Hashing Techniques for Mobile Device Forensics

Shira Danker Rick Ayers Richard P. Mislan

Abstract- Previous research conducted at the National Institute of Standards and Technology has shown that mobile device internal memory hash values are variable when performing back-to-back acquisitions. Hash values are beneficial in providing examiners with the ability to filter known data files, match data objects across platforms and prove that data integrity remains intact. The research conducted at Purdue University compared known hash values with reported values for data objects populated onto mobile devices using various data transmission methods. While the results for the majority of tests were uniform, the hash values reported for data objects transferred via Multimedia Messaging Service (MMS) were variable.

***Index Terms* - Cell Phone Forensics, Mobile Device Forensics, Hashing, MMS, MD5.**

I. INTRODUCTION

With the increasing popularity and technological advances of mobile devices, new challenges arise for forensic examiners and toolmakers [2]. Data recovered from mobile devices has proven useful in solving incidents and investigating criminal activity [3]. Cryptographic hash functions provide forensic examiners with the ability to verify the integrity of acquired data. The resulting hash value, a fixed-size bit string, is often used to identify known files and illustrates that data has not been modified. The two most commonly used hash functions are MD5 and SHA-1 [4].

Minimal research has been performed on how mobile phone forensic tools report hash values for individual data objects. Recent research conducted at Purdue University explored the hash results reported by mobile device forensic tools for acquired graphical images (e.g., .jpg, .bmp, .gif). While research conducted shows consistent behavior across mobile forensic tools, the following area of concern illustrates the need for future research: data objects transferred using Multimedia Messaging Service (MMS).

This paper addresses issues surrounding mobile forensic tools and the ability to use hashing mechanisms to validate the integrity of acquired data objects. The document is divided into the following chapters and appendix:

- *Terminology*: Defines terms used throughout the document.
- *Previous Research*: Provides a summary of earlier research performed in this area.
- *Methodology*: Describes the procedures used for conducting individual tests.
- *Results*: Illustrates the final results of tests conducted over each prescribed scenario.
- *Conclusions*: Provides a summary of the document, test results and future research.
- *Appendix A*: Illustrates individual calculated hash values for individual data objects produced by the forensic workstation and the mobile forensic tools.

II. TERMINOLOGY

- *Data Transfer Methods*: Communication channels (e.g., Bluetooth, Multimedia Messaging Service, etc.) that provide a conduit to populate the internal memory of mobile devices.
- *Secure Hash*: A mathematical algorithm that takes an arbitrary block of data and returns a fixed-size bit string, the hash value, such that any change to the data will modify the hash value.
- *Mobile Device Data Objects*: Individual files (e.g., .jpg, .bmp, .gif, etc.) residing in the internal memory of the mobile device.
- *Mobile Device Forensic Tool*: Acquisition tools designed to perform a logical acquisition from the internal memory of mobile devices.
- *Personal Computer Forensic Tool*: Forensic tools designed to acquire data from hard drives (e.g., IDE, SATA, SCSI, etc.)

III. PREVIOUS RESEARCH

Previous research on mobile device forensic tool hash generation has been minimal. Ayers, Jansen, Moenner, and Delaitre [5] performed a series of tests using multiple mobile forensic tools in an update to their pervious publication regarding an overview of forensic software tools for mobile devices. Two tests related to hashing were conducted: one to determine if mobile forensic applications reported consistent overall case file hashes when performing back-to-back acquisitions, and the other to validate the reported hash values of individual files (i.e., data objects) from subsequent acquisitions. While their research showed that the overall case file hashes were inconsistent, the majority of tools reported consistent hash values for individual data objects.

Sobieraj and Mislan [6] researched the metadata stored for graphical images captured by camera phones. Images contain metadata known as ***Exif*** information (e.g., camera model, time/date stamp, etc.) Their research showed that date and time information is variable and cannot be counted on during an investigation [6]. Therefore, additional metadata attributes may be useful in determining the source of a picture. If metadata tied to graphical data was consistent across camera phones, the ***Exif*** information might be useful in addition to hashing.

