

NAND/NOR Chip Forensics

Cyber Security Division 2012 Principal Investigators' Meeting

10/10/2012

David Weinstein
Senior Security Engineer
viaForensics
dweinstein@viaforensics.com
T: +1 312-878-1100, M: 202-579-9267

viaForensics Overview

Digital security and forensics, focus on mobile

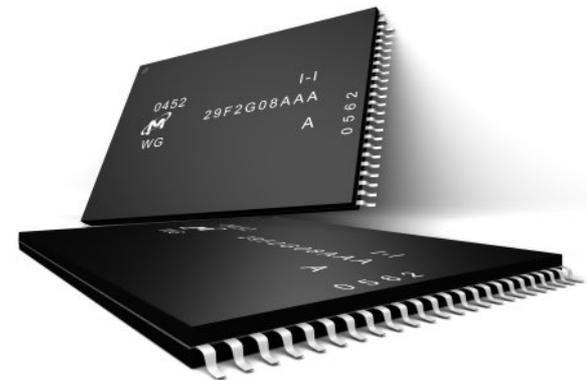
- viaExtract™ forensic software
- liveForensicsSM continuous monitoring
- Advanced forensics training and services
- appSecureSM mobile security audits
- Santoku Linux distro for mobile security and forensics analysis

Challenges

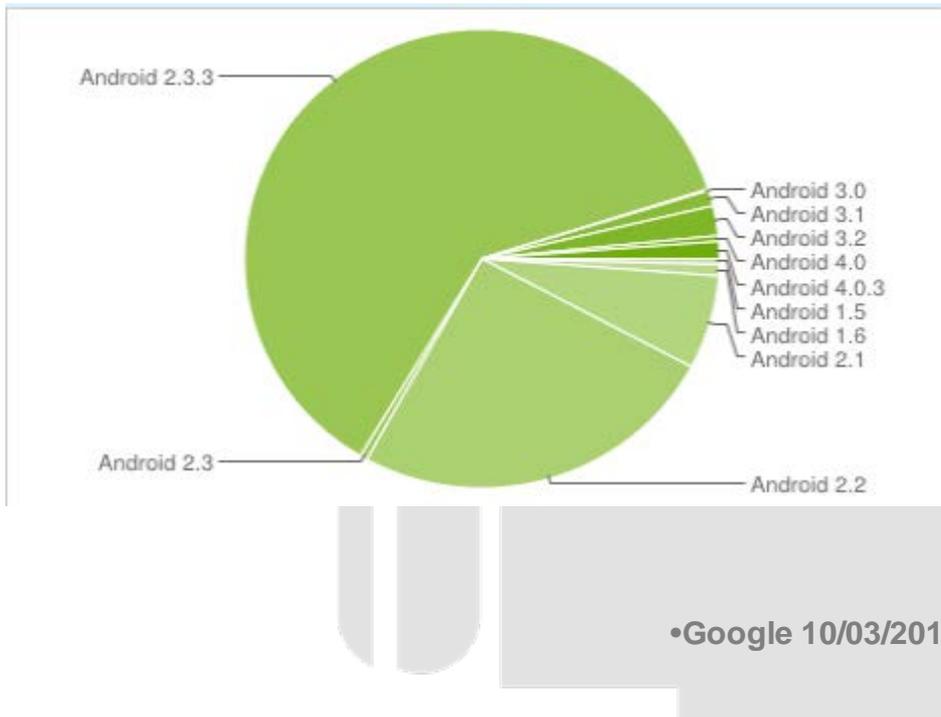
- 
- Significant data on mobile devices, hard to gain access
 - Screen locks, passwords, encryption
 - Authentication (admissibility) of forensic images
 - Meaningful reporting on diverse data sets

NAND Flash Memory

- High potential for data recovery, but difficult to image
- No tool to create forensically sound image (admissibility)
 - We created on-the-fly hashing for image verification
- Once data acquired, must reverse engineer and then analyze



