CERIAS Tech Report 2001-149
Mobile Device Forensics Case File Integrity Verification
by Sean Sobieraj
Center for Education and Research
Information Assurance and Security
Purdue University, West Lafayette, IN 47907-2086

MOBILE DEVICE FORENSICS
CASE FILE INTEGRITY VERIFICATION

A Thesis

Submitted to the Faculty

of

Purdue University

by

Sean C. Sobieraj

In Partial Fulfillment of the

Requirements for the Degree

of

Master of Science

May 2008

Purdue University

West Lafayette, Indiana

TABLE OF CONTENTS

Page

LIST OF TABLES

LIST OF FIGURES

NOMENCLATURE

Acquisition (Process) – Obtaining data and information from a mobile device.

Acquisition (Object) – See Case File.

AT Commands – Communication commands originally developed for communicating with AT (Hayes) compatible modems.

Case File – The collective output of multiple files produced from a single acquisition.

Checksum – See Hash

Collision – When the same hash is produced from distinct data objects.

Data Object – A unique type of acquirable information, such as the phonebook, SMS history, calendar, an image, etc.

FBUS – Communication protocol proprietary to Nokia mobile phones.

Hash – The fixed-size value, or “digital fingerprint” produced by a cryptographic hash function of a specific piece of data.

MD5 – Message-Digest algorithm 5. A cryptographic hash function that produces a 128-bit hash value from a given set of data.

OBEX – Object Exchange. Communications protocol primarily designed for transferring binary objects between devices.

Phone – Mobile phone or device.

SHA1 – Secure Hash Algorithm 1. A cryptographic hash function that produces a 160-bit hash value from a given set of data.

ABSTRACT

Sobieraj, Sean C. M.S., Purdue University, May, 2008. Mobile Device Forensics Case File Integrity Verification. Major Professor: Richard Mislan.

The accuracy of mobile forensic case files is coming under increased scrutiny as a greater emphasis is being put on the ability to maintain the integrity of acquired data. Mobile phones are in use throughout the world in record numbers, and their functionality and convenience may rival that of a desktop computer for many ordinary tasks. Certain attributes of mobile phones have always made them typically difficult to forensically examine, but their prevalence will undoubtedly link them to greater numbers of crimes where they may play a critical role. Forensic tools must provide greater functionality and maintain reliability while overcoming the limitations in this field.

This thesis provides an overview of the forensic significance and legal implications of mobile phones, and provides a review of two dominant mobile forensic tools and their ability to maintain the forensic integrity of the acquired data.

CHAPTER 1. OVERVIEW

1.1. Objectives

The overall goal of this research was to examine the hashing mechanisms implemented in Susteen DataPilot Secure View 1.5 and Paraben Device Seizure 1.3, and determine if they create and preserve a forensically sound case file. This was to be accomplished by…

- Determining how the hashing mechanisms have been implemented in each tool and what their intended purposes are.

- Comparing hash values across multiple acquisitions of various phones from both tools to determine the consistency and repeatability of their results.

- Testing each tool's ability to identify a manipulated or corrupt case file.

1.2. Organization

This thesis covers various aspects of mobile phone forensics pertaining to challenges in maintaining evidence integrity. They are covered in the following six chapters:

- Chapter 2 provides an introduction to the forensic significance of mobile phones.
- Chapter 3 discusses the legal implications of digital forensic evidence as it relates to mobile devices.
- Chapter 4 provides an overview of the forensic tools, mobile phones, and verification tests used in this research.
- Chapter 5 explains the test results from evaluating Susteen DataPilot Secure View.
- Chapter 6 explains the test results from evaluating Paraben Device Seizure.
- Chapter 7 is the conclusion.

CHAPTER 2. FORENSIC SIGNIFICANCE OF MOBILE PHONES

2.1. Introduction

According to The Mobile World, a UK-based telecom analysis company, (HTTP://WWW.THEMOBILEWORLD.COM), the number of mobile phone subscriptions surpassed 3.25 billion worldwide at the end of last year (Ridley, 2007). A survey by CTIA-The Wireless Association has shown that in the United States the number of mobile phone subscriptions exceeded 243 million in the middle of 2007 (CTIA-The Wireless Association, 2007). Based on the current values of the U.S. Census Bureau Population Clocks at 17:53 GMT on February 19, 2008 (HTTP://WWW.CENSUS.GOV/MAIN/WWW/POPCLOCK.HTML), worldwide mobile phone subscriptions have surpassed 50% of the global population, and subscriptions in the United States exceed 82% of the U.S. population. Figure 2.1 shows the growth of the mobile phone market in the U.S.

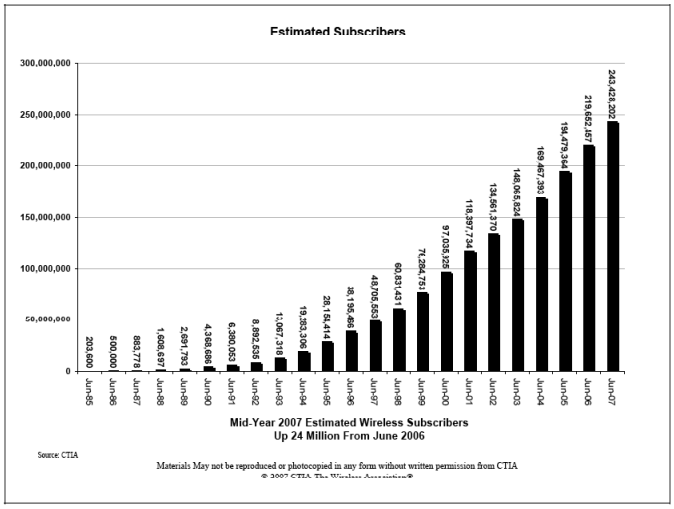

Figure 2.1 Estimated Subscribers in the U.S. (CTIA, 2007, p. 5).

Although an 82% penetration rate sounds significant, the U.S. has actually been a laggard in its adoption of the mobile phone. There are many countries whose mobile phone penetration rate exceeds 100%, with some in excess of 110%, such as Sweden, the United Kingdom, and Italy (M2 Communications, 2006). Percentages have continued to grow past 100 because they reflect the number of subscriptions, and do not take into account people who have more than one, however this does not take away from the overwhelming number of people using mobile phones. Since the mobile phone market is becoming increasingly saturated it may begin to slow, but the numbers will no doubt continue to increase, especially as newer markets continue to grow around the world.

The success of the mobile phone can be attributed to the fact that it helps satisfy the human need for instant gratification. Waiting is inconvenient, which is why the majority of technology in the consumer market is marketed around providing more, better, and faster functionality. As the mobile phone's customer base continues to broaden, so do its capabilities, putting an ever-greater number of resources at a user's fingertips. By today's standards mobile phones are much less phones than they are mobile computers.

For ordinary tasks, modern mobile phones provide much of the same functionality that is provided by a desktop computer. This makes them a potentially valuable source of evidence in a forensic investigation. Larger on-board memory capacity in addition to expandable memory slots, word processors and other third-party applications, and fully functional Internet browsers are just a few additional capabilities of modern mobile phones. These three additional functions alone will drastically increase the abundance and value of information contained in these devices.

2.2. Potential Evidence

Due to the high penetration rate of mobile phones, they will inevitably be connected to and increasing number of criminal activities. Since they may contain information comparable to that of a desktop computer, they are a prime source of evidence. The following list of potential evidence can be found in a mobile phone:

- Subscriber and equipment identifiers
- Date/time, language, and other settings
- Phonebook information
- Appointment calendar information
- Text messages
- Dialed, incoming, and missed call logs
- Electronic mail
- Photos
- Audio and video recordings
- Multi-media messages
- Instant messaging and Web browsing activities
- Electronic documents
- Location information (Jansen & Ayers, 2007, p. 57)

Due to new features on mobile phones such as increased memory storage and third-party applications, both the quantity and complexity of the above evidence will increase, as phones will be able to store larger files and more of them.

Many issues pose a threat to the validity of mobile phone forensics. There are difficulties in acquiring certain types of data that stem from the proprietary nature of mobile phones. In addition, features such as Bluetooth and the ability to run third-party applications can create additional problems. As a result, mobile forensic tools are struggling to reliably acquire data from a wide range of mobile phones. As the amount of evidence and different types of mobile phones

increases, the tools must also advance in functionality to accommodate these changes without sacrifice.

2.3. Issues

Papers exist that bring attention to the various issues surrounding integrity management in mobile phone forensics, however few, if any, are able to provide solutions. Research tends to lead to additional avenues that must be explored, or additional assumptions that need to be verified. This speaks for the difficulty of mobile phone forensics.

Up until recently, the majority of mobile forensic tools did not implement any form of integrity protection. Forensic examiners were relied upon to ensure evidence was not tampered with or corrupted. For example, Oxygen's Mobile Phone Manager is a phone-syncing tool that was used for at least two years by law enforcement to gather evidence from mobile phones before being updated. An updated tamper-resistant "forensic" version was released in April 2007 that uses hash values to help maintain the integrity of acquired data. Before this version was available, it was unclear how integrity management was addressed. Oleg Fedorov, a spokesman for Oxygen Forensic, said, "I can't say precisely how [law enforcement] protected data from tampering. I can only suggest they didn't change any information and didn't press the 'Write' button" (Newitz, 2007, p. 2). Many would consider this unacceptable, especially when it comes to the admissibility of such evidence in court. Since there are currently no certifications or required training classes to become a mobile phone examiner, anyone can attempt to use various forensic tools to gather data.

Paraben Device Seizure is known to maintain acquired data in "tamper-proof evidence files" (Newitz, 2007, p. 2), and it is stated on Paraben's website that Device Seizure verifies file integrity with the use of MD5 and SHA1 hash values (Paraben Corporation, 2007b). Susteen DataPilot Secure View has also

implemented integrity protection in its most recent version, and also claims on their website that it uses MD5 hashes to verify and validate the integrity of acquired data and verifies whether data has been tampered with post-extraction (Susteen Inc., 2008). The integrity protection mechanisms implemented by each tool will be subject to further review in the verification tests explained in chapters 5 and 6.

Mobile forensic tools are beginning to address the issue of integrity management, however proprietary operating systems on mobile phones is still an issue that has implications in data integrity. Proprietary operating systems make retrieving information from phone memory difficult. Some of the current mobile forensic tools claim that they acquire evidence from mobile phones in a forensically sound manor, and maintain its integrity upon further examination. Paraben's product information for Device Seizure states, "Device Seizure does not allow data to be changed on the device" (Paraben Corporation, 2007a, p. 1). These claims may be premature because in most cases forensic tools are limited to the proprietary communication methods of each phone for data acquisition. The forensic software must communicate with the phone operating system over an open connection to access the data. As a result, a write-blocker, which is commonly used in computer forensics to eliminate fear that data on a device is not inadvertently modified during the acquisition process, cannot be used in mobile forensics. Since the mobile phone memory and operating system remain active when acquiring data, it is impossible to avoid modifications to phone memory, especially over several acquisitions. In the Frequently Asked Questions for Device Seizure on Paraben's website a question asks if information on the device changes when data is acquired. In response to this question, Paraben states that because PDAs store all data in memory it is impossible to not have a slight change occur in the acquisition process, but that the changes that occur are so minor that they do not affect the integrity of the user's data (Paraben Corporation, 2007b). This is mostly true as only system files typically change,

while static user data such as images should remain unchanged. However, some of the changes may be significant, such as altering the status of an SMS message from unread to read during an acquisition.

