devices under one make. It is important to note that these tools also have the ability to change the firmware of the device and affect the device file system. A list of these tools may also be found in Table 5.

XII. Summary

This area of digital forensics will grow in scope and size due to the prevalence and proliferation of mobile devices. As the use of these devices grows, more evidence and information important to investigations will be found on them. To ignore examining these devices would be negligent and result in incomplete investigations.

Toolkit manufacturers will have a difficult time trying to interface with every device. It is advantageous to have a selection of tools at an examiner's disposal with the intent to cover as many devices as possible. The evolution of this area will lead to true physical memory acquisitions, compared to current logical data extractions.

Radio isolation of devices will become more important as handheld devices (not just BlackBerry's and Windows Mobile handsets) can be sent a remote kill command to wipe the device from an Internet connected computer/laptop. Another benefit of radio isolation is preservation of evidence on the device.

Examiners need to take prudent steps to document their extraction techniques and cross validate results across multiple toolkits. These actions will allow the examiner to understand what data types can be extracted by the toolkit as well as to validate and confirm the accuracy of the data extraction.

However, keep in mind that analysis of small scale digital devices is unlike traditional static computer based forensics. In this case a write protect intermediary (read only of the digital media) is used to prevent the data (evidence) from being altered during the forensic (bit stream) imaging phase during which the hash value of the forensic image matches that of the original digital media, which is typically a hard drive, memory card, or disc. Hash values in this instance are critical to validate the integrity of the forensic image to the original digital media.

In contrast, the analysis of small scale digital devices is a live state analysis because the device is in an ”on-state” during data acquisition and has *no write protect intermediary*. Therefore, the device memory is in a ”volatile” state and susceptible to network and/or user manipulation. Despite radio/network isolation; two acquisitions of the same device will very likely result in different hash values. The use of hash values, produced by the toolkits, in this instance, appears to be an adopted practice from computer-based forensics. A standard must evolve whereby the forensics community at large must determine whether the use of hash values, with regards to small scale digital devices are useful, or not acceptable. As such the acceptance of hash values may become an ingrained practice decided upon by the legal system rather than by the community. At the present time there are no known methods to write protect data acquisitions from these devices in order to produce a forensic bit stream image that will lead to matching hash values.

APPENDIX A
APPENDIX

TABLE I
MOBILE DEVICE ANALYSIS TOOLS

Aceso (Radio Tactics, Ltd.)	http://radio-tactics.com/
Athena (Radio Tactics, Ltd.)	http://radio-tactics.com/
BitPIM	http://www.bitpim.org/
CellDEK (Logicube)	http://www.logicubeforensics.com/products/hd_duplication/celldek.asp
CellDEK TEK (Logicube)	http://www.logicubeforensics.com/products/hd_duplication/celldek-tek.asp
Device Seizure (Paraben)	http://www.paraben-forensics.com/handheld_forensics.html
MOBILedit! Forensic	http://www.mobiledit.com/forensic/
Neutrino (Guidance Software)	http://www.guidancesoftware.com/products/neutrino.aspx
Oxygen Forensic Suite	http://www.oxygensoftware.com/en/products/forensic/
PhoneBase2 (Envisage)	http://www.envisagesystems.co.uk/html/phonebase.html
Secure View for Forensics (Susteen)	http://www.mobileforensics.com
TULP2G (NFI)	http://tulp2g.sourceforge.net
UFED (Cellebrite)	http://www.cellebrite.com/cellebrite-for-forensics-law-enforcement.html
.XRY (MicroSystemation)	http://www.msab.com/en/

TABLE II
SIM ANALYSIS TOOLS

ForensicSIM	http://www.radio-tactics.com/forensic_sim.htm
SIMCon	http://www.simcon.no
SIMIS	http://www.3gforensics.co.uk/simis.htm
SIMSeizure	http://www.paraben-forensics.com/handheld_forensics.html
USIMdetective	http://www.quantaq.com/usimdetective.htm

