

A decorative graphic consisting of a thin yellow circle on the left side. A thick black bracket is positioned on the left side of the circle, and a thick yellow bracket is on the right side. A horizontal bar with a light olive green gradient is placed across the middle of the circle, containing the title text.

# Viability of Using Hash Values in Mobile Phone Forensics

Shira Dankner

# [ Mobile Phones ]

---

- Users overtaking computer users
  - 3.3 Billion cell phone subscribers
  - Internet users expected to surpass 2 Billion by 2011
- Large amount of evidence
  - Call logs, contact lists, SMS, Images
- Flexible data entry
  - Updated “on the go”

# [ Evidence Integrity ]

- ACPO
  - “**Principle 1:** No action taken by law enforcement agencies or their agents should change data held on a computer or storage media which may subsequently be relied upon in court.”
- Write Blocker
  - Imaging Process
    - Integrated in some mobile forensic tools
- Mobile Phones
  - Not feasible
  - Minimization Techniques
    - Generating hash values

# [ Forensic Hashing ]

---

- MD5, SHA, Checksum
  - MD5 most common
  - Cracked
- No impact on forensic world. Yet.
- Used to verify integrity of images and files
- Used to match distinct files
  - NIST databases

# Mobile Phones - Proprietary Systems

- Hardware
  - Each phone has different specifications
  - Cables
- Operating System
  - Proprietary
- Forensic Software
  - Black Box
    - USB Monitor

# Mobile Phones - Operating System

- Proprietary to manufacturer
- Retrieves evidence for examiner
  - Client/Server
- Black Box
  - Does it alter the evidence recovered?
  - SMS Flag changed
- Volatile data issues
  - Date/Time

# [ Hashing and Mobile Phones ]

---

- Hash Values of Individual Files
  - Supposed to match
- Hash Value of File System
  - Different each acquisition
- Does the handling of evidence alter it?

# [ Current Situation ]

---

- Mobiles phones contain evidence
- Relying on software/phone OS for retrieval
  - OS alters memory contents
- Unknown effect on evidence
- Use hashing to verify integrity of recovered evidence
  - What if it the hash values retrieved are unreliable?

# [ Research Questions ]

---

- Does the OS of a mobile phone manipulate data so that the generated hash values are irrelevant
- Different variables were tested to determine if they affect the final hash value
  - Does transferring an image to a phone from another device alter the hash value?
  - Which transfer methods have an effect on the hash value of an image?
  - Does using the image as either the wallpaper or an icon on the phone affect the hash value?
  - Do file hash values of image files or phonebooks recovered from mobile phones work to create a hash list of the data recovered?

# [ Prior Research ]

---

- Mobile phone forensic tools: An overview and analysis update
  - Found that CellDek and Device Seizure generated hash values for individual files/file system
    - Individual files were consistent
    - File system changed
      - Didn't test other variables
  - Ayers, Jansen, Moenner, Delatire (2007)

# [ Prior Research ]

---

- Forensic analysis of the contents of Nokia mobile phones
  - Series of phones returned the same hash values for files/entire file systems
  - Cell Seizure generated four different hash values, none matched the final report
- Williamson, ApelDorn, Cheam, McDonald (2006)

# [ Methodology ]

---

- Delimitations
  - 8 phones
  - 3 different mobile phone forensic programs
    - Paraben's Device Seizure 2.0 2988.32073
    - Data Pilot's SecureView 1.5.0
    - BitPim 1.05
  - 3 Image formats
    - JPEG, GIF, BMP
- Limitations
  - Selection of mobile phones limited to ITAP contracts/Purdue Cyber Forensics Lab

# [ Phones and Firmware ]

---

- Motorola RAZR V3M
  - SW 24.1\_01.19.07
- LG VX8350
  - HW 1.1
- LG VX8550
  - HW 1.0 LK
- Samsung SCH-U540
  - 8.01/7.012 540v

# [ Variables Tested ]

---

- Manufacturer
- Model
- Image Format
- Utilizing the Image
- Transfer Method
  - Cellebrite UME-36
  - Bluetooth
  - Text Message
  - Storage Card
- Source
  - Desktop (Cellebrite)
  - Camera Phone
  - Manual Input
- Forensic Software
  - Paraben's Device Seizure
  - Data Pilot's Secure View
  - BitPim

# [ Research Questions 1 and 2 ]

**Does transferring an image to a phone from another device alter the hash value?**

**Which transfer methods have an effect on the hash value of an image?**

# [ Image Format Test ]

---

- Cellebrite was used to populate the phones with the pictures
  - Some phones could only handle certain image formats
- Phones acquired via Secure View
  - Motorola phones re-acquired via Device Seizure.

# [ Bluetooth Test ]

---

- Bluetooth.jpg was downloaded from Google images and saved on the forensic desktop
- Bluetooth was enabled on the desktop via the My Bluetooth Places menus
- The phones were put into discover mode and paired with the desktop
- From this point the file system on the phones could be opened via the File System function of the Bluetooth stack
  - The image was copied to the phones in this manner
  - The Motorola RAZR v3m phones required some edits to enable the correct bluetooth function
  - Bluetooth could not be enabled on the Samsung phones
- They were then acquired via Secure View
- The Motorola phones were acquired via Device Seizure as well

# [ MMS Test – First Series ]

---

- The pictures were erased from all of the phones except one of the LG 8550s.
  - Test.jpg was removed as wallpaper on the 8550 and sent to all the phones via SMS.
  - After all of the SMS messages were sent, the source 8550 was acquired for the original hash value of the test.jpg image
  - Test.jpg was deleted from the source 8550 and sent back to it from one of the Motorola RAZR v3m phones
  - Before it was sent to the 8550, the hash value was verified as being the same as the original.
  - Both Motorola phones were also acquired via Device Seizure.