Mobile forensic tools typically use AT commands, FBUS, OBEX or other similar communication protocols to acquire data. The method depends on the phone. All of these methods rely on proprietary phone software, and carry with them the following issues:

- Data can be indirectly altered when using AT commands or Nokia FBUS.
- Important data may be omitted from the phone's response to a command.
- Some data will never be accessible over software interface.
- Data that is accessible on one phone may not be accessible on other, similar phones, using the same commands. (McCarthy, 2005, p. 53)

This creates a problematic situation with mobile forensic tools because the methods relied on to investigate phones may be inherently unreliable. At the same time, forensic investigations cannot wait for an unlikely standardized mobile phone protocol. Therefore, it is critical to make sure that obtainable data remains forensically sound.

Proprietary operating systems require the use of potentially insecure acquisition methods because direct access to mobile phone memory is limited, which prevents it from being forensically duplicated like an ordinary hard drive from a desktop or laptop computer. Using the phone operating system to acquire data from the phone means the memory is constantly active and always changing. This may result in inconsistencies in the hashes of subsequent acquisitions of the same phone memory. Generally, mobile phones also require unique cables and drivers to establish a connection, further complicating the acquisition process.

One instance where certain acquisitions inconsistencies have been recorded is with hashes from Nokia mobile phones. Williamson, Apeldoorn, Cheam, and McDonald (2006) showed that hashes of mobile phone memory were the same for different Nokia handsets. Paraben Cell Seizure was used in their testing. They propose that the hashes were the same for the different phones because of the limited memory storage of the older Nokia 5110 series phones they were using. The memory of these phones appeared to contain only an identical logo, resulting in the same hash. They determined that unique phone information such as the IMEI number was not included in the data hashed by Cell Seizure. They concluded that newer phones with greater memory capacity should not exhibit similar results because they would contain more information, but that it cannot be definitively ruled out. It is also possible these hash anomalies resulted from a flaw in the software that prevents it from actually hashing the entire phone memory.

Multiple acquisitions of same phone memory have also been shown to produce different hashes. This may be due to an internal clock, constantly changing timestamps, or other unique information that is otherwise in flux.

These issues have been inherently accepted due to the nature of mobile phones, as there are no clear solutions for them. However, potential issues with the integrity of the majority of acquirable data are still believed to be limited. Hashes of the entire phone memory may be inconsistent, however these differences should not have an impact on the integrity of static files in the memory such as images, sounds, contact lists, etc. The National Institute of Standards and Technology (NIST) defined acquisition consistency as two consecutive acquisitions producing different overall hashes of the memory, while the hashes of individual database files remain consistent (Ayers, Jansen, Moenner, & Delaitre, 2007). Mobile forensics can still provide successful investigations depending on the data and how it was acquired. However, since hashes of

entire phone memory are expected to be inconsistent, they have no weight in verifying the original contents of a phone, or the same information across multiple acquisitions.

Not only are there no standards among mobile phones, but standards for performing an acquisition are also lacking. There are several generally accepted practices, and each has their own negative consequences. For example, upon confiscating a mobile device, deciding whether to turn it off, leave it on, enable airplane-mode if available, or place it in a faraday bag or container. Potential negative consequences of each of these options are documented in the NIST Guidelines on Cell Phone Forensics:

- Turning the phone off may require the input of authentication codes or passwords when the phone is turned on again
- Leaving the device in an active state may lead to the possibility of modifying the contents of the phone (i.e. incoming calls or text messages)
- Enabling airplane-mode requires interaction with the phone, which poses some risk.
- Leaving the device on and placing it in a faraday bag increases battery depletion as the phone attempts to find a signal. It also may cause the phone to reset or clear network data that would otherwise be useful if recovered. (Jansen & Ayers, 2007, p. 34)

2.4. The Future

The number of unique mobile phones is extensive. Phonescoop.com is a comprehensive database of 992 mobile phones, and covers information for thirty-seven phone manufacturers and fifteen carriers. Standards are not only different across manufacturers and carriers but they differ from phone to phone as well. This makes acquiring data very difficult since each phone must be individually addressed. As a result, forensic tool manufacturers maintain lists of compatible phones and supported features for their software.

Although mobile forensic tools provide solutions for multiple types of phones, familiarity with multiple toolkits is necessary for thorough coverage. As the evidentiary value of data contained in mobile phones becomes more apparent, tools must become increasingly reliable and continuously improved to ensure data integrity. Particularly, forensic tools must increase the granularity on how hashes are calculated for distinct data objects such as address books, text messages, call logs, etc. Each data type provides a unique fingerprint that is believed to remain consistent across multiple acquisitions. Data types that are independent from the phone software such as standard image and sound formats should remain consistent across various phones as well. Although phones will still require proprietary methods to acquire data, a more standardized way of organizing and maintaining acquired data is possible.

Also, just as the mobile phone market will continue to grow, so will the number of examiners using the various forensic tools. This will naturally lead to higher error rates in acquisitions. Simplifying the acquisition process and implementing additional integrity protection will prove valuable.

CHAPTER 3. LEGALITY OF DIGITAL EVIDENCE

The purpose of forensically sound evidence is admissibility in a court of law. This is only possible if the integrity of the evidence remains intact. The methods used to acquire and manage evidence are best if understood and accepted by the majority mobile forensic professionals. As explained earlier there are many unknowns and assumptions in mobile forensic practice. There is certainly no gold standard. It is likely there will never be a single best method to use in every situation, however all methods that will potentially result in legal evidence must be proven and accepted. This is precisely the problem addressed by Frye v. United States, the Federal Rules of Evidence, and Daubert v. Merrell Dow.

3.1. Frye v. United States (1923)

In Frye v. United States (1923), the court announced that a novel scientific technique "must be sufficiently established to have gained general acceptance in the particular field in which it belongs" (Frye v. United States, n.d., p. 2). Frye has come under some criticism because this statement is rather vague. It is not particularly clear when something becomes "sufficiently established," and the ruling offered no explanation for its adoption. Nonetheless, it set a standard for the acceptance of expert testimony in court.

3.2. Federal Rules of Evidence

The Federal Rules of Evidence were enacted on January 2, 1975, and have been amended several times since then by Acts of Congress and the U.S.

Supreme Court. They provide additional definitions and guidelines for the admissibility of evidence.

Article VII, Rule 702 Testimony by Experts, states:

> "If scientific, technical, or other specialized knowledge will assist the trier of fact to understand the evidence or to determine a fact in issue, a witness qualified as an expert by knowledge, skill, experience, training, or education, may testify thereto in the form of an opinion or otherwise, if (1) the testimony is based upon sufficient facts or data, (2) the testimony is the product of reliable principles and methods, and (3) the witness has applied the principles and methods reliably to the facts of the case" (Federal Rules of Evidence, 2004, p. 13).

This rule attempts to define who may testify as an expert, however its interpretation is still relatively subjective, which remains a problem. Similar to the statement "sufficiently established" in Frye v. United States, testimony is still based on the "sufficiency" of facts or data and the "reliability" of principles, methods and their application to the facts of the case. There are no given definitions or requirements as to what constitutes these statements.

The idea of relevancy that is implied by Rule 702 is further defined in Rule 401 Definition of "Relevant Evidence" as follows:

> "'Relevant evidence' means evidence having any tendency to make the existence of any fact that is of consequence to the determination of the action more probable or less probable than it would be without the evidence" (Federal Rules of Evidence, 2004, p. 3).

Since the sufficiency and reliability of evidence is not as well defined as its relevancy, some evidence may be deemed admissible when it should not be. Evidence that is not properly maintained or acquired by inadequate methods may still have an influence on the facts of a case – potentially more so if incorrect or purposely twisted for a desired effect.

The Federal Rules of Evidence also define the terms “original” and “duplicate” in Article X, Rule 1001 as the following:

- Original - An “original” of a writing or recording is the writing or recording itself or any counterpart intended to have the same effect by a person executing or issuing it. An “original” of a photograph includes the negative or any print therefrom. If data are stored in a computer or similar device, any printout or other output readable by sight, shown to reflect the data accurately, is an “original.”
- Duplicate - A “duplicate” is a counterpart produced by the same impression as the original, or from the same matrix, or by means of photography, including enlargements and miniatures, or by mechanical or electronic re-recording, or by chemical reproduction, or by other equivalent techniques which accurately reproduces the original. (Federal Rules of Evidence, 2004, p. 24)

Acquiring the true original of anything in mobile forensics is slim since direct access to mobile phone memory is limited in most cases. The content of static data objects typically remains unchanged, however file metadata such as timestamps may not be preserved. Mobile forensics requires certain specificity when determining what is admissible and what is not.

3.3. Daubert v. Merrell Dow (1993)

Daubert v. Merrell Dow (1993) overruled the Frye opinion because of its lack of clarity. Daubert is based on the interpretation of the Federal Rules of Evidence, specifically Rule 702, but it also introduced additional guidelines for determining the reliability of evidence. States can choose to follow either Frye or Daubert, in addition to unique state legislation. If following the Daubert ruling, Rule 702 of the Federal Rules of Evidence must be met. Figure 3.1 shows the application of the basic principles to determine the admissibility of evidence.

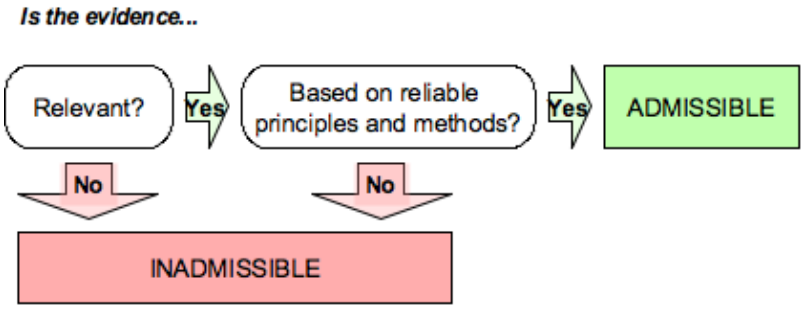

Figure 3.1 Basic Principles of Admissibility

The court also emphasized some additional general factors, however it is important to note that these are merely general observations, and not intended to be a checklist for admissibility:

- Has the scientific theory or technique been empirically tested?
- Has the scientific theory or technique been subjected to peer review and publication? This ensures that flaws in the methodology would have been detected and that the technique is finding its way into use via the literature.
- What is the known or potential error rate? Every scientific idea has Type I and Type II error rates, and these can be estimated with a fair amount of precision. There are known threats to validity and reliability in any tests (experimental and quasi-experimental) of a theory.
- What is the expert's qualifications and stature in the scientific community? And does the technique rely upon the special skills and equipment of one expert, or can it be replicated by other experts elsewhere?
- Can the technique and its results be explained with sufficient clarity and simplicity so that the court and the jury can understand its plain meaning? (O'Connor, 2006, p. 2)

Daubert provides more direction than Frye or the Federal Rules of Evidence when determining the admissibility of evidence. Unfortunately, mobile forensics

does not thoroughly meet these factors or even all of the requirements of Rule 702.

The two principles in Figure 3.1 are the only true requirements, and up until Daubert have been ill defined. The additional factors should be taken into consideration because they help define what is relevant and reliable, however evidence that meets the additional factors listed above does not guarantee its admissibility. Additional requirements or unique circumstances of a case may impose other factors that must be met. One factor that is typical to reliability, and alluded to in the factors above, is repeatability.

3.4. Repeatability

The International Union of Pure and Applied Chemistry (1997) defines repeatability as:

> "The closeness of agreement between independent results obtained with the same method on identical test material, under the same conditions (same operator, same apparatus, same laboratory and after short intervals of time). The measure of repeatability is the standard deviation qualified with the term: 'repeatability' as repeatability standard deviation. In some contexts repeatability may be defined as the value below which the absolute difference between two single test results obtained under the above conditions, may be expected to lie with a specified probability."