Android Fragmentation



Platform	Codename	API Level	Distribution
Android 1.5	Cupcake	3	0.4%
Android 1.6	Donut	4	0.8%
Android 2.1	Eclair	7	6.6%
Android 2.2	Froyo	8	25.3%
Android 2.3 - Android 2.3.2	Gingerbread	9	0.5%
Android 2.3.3 - Android 2.3.7		10	61.5%
Android 3.0	Honeycomb	11	0.1%
Android 3.1		12	1.1%
Android 3.2		13	2.1%
Android 4.0 - Android 4.0.2	Ice Cream Sandwich	14	0.4%
Android 4.0.3		15	1.2%

ANDROID FRAGMENTATION

- More than 11 versions in commercial space
- Different boot loaders per handset manufacturer + device
- Rooting and custom ROMs widespread

Solutions

Phase I

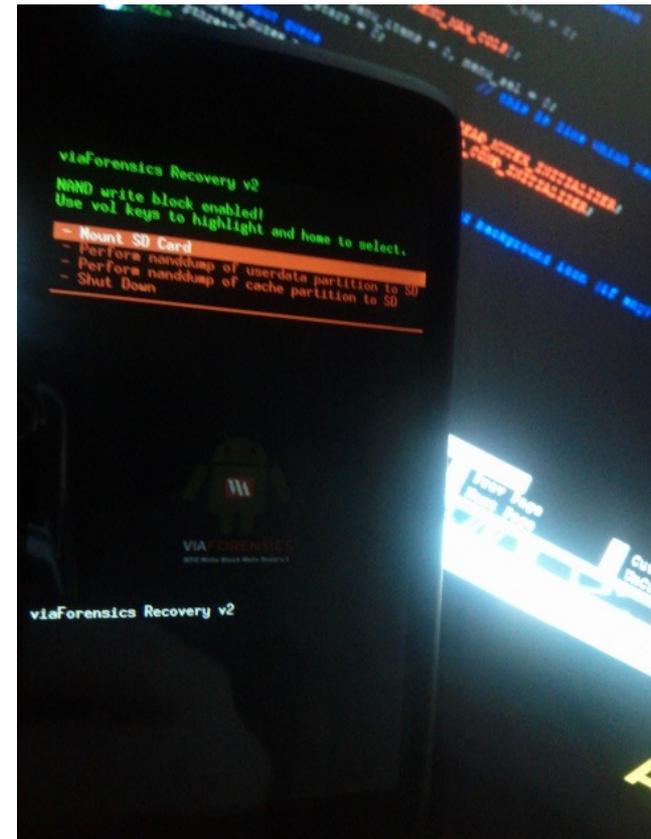
- Develop forensically sound flash write-blocker
- On-the-fly hashing of NAND dumps
- Temporary rooting of devices

Phase II

- Incorporate into viaExtract product
- Support additional devices (iOS, Windows)
- Catalogue techniques
- Mobile forensics training
- Push-button forensics

Forensic Boot Image

- Start early in the boot chain before the system loads
- Provide ADB root shell over USB which can be used to image the device
- Do not mount anything, including cache, to prevent any writes to partitions
- Devices with raw NAND flash and wear leveling implemented in software (YAFFS2) can be prevented from overwriting deleted data



