

CYBER SECURITY DIVISION  
2013 PRINCIPAL INVESTIGATORS'

# Breaking Mobile

Advancements in Mobile Forensics and Cyber Security

viaForensics, LLC

Andrew Hoog

*Sep 17, 2013*



Homeland  
Security

Science and Technology

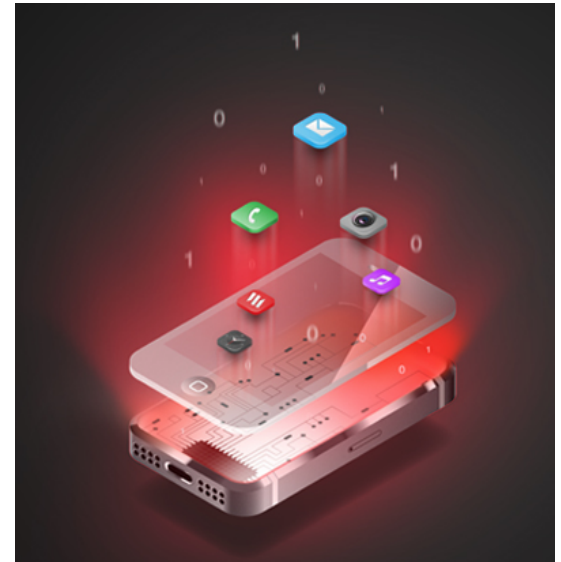
# Company Profile



- Global team of authors, engineers, patent holders, and mobile hackers
- ~40 employees, 10 dedicated to Mobile R&D
- 50% USG, 50% Commercial

# Customer Need

- Verifiable read-only acquisition of recent smartphones (iOS and Android)
- Advanced analytics of mobile forensic data
- Acquisition and analysis of burner phones



# Approach - Smartphone acquisitions

The screenshot displays the AFLogical software interface. On the left, a tree view shows the file structure of the device, including folders like Artifacts, Files, Timeline, and Reports, and various artifact types such as Browser\_Bookmarks, Contacts\_Groups, and IM\_Accounts. The main window is titled 'Device Info' and contains a 'Properties' table and an 'Extraction Options' section.

Properties	
Manufacturer	HTC
Model	HTC Desire CDMA
Serial Number	HT09NHM03155

**Extraction Options**

- Physical**  
Need physical description here.
- Logical: Filesystem**  
Need FS description here.
- Logical: ADB Backup**  
Need ADB description here.
- Logical: AFLogical**  
Need AFL description here.

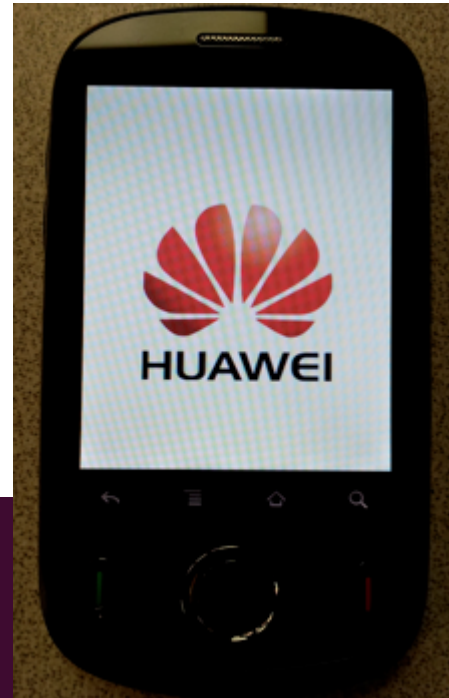
Buttons: Identify Device, Extract

Bottom status bar: Connected - HTC Desire CDMA, Android 4.0, WAITING FOR IP. Progress bar: Complete! Time: 16:47

# Approach - Burner phones

## Huawei M835 Demo

- Extract pin from locked device
- Extract data



```
viaForensics Huawei M835 Pin / Gesture / password removal tool
```

```
-----  
The device should be connected to computer in fastboot mode.  
To put device in fastboot mode, when powering ON, hold  
the volume UP key and press the power on button. The device  
should start, but will stay on the Huawei logo.
```

```
Please press enter when your Huawei M835 is connected to the computer in fastboot mode  
█
```