This definition matches closely with NIST's definition of "repeatability conditions":

- The same measurement procedure
- The same observer
- The same measuring instrument, used under the same conditions
- The same location
- Repetition over a short period of time. (Taylor & Kuyatt, 1994, p. 14)

Both definitions stress that repeatability stems from the same conditions. Without repeatability then it will not be possible to produce the same results. Repeatability is critical in any forensic science, as varying results in any given investigation would prove worthless.

Even if specific test results are consistently inconsistent, determining their cause and their relationship to other data can be helpful in reinforcing the idea that they have no effect on the integrity of the other data.

3.5. MD5 (Message-Digest Algorithm 5)

The integrity of evidence is based on the consistent value of its checksum. MD5 is a popular hash function and it is commonly used to check the integrity of files. The MD5 message-digest algorithm "takes an input message of arbitrary length and produces as output a 128-bit "fingerprint" or "message digest" of the input" (Rivest, 1992, p. 1). No two files produce the same hash, and when dealing with real world data it is computationally infeasible to force two files or messages to produce the same hash. Although MD5 collisions have been demonstrated by Wang, Feng, Lai, and Yu (2004) they are a result of very specific modifications to unintelligible messages. A hash collision occurs when two different input messages produce an identical MD5 hash, as shown in Table 3.1.

Table 3.1 MD5 Collision (Wang et al., 2004)

Message 1	1st Block	02DD31D1 C4EEE6C5 069A3D69 5CF9AF98 **87**B5CA2F AB7E4612 3E580440 897FFBB8 0634AD55 02B3F409 8388E483 5A41**71**25 E8255108 9FC9CDF7 **F2**BD1DD9 5B3C3780
	2nd Block	D11D0B96 9C7B41DC F497D8E4 D555655A **C7**9A7335 0CFDEBF0 66F12930 8FB109D1 797F2775 EB5CD530 BAADE822 5C15**CC**79 DDCB74ED 6DD3C55F **D8**0A9BB1 E3A7CC35
Message 2	1st Block	02DD31D1 C4EEE6C5 069A3D69 5CF9AF98 **07**B5CA2F AB7E4612 3E580440 897FFBB8 0634AD55 02B3F409 8388E483 5A41**F1**25 E8255108 9FC9CDF7 **72**BD1DD9 5B3C3780
	2nd Block	D11D0B96 9C7B41DC F497D8E4 D555655A **47**9A7335 0CFDEBF0 66F12930 8FB109D1 797F2775 EB5CD530 BAADE822 5C15**4C**79 DDCB74ED 6DD3C55F **58**0A9BB1 E3A7CC35
MD5 Hash		8D5E7019 6324C015 715D6B58 61804E08

The MD5 algorithm has 2^{128}, or $3.4x10^{38}$ possible values, making the probability of two files having the same hash extremely small. There are no documented cases of a cryptographer successfully generating a hash collision in a realistic scenario (AccessData, 2006). Whether building a file from scratch or modifying an existing file, it is computationally infeasible to produce an intelligible file and have it produce a predetermined hash value. This is important because although weaknesses have been proven in the MD5 hash algorithm, they do not currently pose a risk in its use for maintaining the integrity of forensic evidence. “No one is going to be breaking digital signatures or reading encrypted messages anytime soon with these techniques. The electronic world is no less secure after these announcements than it was before” (Schneier, 2004, 2).

MD5 hashes are sufficient for forensic application, so it is not necessary to questions the validity of the MD5 algorithm itself, however, its reliability and

efficiency is still hinged on its implementation. Regardless if its implementation is quality, it is still a tool and should not be depended on or used in lieu of proper forensic procedures.

In addition to being used for integrity management, MD5 hash values can also be used to identify known files and file types. Various file types and identical pieces of information in general have unique fingerprints. Known MD5 hash values can be organized into hash sets that can help examiners single out information of interest and ignore that which is not.

McCreight and Patzakis (2001) define two specific types of hash sets. Safe hash sets consist of hash values of files known to be innocuous. These can be used to filter files from an investigation that are harmless and otherwise get in the way. Hashes of original system files are typically included in a safe hash set. This can also contain a custom list of hashes from files determined to be of no consequence from previous investigations. Notable hash sets consist of hash values of known files that may be of interest to the examiner.

Hash sets will become increasingly valuable as the storage capacities of mobile devices grow. They will allow an examiner to focus attention on information that is more pertinent to their objective rather than sifting through data that has been previously determined to be insignificant.

CHAPTER 4. PHONES, TOOLS, AND TEST OVERVIEW

4.1. Phones

The following phones were used in this research.

- Blackberry 7280 (Cingular)
- Blackberry 7290 (Cingular)
- LG VX5200 (Verizon)
- LG VX6100 (Verizon)
- Nokia 5165 (Cingular)
- Nokia 6340i (Cingular)

4.2. Susteen DataPilot Secure View 1.5

Susteen provides a detailed phone compatibility list on their website. Each phone is individually addressed regarding Secure View's ability to Read & Write, Write only, Read only, or Support the following components of a mobile phone: Address Book, Calendar, Images, Movies, MIDI Sound, MP3 Sound, Internet Connect, SMS Manager. Secure View does not support Blackberry devices. The other phones used in this research are supported as shown in Table 4.1.

Table 4.1 Secure View Phone Support

Secure View Phone Support		
Legend:		RW = Read & Write
ADD BK = Address Book	CAL = Calendar	W = Write Only
IMG = Images	MOV = Movies	R = Read Only
MIDI = MIDI Sound	MP3= MP3 Sound	S = Supported
DC = Internet Connect	SMS = SMS Manager	- = Not Supported

Phone	Carrier	ADD BK	CAL	IMG	MOV	MIDI	MP3	DC	SMS
Blackberry 7280	Cingular	-	-	-	-	-	-	-	-
Blackberry 7290	Cingular	-	-	-	-	-	-	-	-
LG VX5200	Verizon	RW	RW	RW	-	RW	RW	S	-
LG VX6100	Verizon	RW	RW	RW	-	RW	RW	S	-
Nokia 5165	Cingular	RW	-	-	-	-	-	-	-
Nokia 6340i	Cingular	RW	RW	-	-	W	-	*	RW

*Nokia 6340i – DC supported on IrDA Model

If a supported data type did not show up in an acquisition then it did not exist on the phone, which is reflected in the report. The compatibility information provided by Susteen is correct.

Secure View 1.5 is a very streamlined mobile forensic tool, and does not provide much functionality outside of acquiring and storing data. It saves an acquisition to a folder named 'year-month-day hour-minute-second-phone model' (i.e. '2008-03-10 15-43-59-LG VX6100'). The contents of this folder are determined by the options selected by the examiner before performing the acquisition. Depending on what is supported by the phone, an examiner may choose to acquire the contacts, call history, calendar, SMS, images & video, and/or ringtones & music, as shown in Figure 4.1.

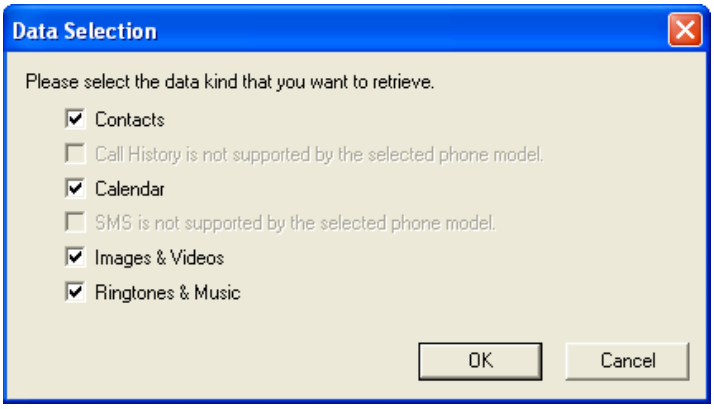

Figure 4.1 Secure View Data Selection

Acquired data is not stored or formatted in a proprietary manner, and does not require Secure View for viewing after an acquisition has been performed. The contacts, calendar, images & videos, and ringtones & music were acquired from an LG VX6100 and Secure View organized them in the folder '2008-03-10 15-43-59-LG VX6100'. In this root folder there were three subfolders named 'Camera Gallery', 'Default Graphics', and 'Default Sounds', each containing the respective file types that were acquired from the phone in their original form, along with text files containing the hex output of each. Along with these folders were four .htm files: 'Comment.htm', 'Contents.htm', 'Frame.htm', and 'Index.htm'. Index.htm provides a neatly formatted presentation of the data and information acquired from the phone. The other .htm files are unrelated to the data acquired from a phone. There are also three comma delimited Microsoft Excel .csv files, 'Calendar.csv', 'Index.csv', and 'Phonebook.csv', that contain the same information that is in the Index.htm file. The files in the three subfolders are referenced in both the .htm and .csv files, however the .htm and .csv files are not linked to each other.

Secure View 1.5 is the first version with an implementation of integrity protection. As mentioned in Chapter 2, Susteen states the MD5 hashes are used to verify and validate the integrity of acquired data and can be used to verify whether data

has been tampered with post-extraction. In the .htm and .csv report files, an MD5 hash is provided for each image & video and ringtone & music file, as well as the list of contacts, and the calendar.

4.3. Paraben Device Seizure 1.3

Paraben classifies supported mobile phones as supporting logical acquisition, physical acquisition, or both. The phones used in this study are classified by Paraben according to Table 4.2.

Table 4.2 Paraben Device Seizure Phone Support

Device Seizure Phone Support		
Phone	Carrier	Acquisition Type
Blackberry 7280	Cingular	Physical
Blackberry 7290	Cingular	Physical
LG VX5200	Verizon	Logical
LG VX6100	Verizon	Logical
Nokia 5165	Cingular	Logical and Physical
Nokia 6340i	Cingular	Logical and Physical

The types of acquirable data varied from phone to phone. Based on the phones in the above table, the LG phones provided options to acquire the 'File System', 'Phonebook', and 'SMS History', the Blackberry phones provided options to acquire 'Databases' and 'Memory Image', the Nokia 5165 allowed only the acquisition of the 'Phonebook', and the Nokia 6340i provided a long list of acquirable data including 'File System' and 'Phonebook'. The full list of acquirable data from the Nokia 6340i can be seen in Appendix B.

When Device Seizure acquires a mobile phone it saves the data in a proprietary case file that is only accessible using Device Seizure, and is protected by MD5 and SHA1 hashes. Each time a user attempts to open the case file, Device

Seizure verifies hash values before allowing access. Completing an acquisition produces five individual files that make up the overall case file:

- .ldo – Binary file, purpose unknown.
- .pds – The primary file recognized by Device Seizure that is used to open the case.
- .pds.hash – This is formatted in XML and contains two sets of different hashes, each containing a single MD5 and a single SHA1 hash.
- .viw – Binary file, purpose unknown.
- .vrs – This file contains a single MD5 hash.

An email requesting additional information regarding how the hashes in these two files are computed and used to verify data integrity was sent to Amber Schroader, CEO of Paraben Corp. She responded, “I am sorry I cannot release that information it is proprietary” (Appendix A). As a result, some conclusions based on the verification tests are speculative.

