Open Source Mobile Device Forensics

Heather Mahalik
Device Acquisition

iOS Devices
• Zdziarski Methods
• Boot Rom Vulnerability Exploits
  – Custom Ramdisk via SSH
  – The iPhone Data Protection Tools
• iTunes

Android Devices
• viaLogical
• ADB Backup
• OSAF Toolkit
• Santoku
• DD
  – Not supported for all devices
• JTAG/Chip-off
Considerations

• How old is the device?
• Is the device locked?
• Is the device damaged?
• Are you Law Enforcement?
• LiME (Linux Memory Extractor)
  – First tool to support full memory captures of Android smartphones!
  – TCP dump or saved to SD card
  – Uses ADB
Analytical Tools...to Name a Few

**iOS Devices**
- iPhone Backup Analyzer
- iExplorer
- iBackupBot
- Scalpel
- SQLite Browser
- Plist Editor
- WhatsApp Extract
  - Contacts.sqlite and ChatStorage.sqlite
- Manual examination
- Customized scripts

**Android Devices**
- Autopsy
  - Android Module
- WhatsApp Extract
  - wa.db and msgstore.db
- Scalpel
- SQLite Browser
- Hex Editor
- Anything capable of mounting EXT
- FTK Imager
- Customized scripts
- Manual examination

© 2014, Basis Technology
Realistically Check!

- Commercial tools are expensive
  - They still miss data
  - They don’t parse third party applications completely
  - They omit relevant databases when extracting data
  - They don’t support all devices
- Open Source tools
  - See above!
/private/var/mobile/library/Spotlight/com.apple.mobilesms/
  – smssearchindex.sqlite

- Provides SMS message data
  - Active and deleted messages
  - Should be compared to sms.db
  - May show traces of attachments (metadata)

*Not commonly parsed by any tool!*
Autopsy

• GUI built on The Sleuth Kit
• Next version (v3.1.1) will include Android module
• Customizable
• Complete analytical platform
• Android dumps can be loaded as normal disk images or file folders

© 2014, Basis Technology
Examining Contacts

- Parsed from Contacts2.db file
  - Raw_contacts and ABPerson
Examining the Raw Contacts (1)
Examining the Raw Contacts (2)
Parsing Messages and Chats

- Parses messages and chats from SMS, MMS and some third party applications
• Encryption vs. Encoding
• Base64 decoder built into Autopsy Android module
Geolocation Support

- Google Maps, Browser, Cache and EXIF location parsing
Geolocation Reporting
Examining Multimedia Files

• EXIF Parser

• Graphics and Videos
Recovering Deleted SQLite Data

- Active files shown in viewer

- Deleted must be examined/recovered in Hex
Custom Scripts

- Mari DeGrazia’s SQLite Parser
References, Sources and Suggested Reading

- www.az4n6.blogspot.com
- https://viaforensics.com/blog/
- http://www.sleuthkit.org/
- Practical Mobile Forensics – Bommisetty, Mahalik, Tamma
- www.smarterforensics.com
- https://code.google.com/p/lime-forensics/
Questions

Heather Mahalik
Basis Technology
www.basistech.com
hmahalik@basistech.com
Twitter: @heathermahalik