TABLE III
HEX DUMP ANALYSIS TOOLS

Cell Phone Analyzer (BK Forensics)	http://cpa.datalifter.com
Hex (Forensic Telecommunication Services, LTD)	http://www.forensicts.co.uk
HeXRY (MicroSystemation)	http://www.msab.com
Pandora's Box	http://www.hex-dump.com/vb/portal.php

TABLE IV
SCREEN CAPTURE TOOLS

Fernico ZRT	http://www.fernico.com/zrt.html
Project-a-Phone	http://www.projectaphone.com

TABLE V
MANUFACTURER SPECIFIC TOOLS

LG Sync Software	http://us.lge.com/support/download/search.jhtml
Nokia PC Suite	http://www.nokiahowto.com/A4410031
Samsung PC Studio and PC Link	http://www.samsung.com/download/index.aspx?agreement=y
Sony Ericsson PC Suite	http://www.sonyericsson.com/cws/support/products/software/w810i/pcsuite21046exe?cc=us&lc=en

TABLE VI
EXAMINER RESOURCES

Control-F	http://www.controlf.net/search/
Electronic Serial Number (ESN)	Converter http://www.elfqrin.com/esndhconv.html
GSM Arena	http://www.gsmarena.com
Hex Dump Forum	http://www.hex-dump.com/vb/portal.php
Mobile Forensics Central	http://www.mobileforensicscentral.com/mfc/
Mobile Forensics Incorporated	http://www.mfi-training.com/forum/
Mobile Forensics World	http://www.mobileforensicsworld.com/
Mobile Device Forensics	http://mobileforensics.wordpress.com/
Mobile Phone Forensics	http://www.mobilephoneforensics.com/mobile-phone-forensics-forums/
Multimedia Forensics Forum	http://multimediaforensics.com
The National Mobile Phone Crime Unit, London, UK	http://www.met.police.uk/mobilephone/
Phone Forensics Forum	http://www.phone-forensics.com
PhoneScoop	http://www.phonescoop.com
Process Text Group (Process various file formats)	http://www.processtext.com/
SSDD Forensics	http://www.ssddforensics.com/
SWGDE	http://68.156.151.124/documents/swgde2007/SpecialConsiderationsWhenDealingwithCellularTelephones-040507.pdf
Trew Mobile Telephone Evidence	http://trewmte.blogspot.com/
Yahoo Group	phoneforensics@yahoogroups.com

ACKNOWLEDGMENT

The authors would like to thank the following individuals for their valuable reviews of and comments for this paper: Members of the Calgary Police Service, Technological Crimes Team: Ossi Haataja, Jeremy Wittman, Dale Heinzig, and Rick Engel; Michael Harrington (Michigan State Police Computer Crimes Unit and Mobile-Examiner.com) and Lee Reiber (Mobile Forensics, Inc.). Finally, Shafik Punja would like to acknowledge Kevin Ripa, (Computer Evidence Recovery) friend, professional colleague and mentor who encouraged the creation of this document.

REFERENCES

[1] H. Kopka and P. W. Daly, *A Guide to LaTeX*, 3rd ed. Harlow, England: Addison-Wesley, 1999.

[2] 3GP. (n.d.). In Wikipedia, The free encyclopedia. Retrieved on December 23, 2007, from http://en.wikipedia.org/wiki/3GP

[3] Apple (n.d.). iPhone User Guide, Retrieved February 28, 2008, from http://www.apple.com/iphone/.

[4] Apple (n.d.). iPhone and iPod touch: Wrong passcode results in red disabled screen, Retrieved June 5, 2008, from http://support.apple.com/kb/HT1212/.

[5] AFP iPhone From Finder. (n.d.) In ModMyiFone Wiki. Retrieved December 17, 2007 from http://www.modmyifone.com/wiki/index.php/AFP_iPhone_from_Finder.