The proprietary nature of mobile phones causes the majority of problems in mobile phone forensics. Implementing proprietary integrity protection may exacerbate these issues, especially when considering the admissibility of evidence in court. The procedures or methods of a proprietary system cannot be directly understood. This makes empirically testing, determining error rates, and demonstrating the reliability of such a system more difficult. Research by Carrier (2003) determined that open source tools may more clearly and comprehensively meet admissibility requirements than closed source tools. He also stated that due to the seriousness of the issues that mobile forensics often address, such as firing employees, convicting criminals, or demonstrating innocence, “the goal of a digital forensic tool should not be market domination by keeping procedural techniques secret…the procedures used should be clearly published, reviewed and debated” (Carrier, 2003, p. 9).

The only information provided by Paraben regarding their implementation of MD5 is found in the Frequently Asked Questions for Device Seizure on their website:

> Q: How is the MD5 calculated with Device Seizure?
>
> A: MD5 is calculated just after the data acquisition from device. You can see the MD5 for each binary data entity in its properties. This MD5 is the exact hash of the binary data portion, which can be stored from any binary (image, sound etc.) entity from hex view. The same MD5 goes into the report and is shown near the file info in the report. The MD5 value that you see in workspace view in the properties window (and in reports) is calculated just once and stored in a database. It reflects the original data state. This MD5 goes into the report as well.
>
> So you can check data integrity by doing the following:
>
> Store the data entity from the hex view and then calculate its MD5 with any external tool. Then compare calculated MD5 to one shown in the properties window - they should be equal to prove data integrity (when you store the file to disk, its MD5 is calculated automatically and stored near the file itself). For the report, you can calculate the MD5 for data files stored in the report files directory (find the exact file following the link) and compare the MD5 to the one shown in report in the file info. (Paraben, 2007b, p. 1)

The hashes of interest are those located in the '.pds.hash' and '.vrs' files, which may be related to Device Seizure's active integrity protection, and are not referenced by Paraben.

4.4. Verification Tests

This section reviews the basic goals of the tests and discusses some information that applies across the study and acquisitions in general.

The verification tests had three main objectives:

- Determine how integrity protection has been implemented in Susteen DataPilot Secure View and Paraben Device Seizure.
- Evaluate the consistency of each tool by comparing results across multiple acquisitions of various mobile phones.
- Challenge each tool's ability to preserve the integrity of acquired data.

Susteen USB cables were used in the phone-pc connection for every phone in this study. The Susteen Phone Setup Wizard was used to establish the initial connection for the LG and Nokia phones. The Blackberry devices required only a basic USB connection for connectivity, so the Phone Setup Wizard was not needed. The Susteen cables and Phone Setup Wizard were used for acquisitions using both Secure View and Device Seizure. When using Device Seizure, after a connection was established with a phone using the Susteen Phone Setup Wizard, the data selection prompt from Secure View was canceled and Device Seizure was opened.

Acquisitions were configured based on the available data from the phone. In most cases, three acquisitions were performed for each unique data type and combination thereof. Hashes were recorded from every acquisition and compared to each other to determine the consistency, or lack thereof, of each tool. Then an acquisition from each tool was manipulated in various ways to test the capability of each to preserve the integrity of the data.

All optional information such as examiner name, case number, company, address, etc, was left blank for all acquisitions to limit the chance of examiner induced differences from one acquisition to another that may have an influence on a hash value. In a quick test this metadata did not appear to have an effect on the hashes that remained consistent in the lab tests, however it is impossible to determine if it has an effect on the inconsistent hashes. Since this research

focused on the data stored in mobile phones, the potential influence of this optional information was eliminated.

The BullZip MD5 Calculator was used as the third-party MD5 utility for verifying MD5 hashes provided by each forensic tool. It is available at WWW.BULLZIP.COM/DOWNLOAD.PHP.

CHAPTER 5. SUSTEEN DATAPILOT SECURE VIEW TEST RESULTS

5.1. Introduction

After completing the Phone Setup Wizard and a connection with a mobile phone has been established, Secure View automatically prompts the user to select the data to be acquired. After selecting, Secure View acquires the data and saves it to an organized directory structure as explained in Chapter 4. The phone being acquired determines which subdirectories are generated and what their names are, as well as which .csv files are generated. For example, pictures acquired from an LG VX6100 were saved to a folder called 'Camera Gallery', and pictures acquired from an LG VX5200 were saved to a folder named 'My Pix'. Aside from establishing a connection with a phone and selecting the data to be acquired, there is no other interaction with Secure View.

Secure View acquired data from each mobile phone and stored it in a way that maintained hash consistency across multiple acquisitions. There were no inconsistencies or other anomalies between the acquisitions or the phones.

Using the Bullzip MD5 Calculator it was determined that the MD5 hashes provided in the Index.htm file for the contacts, calendar, SMS and call history are calculated from hashing the respective .csv file.

5.2. Hash Comparisons

The following four tables show the hash results from Secure View for each data type from each phone over three subsequent acquisitions. Each was verified with the BullZip MD5 Calculator.

Table 5.1 Secure View LG VX5200 Hashes

LG VX5200 Hashes		
Acquisition 1		
Contacts	DataPilot	a47669ae14693eee057632a6cdb7c21a
	BullZip	a47669ae14693eee057632a6cdb7c21a
Call History	DataPilot	c7c7a0b0de140cd0ec1f5348ea81bd8f
	BullZip	c7c7a0b0de140cd0ec1f5348ea81bd8f
Acquisition 2		
Contacts	DataPilot	a47669ae14693eee057632a6cdb7c21a
	BullZip	a47669ae14693eee057632a6cdb7c21a
Call History	DataPilot	c7c7a0b0de140cd0ec1f5348ea81bd8f
	BullZip	c7c7a0b0de140cd0ec1f5348ea81bd8f
Acquisition 3		
Contacts	DataPilot	a47669ae14693eee057632a6cdb7c21a
	BullZip	a47669ae14693eee057632a6cdb7c21a
Call History	DataPilot	c7c7a0b0de140cd0ec1f5348ea81bd8f
	BullZip	c7c7a0b0de140cd0ec1f5348ea81bd8f

Table 5.2 Secure View LG VX6100 Hashes

LG VX6100 Hashes		
Acquisition 1		
Contacts	DataPilot	5915635273fd7ecff0a2e2c404e04dab
	BullZip	5915635273fd7ecff0a2e2c404e04dab
Calendar	DataPilot	e8f442fccbf45a7ba8022eb514d8da14
	BullZip	e8f442fccbf45a7ba8022eb514d8da14
Acquisition 2		
Contacts	DataPilot	5915635273fd7ecff0a2e2c404e04dab
	BullZip	5915635273fd7ecff0a2e2c404e04dab
Calendar	DataPilot	e8f442fccbf45a7ba8022eb514d8da14
	BullZip	e8f442fccbf45a7ba8022eb514d8da14
Acquisition 3		
Contacts	DataPilot	5915635273fd7ecff0a2e2c404e04dab
	BullZip	5915635273fd7ecff0a2e2c404e04dab
Calendar	DataPilot	e8f442fccbf45a7ba8022eb514d8da14
	BullZip	e8f442fccbf45a7ba8022eb514d8da14

Table 5.3 Secure View Nokia 5165 Hashes

Nokia 6340i Hashes		
Acquisition 1		
Contacts	DataPilot	0dfddbeeac4ab9c114ab5c50947cde35
	BullZip	0dfddbeeac4ab9c114ab5c50947cde35
Acquisition 2		
Contacts	DataPilot	0dfddbeeac4ab9c114ab5c50947cde35
	BullZip	0dfddbeeac4ab9c114ab5c50947cde35
Acquisition 3		
Contacts	DataPilot	0dfddbeeac4ab9c114ab5c50947cde35
	BullZip	0dfddbeeac4ab9c114ab5c50947cde35

Table 5.4 Secure View Nokia 6340i Hashes

Nokia 6340i Hashes		
Acquisition 1		
Contacts	DataPilot	dd5ec3b8c4d65b4df8dab887b0904ea0
	Calculator	dd5ec3b8c4d65b4df8dab887b0904ea0
Acquisition 2		
Contacts	DataPilot	dd5ec3b8c4d65b4df8dab887b0904ea0
	Calculator	dd5ec3b8c4d65b4df8dab887b0904ea0
Acquisition 3		
Contacts	DataPilot	dd5ec3b8c4d65b4df8dab887b0904ea0
	Calculator	dd5ec3b8c4d65b4df8dab887b0904ea0

Although Secure View appears to generate reliable hash values for the acquired data, there are other concerns regarding the manner in which the data is stored. Most significantly, all of the acquired data and MD5 hashes are hard-coded into the Index.htm and .csv files, and these files are independent from Secure View and from each other.

5.3. Integrity Protection

The acquired data and MD5 hashes are processed once and then saved to the case files. There is no active integrity protection. It is up to the examiner to check file integrity by re-computing the hash values of specific files and comparing them to the originals provided by Secure View. This may not be as efficient as intended for a number of reasons, and may leave greater potential for the acquired data to become unknowingly corrupted or tampered with.

The Index.htm is the formal report document suitable for printing. Since the hashes in the Index.htm are calculated from the .csv files, they do not guarantee the integrity of the contents of the Index.htm file. Validating the hash is irrelevant in this case. Since it represents a different source of data, it can be positively verified while data may still have changed in the Index.htm file. Since all of the files generated by Secure View are plaintext, independent from one another, and viewed with applications that may not be forensically sound, none of their contents, including the hashes, can be relied upon for verification purposes. Any data in the files could become corrupt and the examiner would be unaware unless it was specifically verified by another means. If someone was intent on tampering with the case files, editing a .csv file, computing its new hash, and editing the Index.htm file to match the new information is easily accomplished. There is no hash of Index.htm provided by Secure View, but if there was, it could be just as easily altered. A backup hash database of all the files, including the Index.htm file, stored separately from the case file would be necessary for integrity verification purposes. As implemented, the hash values provide no security against tampering. As far as protection is concerned, Secure View does not offer any significant advantages over a forensic tool with zero hash functionality, however the consistency of the hashes produced for the various data types across multiple acquisitions

CHAPTER 6. PARABEN DEVICE SEIZURE TEST RESULTS

6.1. Introduction

Device Seizure is more intricate and provides much more functionality than Secure View, however its more complex and proprietary nature made determining the purpose and implementation of MD5 more difficult. Hash values were both consistent and inconsistent across multiple acquisitions depending on the selection of the data that was acquired and which phone was used.

Since there are multiple hashes in use by Device Seizure, the following samples of the key files are provided for clarification as to which hash is being referenced in discussion.

```
<?xml version="1.0"?>
<Hashes xmlns:xsd="http://www.w3.org/2001/XMLSchema"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">
  <MD5>e6f79d9b1e801e8955572dfffb65707a</MD5>
  <SHA1>51863508ed21d599254d484cb27eb31b452b0d3d</SHA1>
</Hashes><?xml version="1.0"?>
<Hashes xmlns:xsd="http://www.w3.org/2001/XMLSchema"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">
  <MD5>9b17d72454bb3442986592ed40029902</MD5>
  <SHA1>7907df3acf81458bfab9f4932c2ae75d49cec515</SHA1>
</Hashes>
```

Figure 6.1 Sample '.pds.hash' File from Paraben Device Seizure

Note there are two different sets of hashes in a .pds.hash file. The first and second MD5 hash will simply be referred to as hash 1 and hash 2, respectively. The SHA1 hashes were of no interest in this research.

```
4d5de0fcf0e673cd1f2d1fffe5820476
```

Figure 6.2 Sample .vrs File from Paraben Device Seizure

The .vrs file contains only a single MD5 hash. This file was identical for every acquisition regardless or the phone or data being acquired. This agrees with the experiences of Williamson et al. (2006). Perhaps this hash is product key related.