IV. METHODOLOGY

Initial preparation begun by calculating MD5 hashes for individual data files listed below in Table 1. Each individual graphic file was downloaded to a forensic workstation and hashed using Access Data's Forensic Toolkit to calculate MD5. The tool was chosen based on availability. The hash values reported for acquired data objects by the mobile device forensic tools were compared to the known start value.

The mobile devices were selected solely on their availability and similar feature set (e.g., MMS, Bluetooth, internal camera). Eight pairs of duplicate (i.e., make, model, firmware) mobile devices were selected. By using duplicate mobile devices one is able to determine if mobile device forensic tools report consistent hash values for pre-defined data objects across shared mobile devices. Two mobile device forensic tools: Paraben's Device Seizure [7] and Susteen's Secure View [8] were selected due to availability, embedded hashing functionality, and acquisition support for the selected mobile devices.

There are numerous ways to transfer data onto a mobile device. Multiple tests were performed to determine if hash values remain consistent across various data transmission methods. The following data transmission methods were used: universal memory exchanger, MMS, Bluetooth, and MicroSD. Additional orientation tests were conducted to determine if reported hash values were modified when a) altering the role of a stored graphic file (i.e., saving as wallpaper) and b) transferring the snapshot taken from the mobile device's internal camera onto the forensic workstation.

The research involved several objectives, which were: a) to determine if discrepancies appeared between known hash values, b) to document that reported hash values remained consistent and finally, c) to document found anomalies. The following subsections outline each individual test.

A. Graphic File Format Tests

The graphic file format tests required populating the target mobile device with graphic files (i.e., .jpg, .bmp, .gif) from a pre-defined dataset using the Cellebrite UME-36 [9] universal memory exchanger. The Cellebrite UME-36 was selected solely on availability and its data transmission scheme. The Cellebrite UME-36 unit is a stand-alone phone memory transfer and backup solution.

B. MMS Tests

MMS tests required mobile devices capable of sending and receiving MMS messages. MMS is used to send a graphic file to target mobile devices. Once the MMS message was successfully received on the target mobile device, the graphic file was saved to the target mobile device internal memory.

C. Bluetooth Tests

Bluetooth tests required Bluetooth enabled mobile devices. A forensic workstation was used to send a graphic file using Bluetooth to all target mobile devices.

D. MicroSD Card Tests

The following techniques were used for the MicroSD card tests based upon the capabilities of the mobile device forensic tools and mobile devices. Mobile devices not supporting MicroSD required a graphic file to be saved on a flash drive and then pushed to the internal memory of the mobile device using Cellebrite UME-36. For mobile devices that supported MicroSD and were acquired using Secure View, the graphic file was copied to the internal memory of the mobile device from the MicroSD card. Acquisition performed by Device Seizure allowed a graphic file to be acquired directly from the MicroSD memory card.

E. Wallpaper Tests

The wallpaper tests required populating the target mobile device with a .jpg graphic file from a pre-defined dataset using the Cellebrite UME-36. Once the graphic file was successfully saved to the mobile device internal memory, the file was manually reassigned as wallpaper.

F. Camera Phone Tests

Camera phone tests required mobile devices containing an internal camera. Graphic files taken with the internal camera phone were transferred to a forensic workstation and mobile devices using the Cellebrite UME-36.

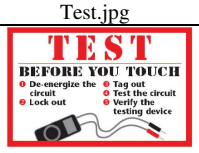
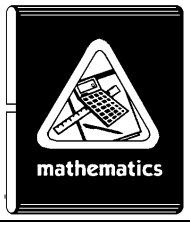
Test.jpg	Bluetooth.jpg	Card.jpg
		
3c3111ded5df821d668aecf9b598100b	6c8a1401a3af8264504f16334e774b5c	77bebd7fb998797dd5768c99fdbda8f6
Mathematics.bmp	Stress-test.gif	Mail.jpg
		
7d3b824769389beadb69b536a0295662	9b902382728b6bbdc65009a5d1084041	d57fac85a5be5a780405a0484254256b

Table 1: Pre-define Data Set (Graphic Files) – MD5Sum

V. RESULTS

The following section summarizes the final results and provides additional information on each test scenario conducted. Due to the mobile device graphic file format limitations, the test results for some devices may not contain a hash entry for a particular test. The subsequent tables illustrate final test results.

