

**2012 DHS S&T/ASD(R&E)
CYBER SECURITY SBIR WORKSHOP**



Homeland
Security
Science and Technology



Innovations in Mobile Forensics: New tools to fight criminals

viaForensics
Andrew Hoog

Challenges

- Significant data on mobile devices, hard to gain access
- Screen locks, passwords
- Encryption
- Authentication of forensic image
- Meaningful reporting on diverse data

CHALLENGE ACCEPTED



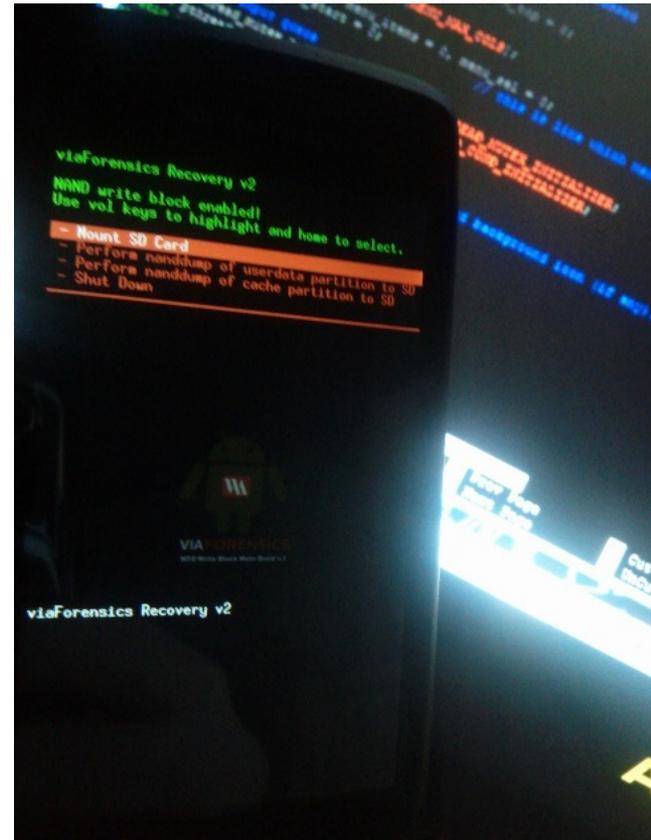
NAND Flash Memory

- High potential for data recovery, 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



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



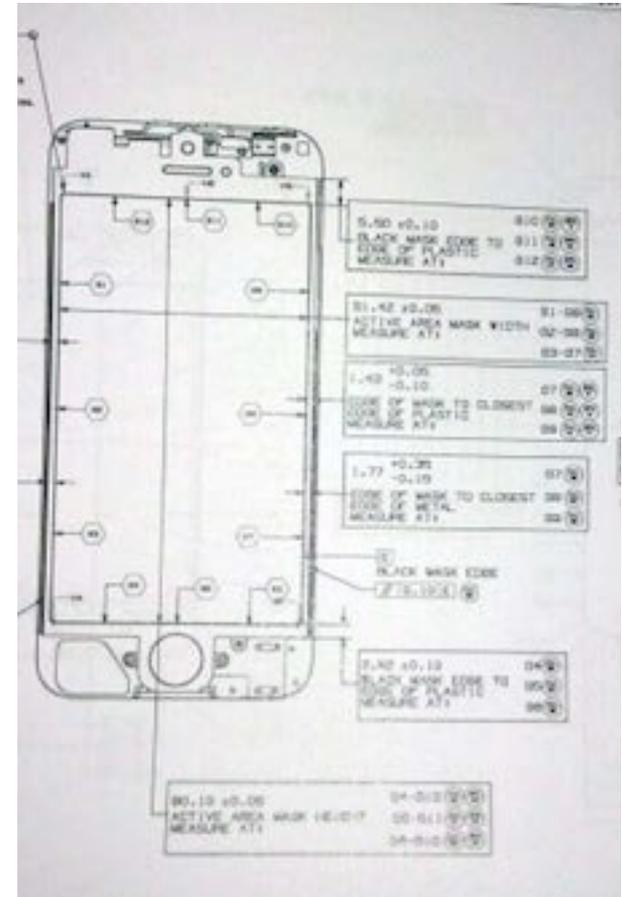
Cracking Encryption

- 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
```

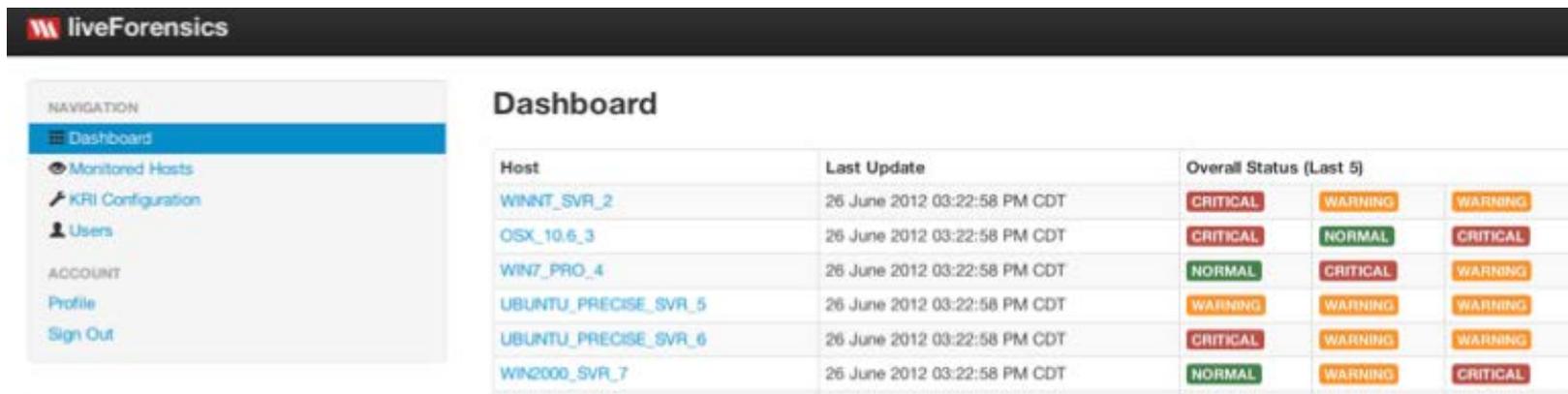

Support More Devices

- 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



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 shows the liveForensics dashboard. On the left is a navigation menu with options: Dashboard (selected), 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