Remember .ldo, .pds, and .viw are the other three files generated by Device Seizure for a case file. Using the Bullzip MD5 calculator to calculate the hashes of these files, it was apparent that hash 1 is a hash of the .pds file, and hash 2 is of the .ldo file.

When a report was generated, the main hash provided for the case was always identical to hash 1. This is contrary to Williamson et al. (2006), who stated in his research that the hash provided in the reports did not match those in .pds.hash file, however they did evaluate an older version of Cell Seizure.

Device Seizure saves a timestamp of when the acquisition was performed in every case file. For this reason alone hash 1 will always be different for every acquisition.

6.2. Hash Comparisons

The following table shows the hash values from the .pds.hash files over multiple acquisitions with varying selections of data from an LG VX6100 mobile phone.

For LG mobile phones, Device Seizure provides a selection to acquire the file sytem, phonebook, or SMS history from the phone. Acquisitions 1 through 3 acquired the file system, phonebook, and SMS history, 4 through 6 acquired only the phonebook, 7 through 9 acquired only the SMS history, and 10 through 12 acquired only the file system.

Table 6.1 Device Seizure LG VX6100 Hash Comparison

LG VX6100 Hash Comparison			
Ac.	Data Acquired	Hash 1 (.pds file)	Hash 2 (.ldo file)
1	FS, PB, SMS	e6f79d9b1e801e8955572dfffb65707a	9b17d72454bb3442986592ed40029902
2	FS, PB, SMS	35c7d4594b31b1206c3b401545a5b351	ccf0995fc06f8a2720cc314123432ba5
3	FS, PB, SMS	b1df741c091d585e99e903e6cb068c04	27506adcad3c92bb4b3c04141024a045
4	PB Only	fd370fceb59bbca85ebd0d082dbf6b9a	ac7527a4d7c2c23a8abe5f54413e8184
5	PB Only	d49ddede6f3bc8597640480138a5f640	ac7527a4d7c2c23a8abe5f54413e8184
6	PB Only	905dca27537e4b774a3f08e33231fb05	ac7527a4d7c2c23a8abe5f54413e8184
7	SMS Only	745f16d505c8f12d6938c88127d1bf0f	ac7527a4d7c2c23a8abe5f54413e8184
8	SMS Only	8d69baf4fb4885ca4c076ab244a42f6f	ac7527a4d7c2c23a8abe5f54413e8184
9	SMS Only	83a6fce2bb86751260c312db0ba35152	ac7527a4d7c2c23a8abe5f54413e8184
10	FS Only	0ce1a0b50c2af5b6a65db42b63e811cc	583f87324d7f0762216b0b949e3c8c21
11	FS Only	e8e8f1421b70762addbd0954ad7c9bec	7c395c6c27f4e54d3880ce0d49497783
12	FS Only	2bb7cbb9e303a1ac81e6033f8afccda8	fd9b36039e39a3e17a7f0dc1d5573d40

The value of hash 2 and the contents of the .ldo file are related to the data that is acquired from the phone. With the LG VX6100, the .ldo file is empty when the file system is not acquired, resulting in the consistent hash.

The next table shows similar acquisitions from an LG VX 5200, with similar results.

Table 6.2 Device Seizure LG VX5200 Hash Comparison

LG VX5200 Hash Comparison			
Ac.	Data Acquired	Hash 1 (.pds file)	Hash 2 (.ldo file)
1	FS, PB, SMS	5a870ec38ed3f605be050a5de208613b	4f5b506c478eb1f513fbf8b1da9fad9f
2	FS, PB, SMS	70e762dc5fc314117a976eee0394b513	401470b3cd893aae5bcca0ad98223b1b
3	FS, PB, SMS	4a73661e2d0f4d53b1dd10d87f2af044	0e0054ab94cc166860c2f2eeadb6cc43
4	SMS Only	2e743b5ae60d566090b3de60c1842856	ac7527a4d7c2c23a8abe5f54413e8184
5	SMS Only	72de60d4354dd617712036938b2365ca	ac7527a4d7c2c23a8abe5f54413e8184
6	SMS Only	6d93c8fa5218bf38b8d53fb02d0a8e7d	ac7527a4d7c2c23a8abe5f54413e8184
7	PB, SMS	57e0d278f0fea33fcf8024472146a1be	ac7527a4d7c2c23a8abe5f54413e8184
8	PB, SMS	1eee1edeaaba361a662457a719533af4	ac7527a4d7c2c23a8abe5f54413e8184
9	PB, SMS	d27e78cb594cc765add121856ba2fb1c	ac7527a4d7c2c23a8abe5f54413e8184

These acquisitions provided the same hash 2 values for acquisitions that did not include the file system, and the same inconsistency throughout the rest of the hashes.

The next two tables show results from the Nokia 5165 and 6340i mobile phones.

Table 6.3 Device Seizure Nokia 5165 Hash Comparison

Nokia 5165 Hash Comparison			
Ac.	Data Acquired	Hash 1 (.pds file)	Hash 2 (.ldo file)
1	PB	4ac3771d4a1a1e0574b59abec34b3bef	ac7527a4d7c2c23a8abe5f54413e8184
2	PB	25f49b0510fa0d2bdbe4b1f9af8ad11d	ac7527a4d7c2c23a8abe5f54413e8184
3	PB	50dbc3d74dd951142f89bfe9d393df78	ac7527a4d7c2c23a8abe5f54413e8184

The Nokia 5165 allowed only the acquisition of the phonebook. The .ldo file was empty, producing the same.

Table 6.4 Device Seizure Nokia 6340i Hash Comparison

Nokia 6340i Hash Comparison			
Ac.	Data Acquired	Hash 1 (.pds file)	Hash 2 (.ldo file)
1	All	829b0f4a45d6ce3b87354343f5721cac	cdd0772f3a64d874c3720e52c840bbb3
2	All	574c35dc6034c9ee96c31d95731e0663	cdd0772f3a64d874c3720e52c840bbb3
3	All	05eb6d5d683ee383796ffa789c184d3c	cdd0772f3a64d874c3720e52c840bbb3
4	PB	ad3cd005776baacd2a9ff545d11b2ff1	ac7527a4d7c2c23a8abe5f54413e8184
5	PB	29ae0588d8c7751e919f080cb26247cf	ac7527a4d7c2c23a8abe5f54413e8184
6	PB	0d1cebf038b228fd133accabcc96410a	ac7527a4d7c2c23a8abe5f54413e8184
7	FS	67e8ca50ca98f765f8a366884aa07b55	ac7527a4d7c2c23a8abe5f54413e8184
8	FS	037f50d117b3377df54cef2844c24def	ac7527a4d7c2c23a8abe5f54413e8184
9	FS	b8ded0814a012be5c41c8f21e2b10d60	ac7527a4d7c2c23a8abe5f54413e8184

No data was obtained from the Nokia 6340i when only the file system was acquired, so it had no affect on hash 2. Hash 1 was still different between of the varying timestamps in the case file. When all of the data options were selected, some information was saved to the .ldo file. It is not clear which data type(s) specifically provided the acquired data.

Next, the two Blackberry devices were acquired. There were only two options for the data selection: databases and memory images.

Table 6.5 Device Seizure Blackberry 7280 Hash Comparison

Blackberry 7280 Hash Comparison			
Ac.	Data Acquired	Hash 1 (.pds file)	Hash 2 (.ldo file)
1	DB, Mem	00adf336250d321139bccdfdddcdeab4	5fb14ead69e47abb6872b31cf919dc36
2	DB, Mem	95ea7865c45623159137983550fcaf89	bf23afd05da5dedf04679a04b4b2004c
3	DB, Mem	b415f7365cec95247b4ad46358506548	c6b31a0e64a8e43f9752897b4df02f23
4	DB	df881c0f2a269a9511f6912e8a1faf36	02667b6e5fd319bcbd3526335d051ff6
5	DB	196f860a09b08a466f124d3d53b62498	02667b6e5fd319bcbd3526335d051ff6
6	DB	9c23fefd7b3dd990d374c96782fdbc25	02667b6e5fd319bcbd3526335d051ff6
7	Mem	a48e1b17869df7cef2df799155c65f26	aa56e2818d9f8498581a9f61ffb3ee51
8	Mem	be13329e893b51a4f95664df7c1c97ee	bca5c596c0aca01738d0bf9a04be8988
9	Mem	cb6fc04f7ee7666c023e03596f7fbd43	e4c8b40abf23c222b35cba8d1f8b2f5d

Table 6.6 Device Seizure Blackberry 7290 Hash Comparison

Blackberry 7290 Hash Comparison			
Ac.	Data Acquired	Hash 1 (.pds file)	Hash 2 (.ldo file)
1	DB, Mem	7168c65c73f0de82fac4cf231114b545	38e76c3886a3378c5fd1e3991762f441
2	DB, Mem	c15fa319fdb81c19a5af932d5e327b31	e5a5c145b4608ba9d42012242b5288c6
3	DB, Mem	31d4eac6c476628c0879cf2827e94feb	4493b0ecb1a484c521f6377a3121bea9
4	DB	9087770cedeaa48aa4e3ed8812cd7bb4	b3af19e75b128a4559b1eaffbc1296fc
5	DB	a7e4b8c36a4f30147c6343f9e01715de	1f226bb3c1ae988849af4370addca042
6	DB	21ceac95a2ed9901d157f817bf02d4be	835f06482381051051e6331034763105
7	Mem	d852b37ef45ce376a70d486c5ddd5f79	c5e5a7c23e37ba22dcfb468704681fa0
8	Mem	696865b76c6b4310afba9e5e7d65518a	c5e5a7c23e37ba22dcfb468704681fa0
9	Mem	5a567c7ab6b26070b2bae352a5decb14	c5e5a7c23e37ba22dcfb468704681fa0

Between the Blackberry 7280 and 7290, acquiring the databases and memory image had opposite effects. The 7280 produced a consistent hash 2 for databases and not for memory images. The 7290 produced a consistent hash 2 for memory image and not databases. In any case, there was always data present in the .ldo file.

The hashes provided by Device Seizure are of little use in manually verifying the integrity of data. Hash 1 is provided in the report but has absolutely no consistency across multiple acquisitions due to the timestamp. It is not clear if there are additional aspects affecting hash 1.

Upon further examination of the .pds.hash file, it was discovered that hash 1 sometimes changes after an acquisition is saved or closed. This occurred inconsistently based on the phone and data acquired. If the file system was selected when acquiring the LG VX6100, Device Seizure prompted to re-save the case before closing it. This also happened when acquiring everything from the Nokia 6340i and Blackberry 7280. It was a result of Device Seizure automatically rendering the images in the acquired data after the acquisition was completed. This changed the .pds file, which altered its hash. When acquiring the Blackberry 7290, Device Seizure did not ask to re-save before closing the case file, however hash 1 still changed when the case was close.

In a case file, Device Seizure allows an examiner to identify certain files and data by enabling their associated checkboxes. If an examiner makes such changes, the case file must be saved. The hashes in .pds.hash never changed when making modifications to the case file were made.

6.3. Case Comparisons

Device Seizure has a feature that compares two cases to identify what differs between them. This was used in several comparisons, shown in table 6.7.