A. Graphic File Format Test Results

Device Seizure and Secure View reported consistent hash values with the forensic workstation.

B. MMS Test Results

MMS hash values for transmitted graphic files were found to be inconsistent within different mobile device families. This generated a second round of testing to verify the findings of hash inconsistencies were related to different mobile device MMS format implementations.

C. Round 2 - MMS Test Results

The second round of tests confirmed that a) inconsistent reported hash values occurred across both alike and different mobile device families and b) resending saved graphic files sent using MMS may result in different hash values as illustrated in Table 6.

D. Bluetooth Test Results

Device Seizure and Secure View reported consistent hash values with the forensic workstation.

E. MicroSD Card Test Results

Device Seizure and Secure View reported consistent hash values with the forensic workstation.

F. Wallpaper Test Results

The mobile device forensic tools generated consistent hashes for all tested mobile devices. Hash values generated by the forensic workstation matched the mobile device forensic tools' reported hash values.

G. Camera Phone Test Results

Device Seizure and Secure View reported consistent hash values with the forensic workstation.

VI. CONCLUSION

The objective of the tests conducted at Purdue University was to determine if reported hash values for graphic files remain consistent between mobile device forensic tools and a forensic workstation. The majority of tests conducted (i.e., graphic file format tests, Bluetooth tests, MicroSD card tests, wallpaper tests, camera phone tests) have shown that the reported hash values remain consistent. Although, inconsistencies occur when mobile device graphic files are transferred using MMS.

With over 2 billion mobile phones in use today, mobile device forensics continues to be a concentrated area of interest among the forensic community [10]. As mobile devices evolve, the storage capacity and richness of data objects increase. From an investigative perspective, the data acquired from mobile devices is often times beneficial in providing leads or solving a case. Therefore, researching the behavior and reliability of mobile device forensic tools is advantageous for toolmakers and the forensic community.

While minimal research has been conducted on the hash values calculated for mobile device data objects, future research exploring the effects of additional data objects (e.g., audio, documents, video) commonly found on mobile devices is paramount.

ACKNOWLEDGEMENTS

The authors, Shira Danker, Rick Ayers and Richard P. Mislan, thank Barbara Guttman and Craig Russell from NIST and Sam Brothers from U.S. Customs and Border Protection for reviewing drafts, technical support and contributions to this document.

Certain commercial entities, equipment, or materials may be identified in this document in order to describe an experimental procedure or concept adequately. Such identification is not intended to imply recommendation or endorsement by the National Institute of Standards and Technology, nor is it intended to imply that the entities, materials, or equipment are necessarily the best available for the purpose.

REFERENCES

[1] Mead, S., (2006). Viability of MD5 and SHA-1 for forensic hashing. Retrieved from http://www.techsec.com/TF-2006-PDF/TF-2006-SteveMead-Viability_of_MD5_SHA1_(NSRLv17)-v4.pdf.

[2] Al Zarouni, M. (2006). Mobile handset forensic evidence: a challenge for law enforcement. Proceedings from the 4th Australian Digital Forensics Conference. Perth, Western Australia, 4 December 2006, pp 1 -10. Edith Cowan University

[3] Shachtman, N. (2006). Fighting crime with cellphones' clues. Retrieved from http://www.nytimes.com/2006/05/03/technology/techspecial3/03cops.html

[4] AccessData (2006). MD5 Collisions: The effect on computer forensics. Retrieved from http://www.accessdata.com/media/en_US/print/papers/wp.MD5_Collisons.en_us.pdf