[6] Association of Chief Police Officers/National Hi-Tech Crime Unit. (n.d.)The Principles of Computer Based Electronic Evidence. Retrieved September 12, 2007 from http://www.acpo.police.uk/asp/policies/Data/gpg_computer_based_evidence_v3.pdf

[7] Ayers, R. (2006). An Overview of Cell Phone Forensic Tools. Retrieved on Sept. 10, 2007 from http://www.techsec.com/TF-2006-PDF/TF-2006-RickAyers-MobileForensics-TechnoForensics.pdf

[8] Ayers, R., Jansen, W. (2006). Forensic Software Tools for Cell Phone Subscriber Identity Modules. Association of Digital Forensics, Security and Law, April 20-21, 2006, Las Vegas, NV.

[9] Ayers, R. Jansen, W. (August, 2004) PDA Forensic Tools: An Overview and Analysis. Retrieved on Sept. 12, 2007 from http://csrc.nist.gov/publications/nistir/nistir-7100-PDAForensics.pdf

[10] Ayers, R., Jansen, W. (November, 2004). Guidelines on PDA Forensics. Retrieved on Sept. 12, 2007 from http://csrc.nist.gov/publications/nistpubs/800-72/sp800-72.pdf

[11] Ayers, R., Jansen, W., Cilleros, N., Daniellou, R. (2006). Cell Phone Forensic Tools: An Overview and Analysis. Retrieved on Sept. 12, 2007 from http://csrc.nist.gov/publications/nistir/nistir-7250.pdf

[12] Ayers, R., Jansen, R., Moenner, L., Delaitre, A. (2007). Cell Phone Forensic Tools: An Overview and Analysis Update. Retrieved on Sept. 10, 2007 from http://csrc.nist.gov/publications/nistir/nistir-7387.pdf

[13] Ayers, R., Jansen, W. (May, 2007). Guideline on Cell Phone Forensics. Retrieved September 12, 2007 from http://csrc.nist.gov/publications/nistpubs/800-101/SP800-101.pdf

[14] Ayers, R., Jansen, W. (2006). Forensic Software Tools for Cell Phone Subscriber Identity Modules. Association of Digital Forensics, Security and Law. April 20-21, 2006. Las Vegas, NV.

[15] Brown, M. (January, 2007). BlackBerry Forensics. Power Point Presentation to Department of Defence Cyber Crime Conference.

[16] CDMA (n.d.). CDMA Development Group Retrieved on January 29, 2008 from www.cdg.org.

[17] CTIA. (June, 2007). Wireless Quick Facts Mid-Year Figures. Retrieved on Sept. 10, 2007 from http://ctia.org/media/industry_info/index.cfm/AID/10323

[18] Electronic Serial Number. (n.d.). In Wikipedia, The free encyclopedia. Retrieved on December 15, 2007, from http://en.wikipedia.org/wiki/Electronic_Serial_Number

[19] ETSI (1995). Digital cellular telecommunications system (Phase 2+); Specification of the Subscriber Identity Module - Mobile Equipment (SIM - ME) interface (GSM 11.11). Retrieved Sept. 10, 2007 from http://www.ttfn.net/techno/smartcards/gsm11-11.pdf

[20] Federal Communications Commission (1934). Communications Act of 1934. Retrieved January 12, 2008, from http://wireless.fcc.gov/services/index.htm?job=operations_2&id=cellular

[21] Federal Communications Commission (2008). Cellular Services. Retrieved January 12, 2008 from http://wireless.fcc.gov/services/index.htm?job=service_home&id=cellular

[22] Flash Memory. (n.d.) In Wikipedia, The free encyclopedia. Retrieved on December 16, 2007, from http://en.wikipedia.org/wiki/Flash_memory.

[23] Grand, J. (2002). Forensic Analysis of Palm Devices. Forum of Incident Response and Security Teams in the Proceedings of the 14th Annual Computer Security Incident Handling Conference, Waikoloa, Hawaii, June 24-28, 2002. Retrieved January 3, 2007 from http://grandideastudio.com/wp-admin/uploads/pdd_paper.pdf

[24] GSM (n.d.). GSM Association, Retrieved on January 29, 2008 from , http://www.gsmworld.com/.