Table 6.7 Paraben Device Seizure Case Comparisons

Comp.	Phone	Acquisitions	Data	Table	Hash1 Diff	Hash2 Diff
1	LG VX6100	1 and 2	FS, PB, SMS	6.1	Yes	Yes
2	LG VX6100	1 and 3	FS, PB, SMS	6.1	Yes	Yes
3	LG VX5200	1 and 2	FS, PB, SMS	6.2	Yes	Yes
4	LG VX5200	1 and 3	FS, PB, SMS	6.2	Yes	Yes
5	LG VX5200	8 and 9	PB, SMS	6.2	Yes	No
6	Nokia 5165	1 and 2	PB	6.3	Yes	No
7	Nokia 6340i	1 and 2	All	6.4	Yes	No
8	Blackberry 7280	1 and 2	DB, Mem	6.5	Yes	Yes
9	Blackberry 7290	1 and 2	DB, Mem	6.6	Yes	Yes

This table shows the comparison number, phone, acquisitions, data acquired, referring table, and whether the hashes were different between the two acquisitions.

The first comparison, between acquisitions 1 and 2 of the LG VX6100 revealed three files that were different, ‘nvm_0000’, ‘nvm_0005’, and ‘0002’. Figures 6.3 to 6.5 show these files and their different hashes. Figures 6.6 to 6.8 show the content of the files.

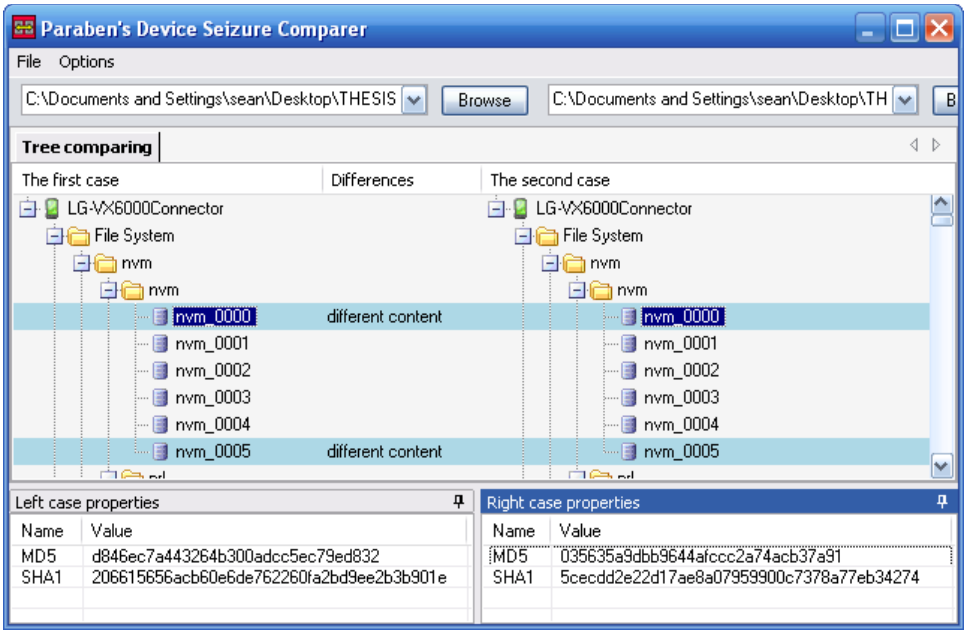

Figure 6.3 LG VX6100 Acquisitions 1 and 2 'nvm_0000' file

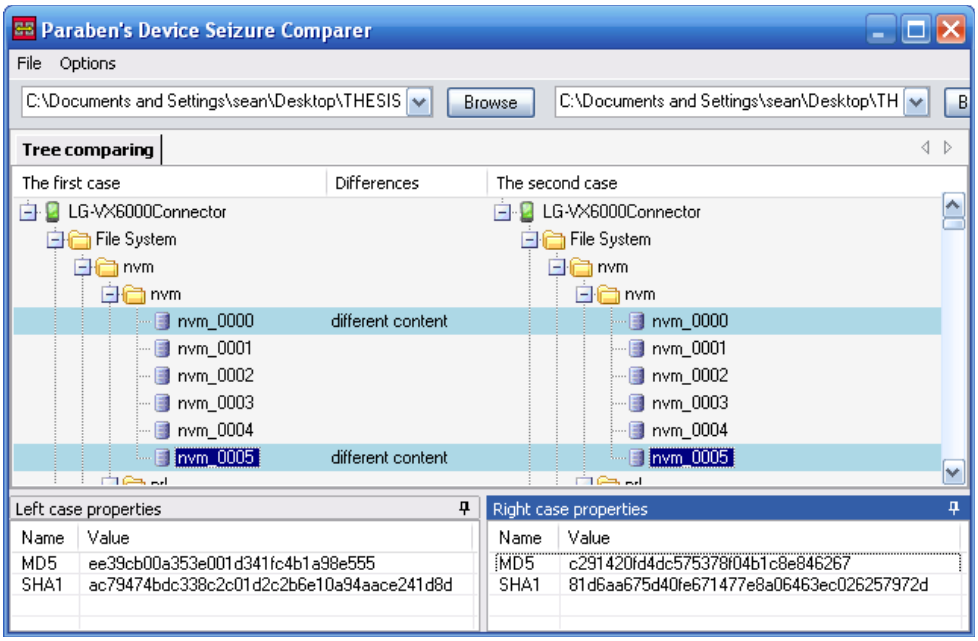

Figure 6.4 LG VX6100 Acquisitions 1 and 2 'nvm_0005' file

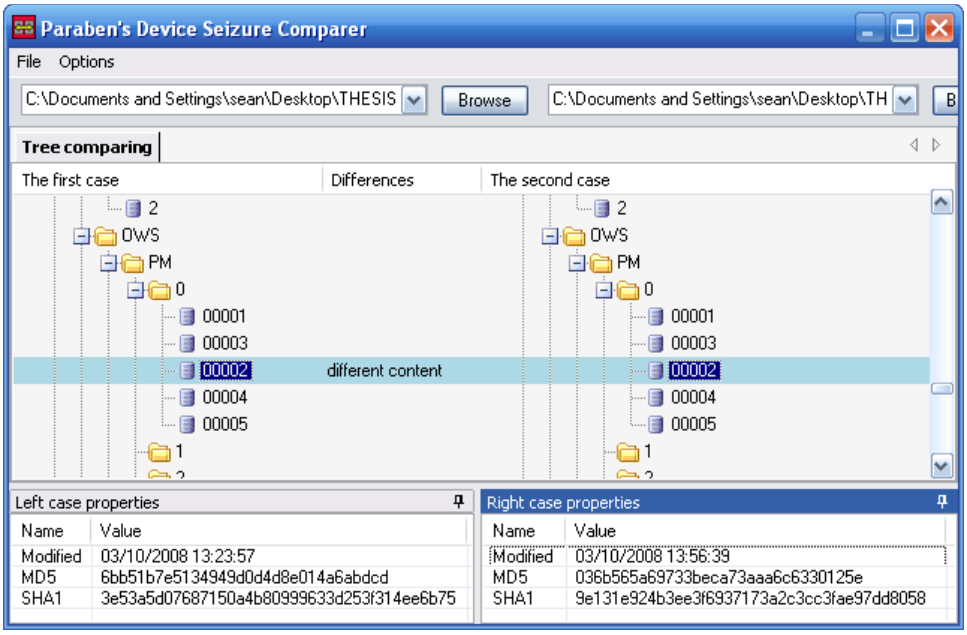

Figure 6.5 LG VX6100 Acquisitions 1 and 2 '00002' file

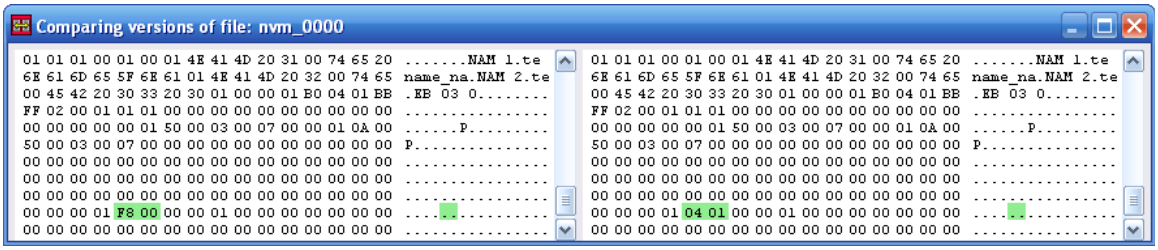

Figure 6.6 LG VX6100 Acquisitions 1 and 2 'nvm_0000' Content

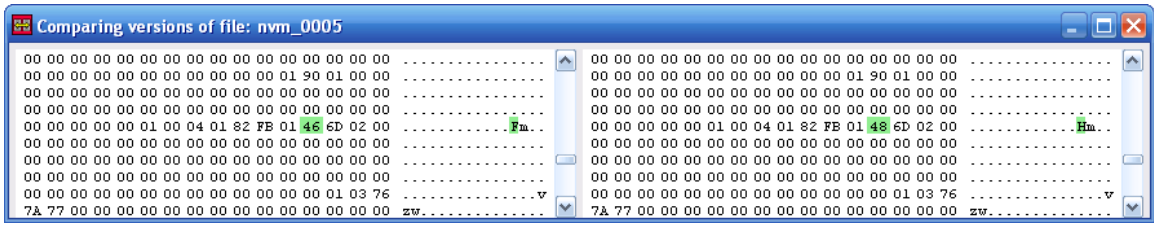

Figure 6.7 LG VX6100 Acquisitions 1 and 2 'nvm_0005' Content

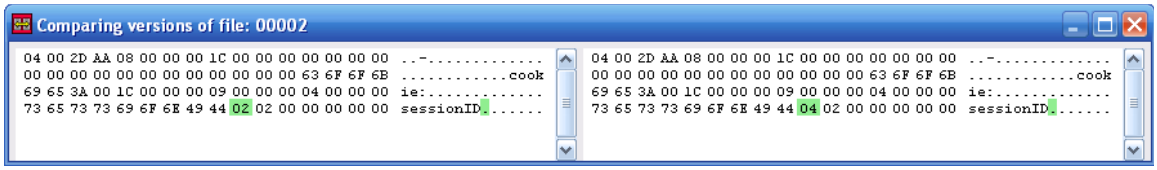

Figure 6.8 LG VX6100 Acquisitions 1 and 2 '00002' Content

The values in the files nvm_0005 and 0002 both differ by an increment of two. The value in 0002 reflects a session ID. Comparison 2 of acquisitions 1 and 3 revealed a difference of four in the same values, showing the session ID incremented by two for each subsequent acquisition.

Comparisons 3 and 4 of the LG VX5200 showed similar differences in the same files as the LG VX6100. In addition, file 'nvm_0002' and the image '1017061222.jpg' were different. Figures 6.9 and 6.10 show the differing image file across all three acquisitions, and Figure 6.11 shows the actual image.