[5] Ayers, R., Jansen, W., Moenner, L., & Delaitre, A. (2007). Cell phone forensic tools: An overview and analysis update. Retrieved from http://csrc.nist.gov/publications/nistir/nistir-7387.pdf

[6] Sobieraj, S., & Mislan, R. (2007) Mobile phones: Digital photo metadata. Retrieved from http://www.cerias.purdue.edu/symposium/2007/materials/pdfs/E26-CF9.pdf

[7] Paraben Forensics. (2007). Device Seizure v1.3> Retrieved from http://www.paraben-forensics.com/catalog/product_info.php?cPath=25&products_id=405

[8] Secure View. (2009). Secure View Kit for Forensics> Retrieved from http://www.datapilot.com/productdetail/253/producthl/Notempty

[9] Cellebrite. (2008). Retrieved from http://www.cellebrite.com

[10] Murph, Darren. (2007). Mobile phone subscriptions hit 3.3 billion. Retrieved January 12, 2007 from http://www.engadget.com/2007/11/29/mobile-phone-subscriptions-hit-3-3-billion.html>

APPENDIX A

Table 2 – Image Format Test - JPEG Results (Test.jpg)

Computer Hash Value	*Motorola Phones*	Hash Value – *Secure View*	Hash Value – *Device Seizure*
3c3111ded5df821d668aecf9b598100b	Motorola RAZR V3m ID:1347	3c3111ded5df821d668aecf9b598100b	3c3111ded5df821d668aecf9b598100b
3c3111ded5df821d668aecf9b598100b	Motorola RAZR V3m ID:1556	3c3111ded5df821d668aecf9b598100b	3c3111ded5df821d668aecf9b598100b
	LG Phones		
3c3111ded5df821d668aecf9b598100b	LG VX8550 chocolate ID:5297	3c3111ded5df821d668aecf9b598100b	N/A
3c3111ded5df821d668aecf9b598100b	LG VX8550 chocolate ID:7361	3c3111ded5df821d668aecf9b598100b	N/A
3c3111ded5df821d668aecf9b598100b	LG VX8350 ID:7938	3c3111ded5df821d668aecf9b598100b	N/A
3c3111ded5df821d668aecf9b598100b	LG VX8350 ID:7939	3c3111ded5df821d668aecf9b598100b	N/A
	Samsung Phones		
3c3111ded5df821d668aecf9b598100b	Samsung SCH-U540 ID:8448	3c3111ded5df821d668aecf9b598100b	N/A
3c3111ded5df821d668aecf9b598100b	Samsung SCH-U540 ID:8204	3c3111ded5df821d668aecf9b598100b	N/A

Table 3 – Image Format Test - BMP Results (Mathematics.bmp)

Computer Hash Value	*Motorola Phones*	Hash Value – *Secure View*	Hash Value – *Device Seizure*
7d3b824769389beadb69b536a0295662	Motorola RAZR V3m ID:1347	7d3b824769389beadb69b536a0295662	7d3b824769389beadb69b536a0295662
7d3b824769389beadb69b536a0295662	Motorola RAZR V3m ID:1556	7d3b824769389beadb69b536a0295662	7d3b824769389beadb69b536a0295662
	LG Phones		
7d3b824769389beadb69b536a0295662	LG VX8550 chocolate ID:5297	7d3b824769389beadb69b536a0295662	N/A
7d3b824769389beadb69b536a0295662	LG VX8550 chocolate ID:7361	7d3b824769389beadb69b536a0295662	N/A

Table 4 – Image Format Test - GIF Results (Stress-test.gif)

Computer Hash Value	*Motorola Phones*	Hash Value – *Secure View*	Hash Value – *Device Seizure*
9b902382728b6bbdc65009a5d1084041	Motorola RAZR V3m ID:1347	9b902382728b6bbdc65009a5d1084041	9b902382728b6bbdc65009a5d1084041
9b902382728b6bbdc65009a5d1084041	Motorola RAZR V3m ID:1556	9b902382728b6bbdc65009a5d1084041	9b902382728b6bbdc65009a5d1084041
	LG Phones		
9b902382728b6bbdc65009a5d1084041	LG VX8550 chocolate ID:5297	9b902382728b6bbdc65009a5d1084041	N/A
9b902382728b6bbdc65009a5d1084041	LG VX8550 chocolate ID:7361	9b902382728b6bbdc65009a5d1084041	N/A