# [ Camera Phone Test ]

---

- One of the LG 8550s was used to take a picture and then it was backed up via the Cellebrite.
- All other pictures on the remaining phones were erased, and the picture from the LG 8550 was then transferred to the them.
- All of the phones were acquired via Secure View
- The Motorola phones were acquired via Device Seizure.

# [ MicroSD Card Test ]

---

- Card.jpg was pushed to a phone via the Cellebrite, since that method hadn't altered the hash value in previous tests.
- The picture was moved to an LG 8550 and then saved to the microSD card. The phone was then acquired via Secure View.
- The Motorola phones required the image to be moved from the card on to the phone explicitly before Secure View could see the image.
- Device Seizure didn't have this issue and could recover all information on the microSD card without it being moved to the phone's memory.

# [ Research Question 3 ]

---

**Does using the image as either the wallpaper or an icon on the phone affect the hash value?**

# [ Wallpaper Test ]

---

- Tested whether or not setting a picture as wallpaper would change the hash value.
- All pictures except for the JPEG from the previous test were deleted from the phone
- Image was set as the main wallpaper on the phone
- The phones were then powered off and back on, and then reacquired.

# [ Research Question 4 ]

---

**Do file hash values of image files or phonebooks recovered from mobile phones work to create a hash list of the data recovered?**

# [ Contact Entry Test ]

- One contact with the following details was entered into the LG 8550, 8530 and Motorola RAZR v3m series phones.
  - Contact Name: John Smith
  - Contact Number: 765-555-5555
  - Contact Email Address: jsmith@t.com
  
- The phones were then acquired with BitPim and Device Seizure
- While BitPim doesn't calculate an MD5 hash value on its own, it can be calculated using FTK Imager.
- Device Seizure calculates the hash value on its own, so a report was generated that included the entire file structure and the hash values associated with the files.

# [ Results ]

---

- Using a Cellebrite system to copy images from a thumb drive to a phone has no effect on the hash value
  - Important to note due to it's use in subsequent tests
- Most of the tests showed no change to the hash value
- Sending an image via MMS showed different hash values, even between the same make and model of phone
- Identical contact information resulted in different hash values

[ Further Testing ]

---

**Additional Tests to Expand on Earlier Results**

# Camera Phone Test – BitPim Verification

- BitPim was also used to verify that another application didn't affect the final hash value.
- The picture taken in the camera tests was reacquired on both an LG 8550, and LG 8350 via BitPim

# [ MMS Test – Second Series ]

- Mail.jpg was transferred to the Motorola RAZR V3m device via Bluetooth, as the Cellebrite was not accessible at the time of this test.
  - The image was then verified for hash consistency.
- Mail.jpg was then sent to the LG VX8550s and the other Motorola RAZR V3m
  - The image was saved from the MMS message to the mobile phone's internal memory.
- The devices were acquired via Secure View.
- Mail.jpg was deleted from the original source Motorola RAZR V3m
- The other Motorola RAZR V3m was used to send mail.jpg to the original source Motorola RAZR V3m
  - Both phones were then reacquired via Secure View

# [ In Depth – MMS Tests ]

---

- LG VX8550s and Samsung SCH-U540 generated different hash values from the rest of the phones in the first series of tests
- The LG VX8550s and the Motorola RAZR V3m generated different hash values in the second series of tests
- The file size changed along with the hash value

# MMS First Series of Tests

Phone	Hash Value	Size
LG VX8550 Source 1st Series	3c3111ded5df821d6 68aecf9b598100b	26,823 bytes
LG VX8550 Recipient 1st Series	459c85d0fb2344821 42787c91dfca003	34,028 bytes
SCH-U540	459c85d0fb2344821 42787c91dfca003	34,028 bytes
Motorola RAZR V3m	3c3111ded5df821d6 68aecf9b598100b	26,823 bytes

# MMS Second Series of Tests

Phone	Hash Value	Size
Motorola RAZR V3m Source 2nd Series	d57fac85a5be5a780 405a0484254256b	5,926 bytes
Motorola RAZR V3m Recipient 2nd Series	821718317819a169 dcf01ef49eaf0d5c	4,793 bytes
LG VX8550	a2712817b8fce9b92 5e8a710e979e1b9	8,605 bytes

# [ In Depth – Contact Entries ]

- Motorola RAZR V3m, LG VX8350, VX8550
- Identical PIM file structure per manufacturer
- LG Phones
  - Empty files generate the same hash value
  - Pbentry.dat file adds additional characters to each contact entry, thus resulting in different hash values



# [ Conclusions ]

---

- Hash values generated from recovered items from cell phones cannot be relied upon
- Though most of the tests resulted in no change to the hash value, it would be up to the investigator to say for certain how the image arrived at the phone
  - If via MMS, the hash could potentially have changed
- The “essence” of the data is the same, but results in a different hash value

# Importance to Forensic Community

---

- Community has told courts that hash values should match
  - Hash values cannot be relied upon in this instance
- Standards for using hash values need to be changed
- Forensic community must be informed and kept up to date

# [ Alternatives to Hashing ]

---

- Using other information to verify the integrity of recovered evidence
  - EXIF
- Requires some standards across all mobile phone manufacturers
  - Feature Set Recognition
  - Image Source Identification

# [ Future Research ]

---

- Explore the explanation behind the hash value changes
- Document other inconsistencies that exist when dealing with hash values
- Need for prior documentation and standardization for courts