2013 DHS S&T/DoD ASD (R&E)
CYBER SECURITY SBIR WORKSHOP

viaExtract™ - Advancements in Mobile Forensics and Cyber Security

viaForensics, LLC
Rozel Audric Kouadio

July 22nd 2013

Homeland Security
Science and Technology

Company Profile

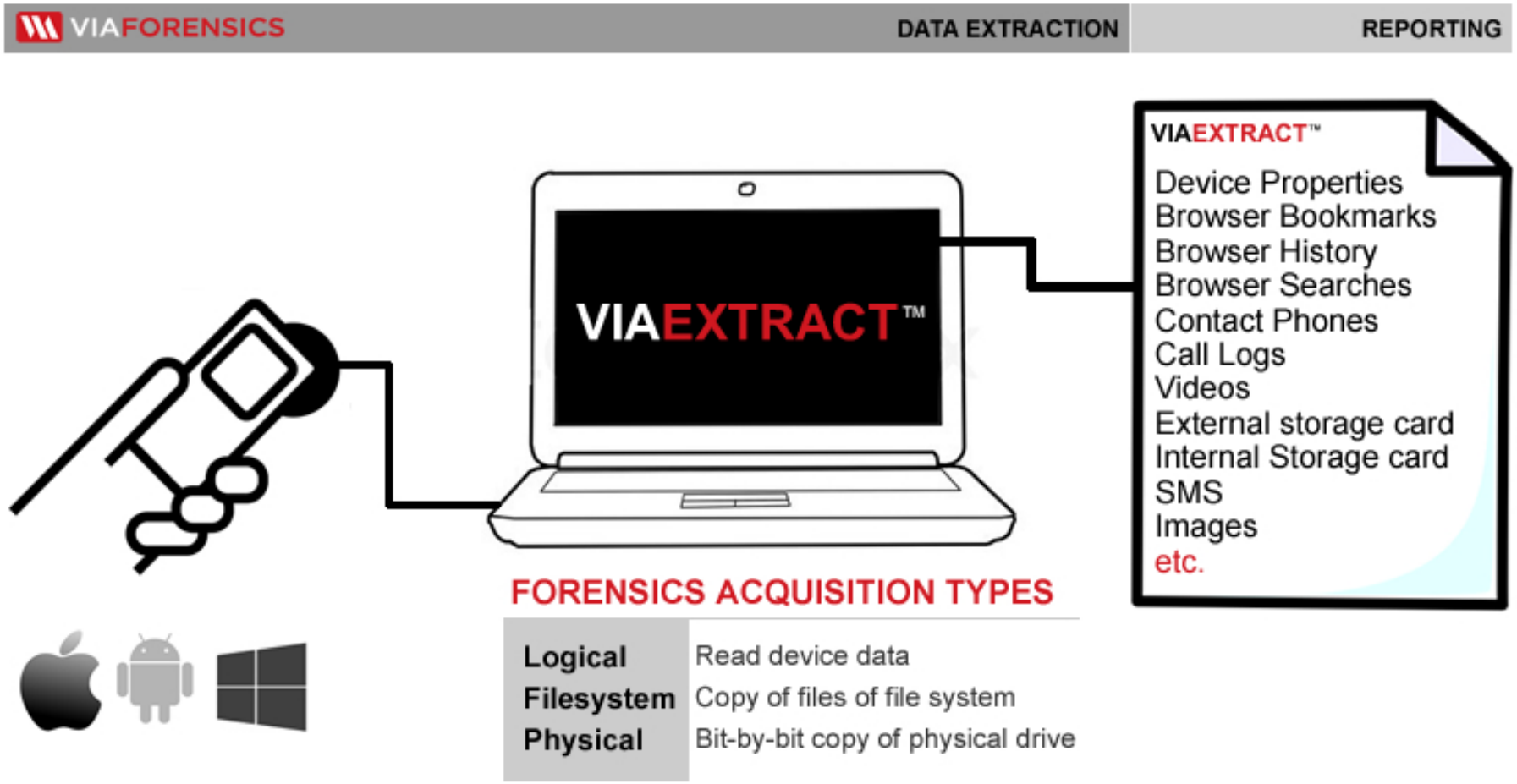
VIAFORENSICS
advancing mobile security

- Global team of authors, engineers, patent holders, and mobile hackers
- Provide advanced mobile security and forensics products and services to Government, Law Enforcement, Fortune 500 and other corporations
- Customers include DARPA, Top 5 banks and Global Fortune 100
- Strategic partnership with CompTIA to produce the first major Secure Mobile App Development Certifications (iOS, Android)

Customer Need

- Government and companies need to thoroughly investigate and secure mobile devices.
- They require tools which can provide:
  - Depth of data recovery
  - Range of devices
  - Efficient reporting
  - Cross-platform capability
  - Forensically sound process

Approach


VIAFORENSICS
DATA EXTRACTION
REPORTING
VIAEXTRACT™
Device Properties
Browser Bookmarks
Browser History
Browser Searches
Contact Phones
Call Logs
Videos
External storage card
Internal Storage card
SMS
Images
etc.
VIAEXTRACT™
FORENSICS ACQUISITION TYPES
Logical
Read device data
Filesystem
Copy of files of file system
Physical
Bit-by-bit copy of physical drive

Approach

Data Acquisition

- Several methods (physical, filesystem) including totally new logical methods on iOS
- Bypass many existing phone locks
- Support for iOS A6/A5/A4 processors

Analysis

- Rapid extraction of most common artifacts such as contacts, call history, browser, SMS/MMS and geolocation
- Access to raw data artifacts for analyst investigation
- Timeline of activities across artifacts

Reporting

- Browse, sort, and filter data
- Customize report content
- Export to standard formats (e.g. DFXML)

Benefits

Customer Benefits

- Greater depth of information recovered from the most popular mobile devices
- Fast, efficient data acquisition and reporting processes
- Cross-platform acquisition from powerful Santoku Linux OS environment
- Software-based security bypass can save investigators weeks of time waiting for physical recoveries (e.g. chip-off)
- New techniques for zero-write forensic acquisitions

- **NET:** Better, more thorough forensic investigation from affordable software

Current Status

Completed

- viaExtract™ software for Android logical data acquisition.
- Online JTAG training series for mobile forensics.
- Logical acquisition on iOS and WP8 (alpha).
- Physical acquisition on Android and iOS (alpha).

In Progress

- Further R&D on iOS 7, Windows Phone 8, new Android devices.
- Complete integration of new acquisition methods in viaExtract
- Updated Analysis & reporting in viaExtract

Next Steps

viaForensics will release viaExtract 2.0 with support for Android physical by September 2013.

Two primary commercial objectives

- Government and Law Enforcement can license the software and benefit directly
- System Integrators may wish to resell, or license data acquisition or other technologies developed by viaForensics

Contact Information

Rozel Audric Kouadio
Senior Security Manager, viaForensics
rkouadio@viaforensics.com

https://viaforensics.com

VIAFORENSICS
advancing mobile security