[25] Gratzner, V., Naccache, D., Znaty, D.(2006). Law Enforcement, Forensics and Mobile Communications. Retrieved on Sept. 10, 2007 from http://www.cl.cam.ac.uk/ fms27/persec-2006/goodies/2006-Naccache-forensic.pdf

[26] Harrington, M. (2007). How-to BlackBerry Exams. Retrieved on December 15, 2007 from http://www.Mobile-Examiner.com

[27] Harrington, M. (2007). IPD Files Demystified. Retrieved on December 15, 2007 from http://www.Mobile-Examiner.com

[28] History of Mobile Phones. (n.d.). In Wikipedia, The free encyclopedia. Retrieved on December 15, 2007, from http://en.wikipedia.org/wiki/History_of_mobile_phones.

[29] Hylton, H. (2007). What Your Cell Phone Knows About You. Time. Retrieved on September 1, 2007 from http://www.time.com/time/health/article/0,8599,1653267,00.html

[30] IMEI. (n.d.). In International Numbering Plans. Retrieved on December 15, 2007 from http://www.numberingplans.com/?page=analysis&sub=imeinr.

[31] iPhone. (n.d.). In Wikipedia, The free encyclopedia. Retrieved on January 8, 2008 from http://en.wikipedia.org/wiki/IPhone.

[32] International Organization on Computer Evidence (2000). Good Practices for Seizing Electronic Devices - Mobile Telephones. Retrieved September 12, 2007 from http://www.ioce.org/fileadmin/user_upload/2000/ioce%202000%20electronic%20devices%20good%20practices.doc

[33] Interpol Mobile Phone Forensic Tools Sub-Group. (2006). Good Practice Guide for Mobile Phone Seizure & Examination. Retrieved September 12, 2007 from http://www.holmes.nl/MPF/Principles.doc

[34] Janke., M. (n.d.) Hack That Phone. Retrieved December 17, 2007 from http://www.hackthatphone.com/

[35] Jansen, W., Ayers,R. (2007). Guidelines on Cell Phone Forensics. Retrieved Sept. 10, 2007 from http://csrc.nist.gov/publications/nistpubs/800-101/SP800-101.pdf

[36] Kim, K., Hong, D., Chung, K., Ryou, J. (2007). Data Acquisition from Cell Phone using Logical Approach. Proceedings of World Academy of Science, Engineering and Technology. Vol. 26. December 2007.

[37] McCarthy, P. (2005). Forensic Analysis of Mobile Phones. Retrieved Sept. 10, 2007 from http://esm.cis.unisa.edu.au/new_esml/resources/publications/forensic%20analysis%20of%20mobile%20phones.pdf

[38] McCullough, J. (2004). 185 Wireless Secrets, Wiley Press. p. 192.

[39] Micro SD. (n.d.). In Wikipedia, The free encyclopedia. Retrieved on December 21, 2007 from http://en.wikipedia.org/wiki/MicroSD.

[40] Mobile Phone. (n.d.). In Wikipedia, The free encyclopedia. Retrieved on December 15, 2007, from http://en.wikipedia.org/wiki/Mobile_phone.

[41] Napieralski, B. (2006) How to Easily Process a BlackBerry Device. Retrieved on December 15, 2007 from http://www.mfi-training.com/forum.

[42] Paraben Corporation. (August, 2005), Cell Seizure & Analysis, Power Point Presentation, 2005 High Technology Crime Investigation Conference.

[43] Paraben Corporation. (n.d.). Paraben's Wireless StrongHold Bag. Retrieved on September 20, 2007 from http://www.paraben-forensics.com/catalog/product_info.php?products_id=173&osCsid=45231cbd175b01532932e348deac741f

[44] Porter, A. (2007) Disk for iPhone. Retrieved on December 15, 2007, from http://code.google.com/p/iphonedisk/.