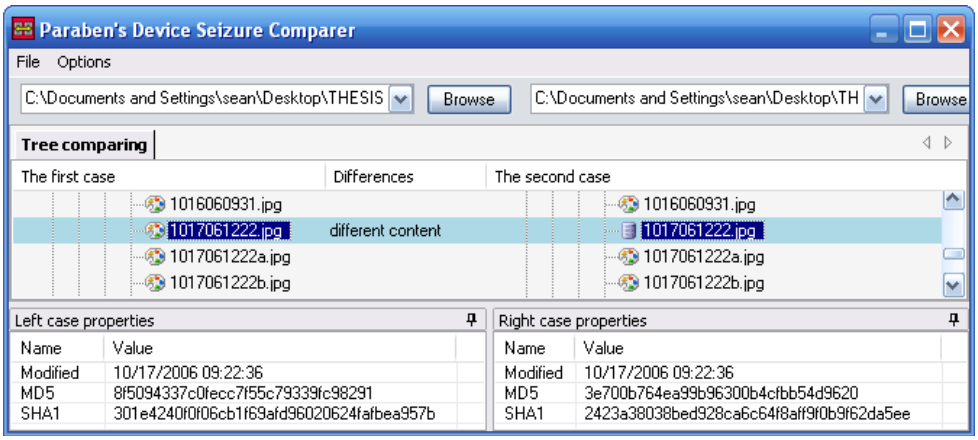

Figure 6.9 LG VX5200 Acquisitions 1 and 2 '1017061222.jpg'

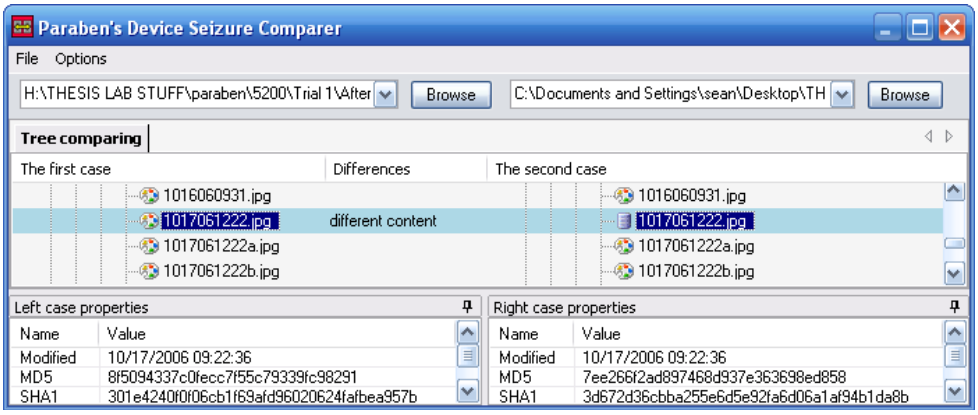

Figure 6.10 LG VX5200 Acquisitions 1 and 3 '1017061222.jpg'

The icon next to the image file name is different between acquisition one and acquisitions two and three, and the hashes are different across all three. Some system files are expected to differ from acquisition to acquisition due to timestamps or other system information such a session ID, as seen in these examples, however it is not clear why an image is different across multiple acquisitions. This was the only occurrence of this that was found.

Figure 6.11 LG VX5200 '1017061222.jpg'

Figure 6.11 is the actual image exported from a case file. The image is a black rectangle in all three acquisitions. Its source is unknown, but as you can see in Figure 6.10 there are other images with similar filenames.

Comparison 5 is of the phonebook and SMS from the LG VX5200. Figure 6.12 shows the results.

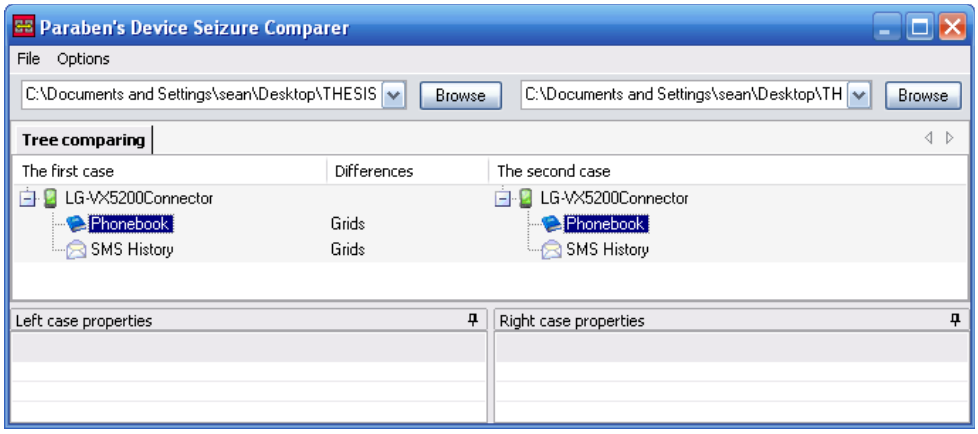

Figure 6.12 LG VX5200 Acquisitions 8 and 9 Phonebook and SMS

Device Seizure did not highlight the different items this time, however it noted that the 'Grids' were different between the phonebooks and SMS History in each acquisition. Grid may refer to the table that the acquired data is saved in, like a spreadsheet. Within Device Seizure, when viewing the phonebook or sms history, the table that contains the information is labeled as "Grid." Reviewing the reports generated from each case did not reveal any differences in the data acquired form the phone. The only apparent difference between the two reports is timestamp of when the acquisition was performed, so the Grid difference is a result of Device Seizure and not the phone.

Comparisons 6 and 7, of the Nokia 5165 and 6340i mobile phones, both produced only Grid differences across the acquisitions. Since the hashes from

the acquisitions 1 through 3 of the Nokia 6340i were consistent, and only Grid differences exist between the acquisitions, data specific hashes must be possible within Device Seizure's functionality.

Comparison 8 of the Blackberry 7280 has grid differences and a different size memory image, shown in Figure 6.13.

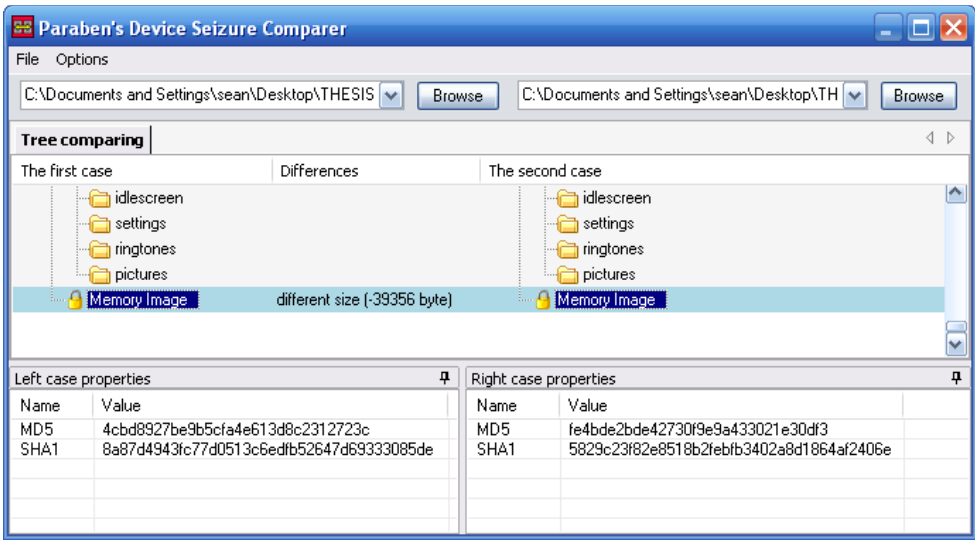

Figure 6.13 Blackberry 7280 Comparison

Comparison 9 of the Blackberry 7290 had grid differences and different content in two binary files. The memory of the 7290 was not different.

6.4. Case File Manipulation

To see how Device Seizure responds to tampered or corrupted data, each case file was manipulated and then the .pds file re-opened.

If the hash in the .vrs file is altered, Device Seizure throws an error stating that the case file is not supported or corrupt, as shown in Figure 6.14.

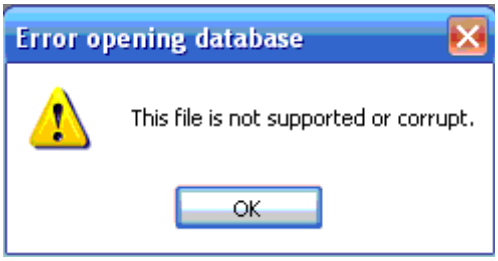

Figure 6.14 '.vrs' Manipulation

If either of the hashes in the .pds.hash file are changed, they are returned to their original values by Device Seizure upon opening and closing the case file. If the .pds.hash file is deleted, the case file still opens normally, and a new .pds.hash file is created when the case is closed. It is not clear if these hashes are the ones used to maintain the integrity of the data, but it is clear that this file is not their source.

If the .ldo or .pds files are manipulated, Device Seizure says the hashes are different, as shown in Figure 6.15.

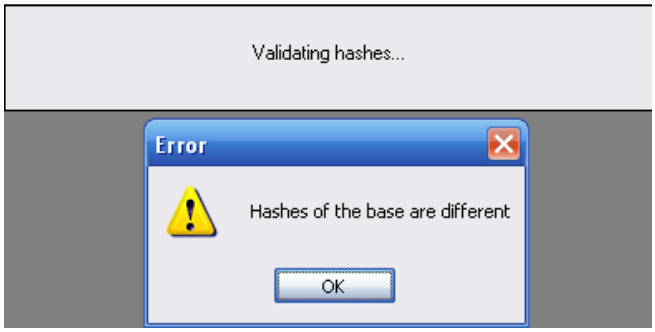

Figure 6.15 '.ldo' Manipulation

If the hash in the .pds.hash file is replaced with the new hash of a manipulated .ldo or .pds file, Device Seizure still says the hashes do not match. This makes

sense since it has already been shown that the .pds.hash file is not used by Device Seizure for integrity preservation.

Manipulating the .viw file causes Device Seizure to throw a storage format error, shown in Figure 6.16.

Figure 6.16 '.viw' Manipulation

Based on these tests it is clear Device Seizure actively maintains some form of integrity protection for the case files. If any one of these errors is encountered then the case file and its contents are no longer accessible.

CHAPTER 7. CONCLUSION

Both Susteen DataPilot Secure View and Paraben Device Seizure offer valuable solutions for maintaining the integrity of mobile forensic case files. Most notably, Secure View produces consistent hashes for unique data types, and Device Seizure stores data in a secure case file with active integrity protection. Both of these tools also have weaknesses that make them more easily scrutinized in a court of law. For example, Secure View stores data in a way that can be easily modified, and the processes of Device Seizure are propriety and its hashing implementation is not as granular or consistent as it could be for certain types of data. Device Seizure may be capable of acquiring far more data than Secure View, however even if it acquires data from a mobile phone that is inconsistent from one acquisition to another, this data can be distinguished from data that does not change.

An implementation that incorporates functionality from both tools would offer more effective integrity protection that would also be more acceptable in a court of law. Integrity protection would be more effective because more granular hash results would be generated while a high level of security is maintained. This would contribute to the concept of repeatability because it would clearly distinguish consistent and inconsistent data, showing that there is valuable information in mobile phones that can be reliably acquired and verified. Moving away from a proprietary mentality would benefit the ability to empirically test and peer review the methodology of tools in forensic acquisitions. As a result, such forensic tools would be more easily subjected to basic admissibility guidelines, such as those introduced by Daubert, in determining the legal relevance of the tool and its results.