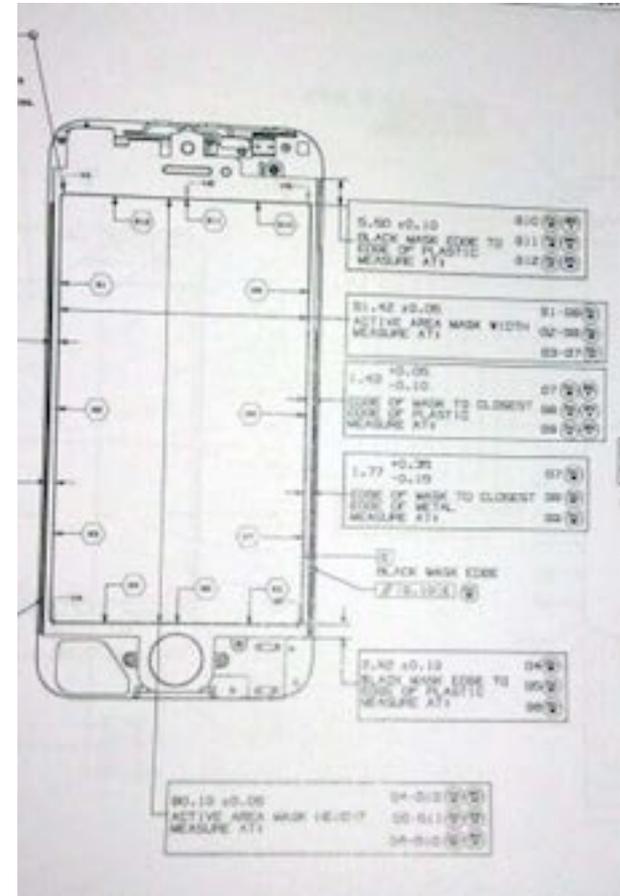
Cracking Encryption

- Parse footer
- Locate Salt and Encrypted Master Key
- Run a password guess through PBKDF2 with salt, use resulting key and IV to decrypt master key, use resulting master key to decrypt first sector of encrypted image.
- If password is correct, plain text will be revealed

```
Magic : 0xD0B5B1C4
Major Version : 1
Minor Version : 0
Footer Size : 104 bytes
Flags : 0x00000000
Key Size : 128 bits
Failed Decrypts: 0
Crypto Type : aes-cbc-essiv:sha256
Encrypted Key : 0x82AF933B1AF0968D835239CE69526C60
Salt : 0x31D720E6F7F78A23D793E125378E5F49
-----
Trying Password: 1234
Derived Key : 0x38E6A59647776E94AD09C1DACA7B4971
Derived IV : 0xB3F8D260076D92A1CFAE7D807DC1613C
Decrypted Key : 0x0552393822D311BE023617F258C3E1BB
```


Support More Devices

- Increase number of supported Android devices
- Add support for iOS logical and physical acquisitions
- Add support for Windows Phone, provided they can reverse downward trend



Training and Automation



Santoku Linux

- Free and open bootable Linux distribution full of tools
 - Mobile Forensics
 - Mobile App Security Testing
 - Mobile Malware Analysis
- Project is a collaboration with other mobile security and forensic pros



Advanced Analytics

- Must go beyond simple presentation of logical data
- Canonicalization and provenance
- Visualizations
- “Web 2.0” reporting interface
- Export to standard formats for verification (DFXML) and additional analysis



The screenshot displays the liveForensics dashboard. On the left is a navigation menu with options: Dashboard, Monitored Hosts, KRI Configuration, Users, ACCOUNT, Profile, and Sign Out. The main content area is titled 'Dashboard' and contains a table with the following data:

Host	Last Update	Overall Status (Last 5)		
WINNT_SVR_2	26 June 2012 03:22:58 PM CDT	CRITICAL	WARNING	WARNING
OSX_10.6_3	26 June 2012 03:22:58 PM CDT	CRITICAL	NORMAL	CRITICAL
WIN7_PRO_4	26 June 2012 03:22:58 PM CDT	NORMAL	CRITICAL	WARNING
UBUNTU_PRECISE_SVR_5	26 June 2012 03:22:58 PM CDT	WARNING	WARNING	WARNING
UBUNTU_PRECISE_SVR_6	26 June 2012 03:22:58 PM CDT	CRITICAL	WARNING	WARNING
WIN2000_SVR_7	26 June 2012 03:22:58 PM CDT	NORMAL	WARNING	CRITICAL