Table 5 - MMS Test (Test.jpg)

Computer Hash Value	*Motorola Phones*	Hash Value – *Secure View*	Hash Value – *Device Seizure*
N/A	Motorola RAZR V3m ID:1347	3c3111ded5df821d668aecf9b598100b	3c3111ded5df821d668aecf9b598100b
N/A	Motorola RAZR V3m ID:1556	3c3111ded5df821d668aecf9b598100b	3c3111ded5df821d668aecf9b598100b
	LG Phones		
N/A	LG VX8550 chocolate	459c85d0fb234482142787c91dfca003	N/A

	ID:5297		
N/A	LG VX8550 chocolate ID:7361	459c85d0fb234482142787c91dfca003	N/A
N/A	LG VX8350 ID:7938	3c3111ded5df821d668aecf9b598100b	N/A
N/A	LG VX8350 ID:7939	3c3111ded5df821d668aecf9b598100b	N/A
	Samsung Phones		
N/A	Samsung SCH-U540 ID:8448	459c85d0fb234482142787c91dfca003	N/A

Table 6 - MMS 2nd Round (Mail.jpg)

Computer Hash Value	***Motorola Phones***	**Hash Value – *Secure View***
N/A	Motorola RAZR V3m ID:1347	d57fac85a5be5a780405a0484254256b
N/A	Motorola Motorola RAZR V3m ID:1556	d57fac85a5be5a780405a0484254256b
N/A	Motorola RAZR V3m ID:1347	821718317819a169dcf01ef49eaf0d5c
N/A	Motorola RAZR V3m ID:1556	d57fac85a5be5a780405a0484254256b
	LG Phones	
N/A	LG VX8550 chocolate ID:5297	a2712817b8fce9b925e8a710e979e1b9
N/A	LG VX8550 chocolate ID:7361	a2712817b8fce9b925e8a710e979e1b9

Table 7 - Bluetooth Tests (Bluetooth.jpg)

Computer Hash Value	***Motorola Phones***	**Hash Value – *Secure View***	**Hash Value – *Device Seizure***
6c8a1401a3af8264504f16334e774b5c	Motorola RAZR V3m ID:1347	6c8a1401a3af8264504f16334e774b5c	6c8a1401a3af8264504f16334e774b5c
6c8a1401a3af8264504f16334e774b5c	Motorola RAZR V3m ID:1556	6c8a1401a3af8264504f16334e774b5c	6c8a1401a3af8264504f16334e774b5c
	LG Phones		
6c8a1401a3af8264504f16334e774b5c	LG VX8550 chocolate ID:5297	6c8a1401a3af8264504f16334e774b5c	N/A
6c8a1401a3af8264504f16334e774b5c	LG VX8550 chocolate ID:7361	6c8a1401a3af8264504f16334e774b5c	N/A
6c8a1401a3af8264504f16334e774b5c	LG VX8350 ID:7938	6c8a1401a3af8264504f16334e774b5c	N/A
6c8a1401a3af8264504f16334e774b5c	LG VX8350 ID:7939	6c8a1401a3af8264504f16334e774b5c	N/A

Table 8 - MicroSD Card Tests (SD card.jpg)