LIST OF REFERENCES

AccessData. (2006). "White Paper: MD5 Collisions – The Effect on Computer Forensics." Retrieved March 1, 2008 from, HTTP://WWW.ACCESSDATA.COM/MEDIA/EN_US/PRINT/PAPERS/WP.MD5_COLLISIONS.EN_US.PDF

Ayers, R., Jansen, W., Moenner, L., Delaitre, A. (2007). "Cell Phone Forensic Tools: An Overview and Analysis Update." Retrieved February 12, 2008, from HTTP://CSRC.NIST.GOV/PUBLICATIONS/NISTIR/NISTIR-7387.PDF

Carrier, B. (2003). "Open Source Digital Forensic Tools." Retrieved March 13, 2008, from HTTP://WWW.DIGITAL-EVIDENCE.ORG/PAPERS/OPENSRC_LEGAL.PDF

CTIA-The Wireless Association. (2007). "CTIA's Semi-Annual Wireless Industry Survey." Retrieved February 19, 2008, from HTTP://FILES.CTIA.ORG/PDF/CTIA_SURVEY_MID_YEAR_2007.PDF

"Federal Rules of Evidence." (2004). Retrieved February 24, 2008, from HTTP://JUDICIARY.HOUSE.GOV/MEDIA/PDFS/PRINTERS/108TH/EVID2004.PDF

"Frye v. United States." Retrieved February 24, 2008, from HTTP://LAW.JRANK.ORG/PAGES/12871/FRYE-V-UNITED-STATES.HTML

International Union of Pure and Applied Chemistry. (1997). "Repeatability." Retrieved February 29, 2008, from HTTP://WWW.IUPAC.ORG/GOLDBOOK/R05293.PDF

Jansen, W., Ayers, R. (2007). "Guidelines on Cell Phone Forensics." Retrieved February 20, 2008, from HTTP://CSRC.NIST.GOV/PUBLICATIONS/NISTPUBS/800-101/SP800-101.PDF

M2 Communications. (2006). "Many countries now have mobile penetration rate about 100%, report says." Retrieved February 19, 2008, from HTTP://FINDARTICLES.COM/P/ARTICLES/MI_M0ECZ/IS_2006_JUNE_9/AI_N16464839

McCarthy, P. (2005). "Forensic Analysis of Mobile Phones." Retrieved February 20, 2008, from HTTP://ESM.CIS.UNISA.EDU.AU/NEW_ESML/RESOURCES/PUBLICATIONS/FORENSIC%20ANALYSIS%20OF%20MOBILE%20PHONES.PDF

McCreight, S., Patzakis, J. (2001). "Hash Sets and Their Proper Construction." Retrieved March 8, 2008, from HTTP://ISIS.POLY.EDU/KULESH/FORENSICS/DOCS/HASHSET.PDF

Newitz, A. (2007). "Courts Cast Wary Eye on Evidence Gleaned From Cell Phones." Retrieved February 20, 2008, from HTTP://WWW.WIRED.COM/POLITICS/LAW/NEWS/2007/05/CELLPHONE_FORENSICS

Nordberg, P. (2007). "The Daubert Worldview." Retrieved February 24. 2008, from HTTP://WWW.DAUBERTONTHEWEB.COM/SUBSTANCE.HTM

O'Connor, T. (2006). "Admissibility of Scientific Evidence Under Daubert." Retrieved February 24, 2008, from HTTP://WWW.APSU.EDU/OCONNORT/3210/3210LECT01A.HTM

Paraben Corporation. (2007a). "Device Seizure v1.3 – Cell Phone & PDA Forensic Software." Retrieved March 3, 2008, from HTTP://WWW.PARABEN-FORENSICS.COM/CATALOG/PRODUCT_INFO.PHP?CPATH=25&PRODUCTS_ID=405

Paraben Corporation. (2007b). "Frequently Asked Questions for Device Seizure." Retrieved February 29, 2008, from HTTP://SUPPORT.PARABEN.COM/DEVICEFAQ.HTML

Ridley, K. (2007). "Global mobile phone use to hit record 3.25 billion." Retrieved February 19, 2008, from HTTP://WWW.REUTERS.COM/ARTICLE/COMPANYNEWSANDPR/IDUSL2712199720070627

Rivest, R. (1992). "RFC 1321 – The MD5 Message-Digest Algorithm." Retrieved March 1, 2008, from HTTP://WWW.FAQS.ORG/RFCS/RFC1321.HTML

Schneier, B. (2004). "Opinion: Cryptanalysis of MD5 and SHA: Time for a new standard." Retrieved March 1, 2008, from HTTP://WWW.COMPUTERWORLD.COM/INDUSTRYTOPICS/DEFENSE/STORY/0,10801,95343,00.HTML

Susteen Inc. (2008). "DataPilot Secure View Kit for Forensics – Features." Retrieved March 3, 2008, from HTTP://WWW.DATAPILOT.COM/PRODUCTDETAIL/253/FEATURES/NOTEMPTY

Taylor, B., Kuyatt, C. (1994). "Guidelines for Evaluating and Expressing the Uncertainty of NIST Measurement Results." Retrieved February 29, 2008, from HTTP://PHYSICS.NIST.GOV/PUBS/GUIDELINES/TN1297/TN1297S.PDF

Wang, X., Feng, D., Lai, X., Yu, H. (2004). "Collisions for Hash Functions MD4, MD5, HAVAL-128 and RIPEMD." Retrieved March 1, 2008, from HTTP://EPRINT.IACR.ORG/2004/199.PDF

Williamson, B., Apeldoorn, P., Cheam, B., McDonald, M. (2006). "Forensic Analysis of the Contents of Nokia Mobile Phones." Retrieved February 10, 2008, from HTTP://SCISSEC.SCIS.ECU.EDU.AU/WORDPRESS/CONFERENCE_PROCEEDINGS/2006/FORENSICS/WILLIAMSON%20ET%20AL%20-%20FORENSIC%20ANALYSIS%20OF%20THE%20CONTENTS%20OF%20NOKIA%20MOBILE%20PHONES.PDF

Appendix A. Email Correspondence

From: "Amber Schroader" <redacted>
Subject: RE: Device Seizure hashes
Date: February 18, 2008 11:32:29 AM GMT-05:00
To: "'Sean Sobieraj'" <redacted>
Cc: "'Richard P Mislan'" <redacted>

Sean,
I am sorry I cannot release that information it is proprietary.
--Amber

-----Original Message-----
From: Sean Sobieraj [redacted]
Sent: Wednesday, February 13, 2008 9:29 AM
To: "Amber Schroader" <redacted>
Cc: 'Richard P Mislan'
Subject: Re: Device Seizure hashes

Amber,
Sorry, we will be using the information to understand how MD5 is being implemented in an effort to verify that the integrity of mobile forensic case files is maintained. We are looking at several products that have implemented some form of integrity protection. I am using this work for my thesis.
Thanks,
Sean

On Feb 13, 2008, at 9:34 AM, Amber Schroader wrote:
Sean,
Before I answer what is this information being used for?
--Amber
Paraben Corp.

-----Original Message-----
From: Sean Sobieraj [redacted]
Sent: Friday, February 08, 2008 3:49 PM
To: "Amber Schroader" <redacted>

Cc: Richard P Mislan
Subject: Device Seizure hashes

Amber,
I am a graduate student at Purdue University and I am writing a thesis on mobile phone forensics and integrity management with Rick Mislan. I am curious how Device Seizure computes the hashes it uses to verify data integrity. I see two sets of hashes in the '.pds.hash' file and a single hash in the '.vrs' file that are created during an acquisition. I am interested in what each of these hashes (and others if I missed them) represent, how they are calculated, from what data, and how each are used to verify the integrity of the collected data. Any information would be appreciated, however I understand if you are unable to provide such details.
Thanks,
Sean

--
Sean Sobieraj
Graduate Student
Center for Education and Research in Information Assurance and Security (CERIAS)
Purdue University

Figure A.1 Email with Amber Schroader, CEO of Paraben Corp.

No response.

-----Original Message-----
From: Sean Sobieraj [redacted]
Sent: Monday, March 31, 2008 9:45 AM
To: "Javier Martinez" <redacted>
Cc: Richard P Mislan
Subject: Secure View Hash Implementation

Javier,
I am a graduate student at Purdue University and I am writing a thesis on verifying case file integrity in mobile phone forensics with Rick Mislan.
I am curious how hashing is implemented in the new version of Susteen DataPilot, and how the hashes are used to verify data integrity. I see that DataPilot provides hashes for the different

data types acquired from the phone (contacts, call history, phonebook, each image, etc). I am interested in things such as how these hashes are calculated, at what point in the acquisition process, from what data, and how they can be used to verify whether data is tampered with.
It would also be helpful to know how DataPilot acquires information from a phone (AT commands, OBEX, F-Bus, etc).
We will be using the information to understand various implementations of MD5 and how they are used to maintain the integrity of a mobile forensic case file. We are looking at several products that have implemented some form of integrity protection.
Any information would be appreciated, however I understand if you are unable to provide such details.
Thanks,
Sean

--
Sean Sobieraj
Graduate Student
Center for Education and Research in Information Assurance and Security (CERIAS)
Purdue University

Figure A.2 Email with Javier Martinez, Susteen Inc.

Appendix B. Nokia 6340i Data Selection

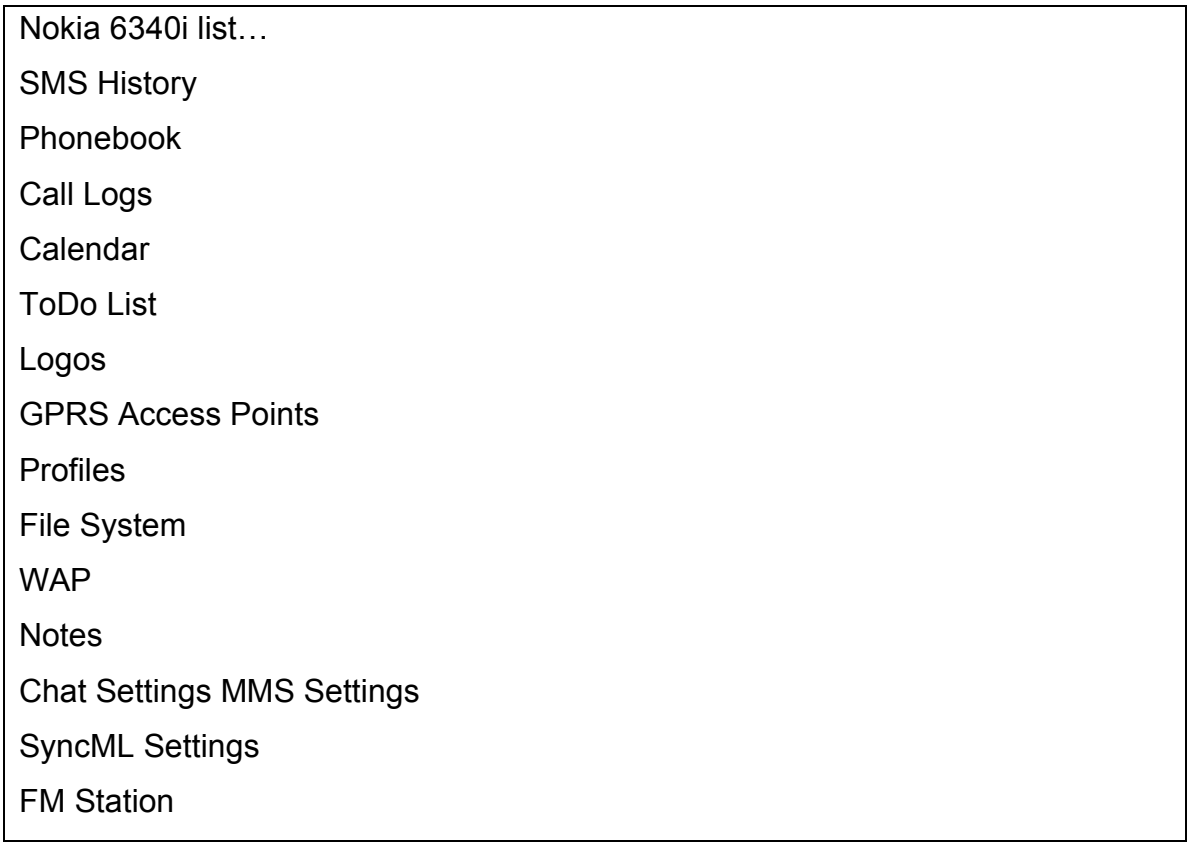

Figure B.1 Device Seizure Selection of Data from Nokia 6340i

LIST OF REFERENCES

APPENDICES