# Benefits



## Customer Benefits

- Forensically sound process
- Extensive data set extracted
- Extract of newest and most popular burner phones

# Current Status

## Status

- viaExtract 1.7 (AFLogical) released
- 2.0 (Android Physical) release in Oct 2013
- Integration of Burner Phone BAA (Dec 2013)

## Upcoming (proposed if funded)

- 3.0 (iOS Logical and Physical)
- Implementation of fusion engine
- Export data to open, machine-readable standards-based format





# Next Steps

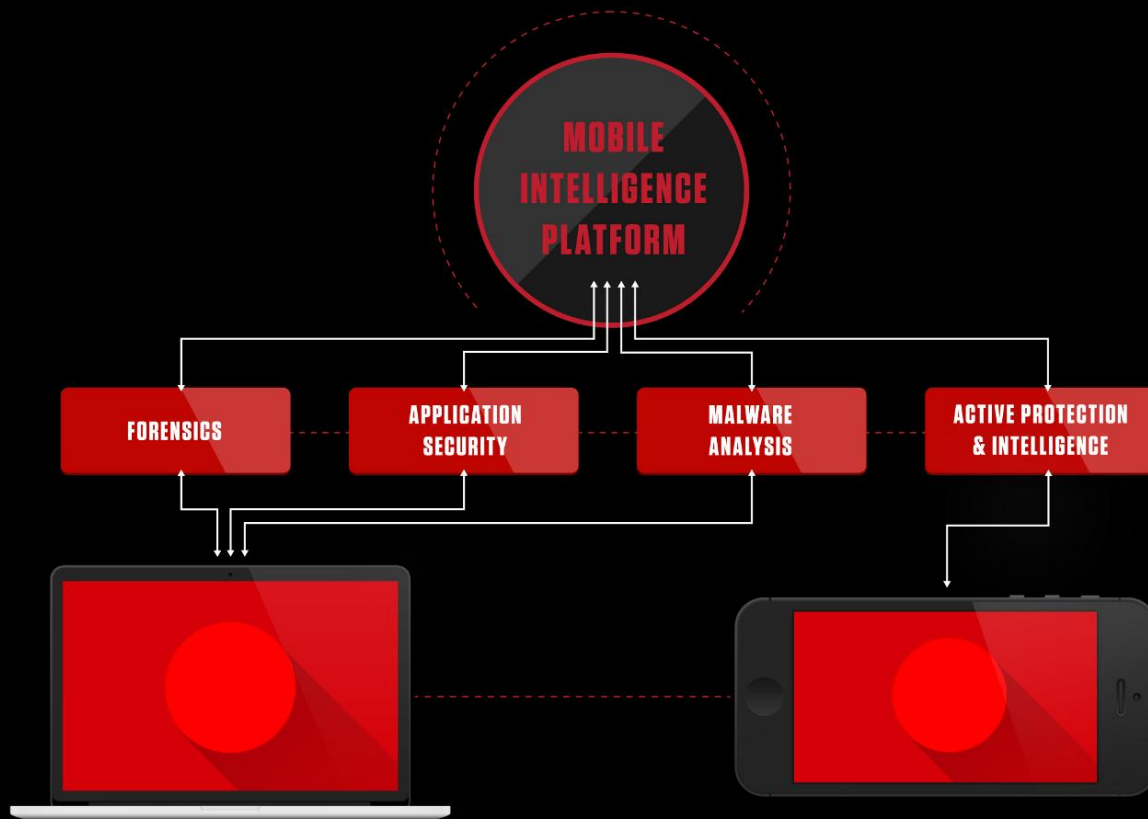


## Commercial opportunities

- Direct sales
- Partner with defense contractor as USG reseller
- Redeploying capabilities (i.e., proactive mobile forensics)
- Technology licensing opportunities from forensics and security vendors



# Next Steps - Mobile Intelligence Platform



# Contact Information

Andrew Hoog  
CEO/Co-Founder, viaForensics  
[ahoog@viaforensics.com](mailto:ahoog@viaforensics.com)

<https://viaforensics.com>