[45] Prism Holdings Limited. (n.d.). In Prism 3G uSIMetrix Overview. Retrieved on December 15, 2007, from http://www.prism.co.za.

[46] Ramsey Electronics. (n.d.). STE3000B - RF Shielded Test Enclosure. Retrieved on September 20, 2007 from http://www.ramseyelectronics.com/cgi-bin/commerce.exe?preadd=action&key=STE3000B

[47] Ray, B. (2007). One plug to rule them all. The Register. Retrieved on September 21, 2007 from http://www.theregister.co.uk/2007/09/21/omtp_data_standard/

[48] Reiber, L (2007). iPhone Data Extraction, Mobile Forensics Inc. Retrieved 2007, from http://www.mfi-training.com/forum/

[49] Research In Motion (2006). BlackBerry Enterprise Solution Security Version 4.0.x Technical Overview, Retrieved February 23, 2008 from http://na.blackberry.com/eng/support/

[50] Richardson, W. (2007). How To Mount Your iPhone Filesystem On Your Desktop In Ubuntu. Retrieved on December 15, 2007, from http://www.fsckin.com/2007/09/23/how-to-mount-your-iphone-filesystem-on-your-desktop-in-ubuntu/.

[51] Robinson, G., Smith, G. (2001). Evidence from mobile phones. The Legal Executive. Journal of the Institute of Legal Executives. Retrieved on September 12, 2007 from http://www.ilexjournal.com/special_features/article.asp?theid=284&the mode=2

[52] Singh. (2007). MacFuse. Retrieved December 17, 2007 from http://code.google.com/p/macfuse/.

[53] Scientific Working Group on Digital Evidence. (2007). Special Considerations When Dealing With Cellular Telephones. Retrieved September 12, 2007 from http://68.156.151.124/documents/swgde2007/SpecialConsiderationsWhen DealingwithCellularTelephones-040507.pdf

[54] Traud, A. (n.d.). 3GPP TS 27.005 / 27.007. Retrieved September 10, 2007 from http://www.traud.de/gsm/index.html

[55] Wee, C., Wong, L. (2005) Forensic Image Analysis of Familiar-based iPAQ. School of Computer and Information Science, Edith Cowan University.Retrieved May 12, 2007, from http://www.forensicfocus.com/downloads/familiar-ipaq-forensic-analysis.pdf

[56] Virki, T. (2007). Global cell phone use at 50 percent. Reuters. Retrieved January 7, 2007 from http://www.reuters.com/article/technologyNews/idUSL2917209520071129

[57] Web2Pin. (n.d.). Blackberry PIN Messaging Solutions. Retrieved December 15, 2007, from http://www.web2pin.com/Web2PinFree.aspx.

[58] Willassen, S. (2003). Forensics and the GSM mobile telephone system. International Journal of Digital Evidence. Vol. 2, No. 1.

[59] Willassen, S. (2005). Evidence in Mobile Phone Systems. Retrieved February 19, 2005, from http://www.mobileforensics.com.

[60] Wireless Quick Facts. (n.d.). In CTIA Quick Facts. Retrieved December 15, 2007, from http://www.ctia.org/media/index.cfm/AID/10323.

Shafik G. Punja Shafik G. Punja is a Constable with the Calgary Police Service's, Electronic Surveillance Unit - Technological Crimes Team, Calgary, Canada. He has worked in the area of digital forensics since November 2003. In March of 2004 he began to develop an interest in analysis of handheld mobile devices. He can be reached at shafik@calgarytechcrime.ca or pol3066@calgarypolice.ca.

Richard P. Mislan Richard P. Mislan is an Assistant Professor at the Cyber Forensics Lab, in the Computer and Information Technology department of the College of Technology at Purdue University, in West Lafayette, Indiana, USA. Additionally, Richard serves as Editor of the Small Scale Digital Device Forensics Journal (http://ssddfj.org) and Director of the Mobile Forensics World Conference (http://www.MobileForensicsWorld.com). Richard can be reached at rmislan@purdue.edu.