Computer Hash Value	***Motorola Phones***	**Hash Value – *Secure View***	**Hash Value – *Device Seizure***
77bebd7fb998797dd5768c99fdbda8f6	Motorola RAZR V3m ID:1347	77bebd7fb998797dd5768c99fdbda8f6	77bebd7fb998797dd5768c99fdbda8f6
77bebd7fb998797dd5768c99fdbda8f6	Motorola RAZR V3m ID:1556	77bebd7fb998797dd5768c99fdbda8f6	77bebd7fb998797dd5768c99fdbda8f6
	LG Phones		
77bebd7fb998797dd5768c99fdbda8f6	LG VX8550 chocolate ID:5297	77bebd7fb998797dd5768c99fdbda8f6	N/A
77bebd7fb998797dd5768c99fdbda8f6	LG VX8550 chocolate ID:7361	77bebd7fb998797dd5768c99fdbda8f6	N/A
77bebd7fb998797dd5768c99fdbda8f6	LG VX8350	77bebd7fb998797dd5768c99fdbda8f6	N/A

	ID:7938		
77bebd7fb998797dd5768c99fdbda8f6	LG VX8350 ID:7939	77bebd7fb998797dd5768c99fdbda8f6	N/A
	Samsung Phones		
77bebd7fb998797dd5768c99fdbda8f6	Samsung SCH-U540 ID:8448	77bebd7fb998797dd5768c99fdbda8f6	N/A
77bebd7fb998797dd5768c99fdbda8f6	Samsung SCH-U540 ID:8204	77bebd7fb998797dd5768c99fdbda8f6	N/A

Table 9 - Wallpaper Tests (Test.jpg)

Computer Hash Value	***Motorola Phones***	**Hash Value – *Secure View***
3c3111ded5df821d668aecf9b598100b	Motorola RAZR V3m ID:1347	3c3111ded5df821d668aecf9b598100b
3c3111ded5df821d668aecf9b598100b	Motorola RAZR V3m ID:1556	3c3111ded5df821d668aecf9b598100b
	LG Phones	
3c3111ded5df821d668aecf9b598100b	LG VX8550 chocolate ID:5297	3c3111ded5df821d668aecf9b598100b
3c3111ded5df821d668aecf9b598100b	LG VX8550 chocolate ID:7361	3c3111ded5df821d668aecf9b598100b
3c3111ded5df821d668aecf9b598100b	LG VX8350 ID:7938	3c3111ded5df821d668aecf9b598100b
3c3111ded5df821d668aecf9b598100b	LG VX8350 ID:7939	3c3111ded5df821d668aecf9b598100b
	Samsung Phones	
3c3111ded5df821d668aecf9b598100b	Samsung SCH-U540 ID:8448	3c3111ded5df821d668aecf9b598100b
3c3111ded5df821d668aecf9b598100b	Samsung SCH-U540 ID:8204	3c3111ded5df821d668aecf9b598100b

Table 10 - Camera Phone Pictures

Computer Hash Value	***Motorola Phones***	**Hash Value – *Secure View***	**Hash Value – *Device Seizure***
2214247fec280890e04d6e923e88dc90	Motorola RAZR V3m ID:1347	2214247fec280890e04d6e923e88dc90	2214247fec280890e04d6e923e88dc90
2214247fec280890e04d6e923e88dc90	Motorola RAZR V3m ID:1556	2214247fec280890e04d6e923e88dc90	2214247fec280890e04d6e923e88dc90
	LG Phones		
2214247fec280890e04d6e923e88dc90	LG VX8550 chocolate ID:5297	2214247fec280890e04d6e923e88dc90	N/A
2214247fec280890e04d6e923e88dc90	LG VX8550 chocolate ID:7361	2214247fec280890e04d6e923e88dc90	N/A
2214247fec280890e04d6e923e88dc90	LG VX8350 7938	2214247fec280890e04d6e923e88dc90	N/A
2214247fec280890e04d6e923e88dc90	LG VX8350 7939	2214247fec280890e04d6e923e88dc90	N/A
	Samsung Phones		
2214247fec280890e04d6e923e88dc90	Samsung SCH-U540 ID:8448	2214247fec280890e04d6e923e88dc90	N/A
2214247fec280890e04d6e923e88dc90	Samsung SCH-U540 ID:8204	2214247fec280890e04d6e923e88dc90	N/A