Flash & Phones

Advanced Laboratory Data Recovery from Secure Mobile Devices

Session 301-I

Presented by:

Will DeLisi

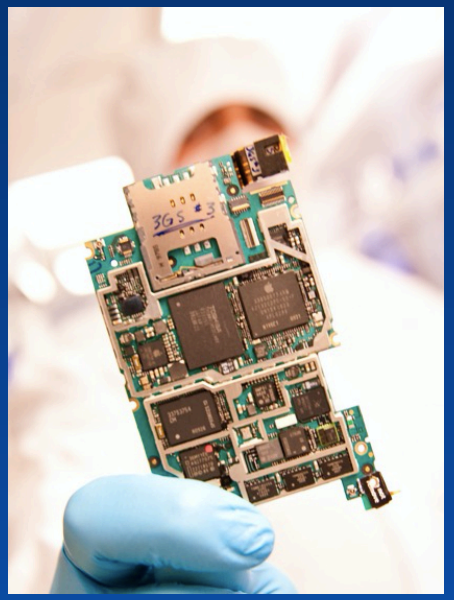
DriveSavers Data Recovery,

eDiscovery & Digital Forensics

Santa Clara, CA
August 2016

Agenda

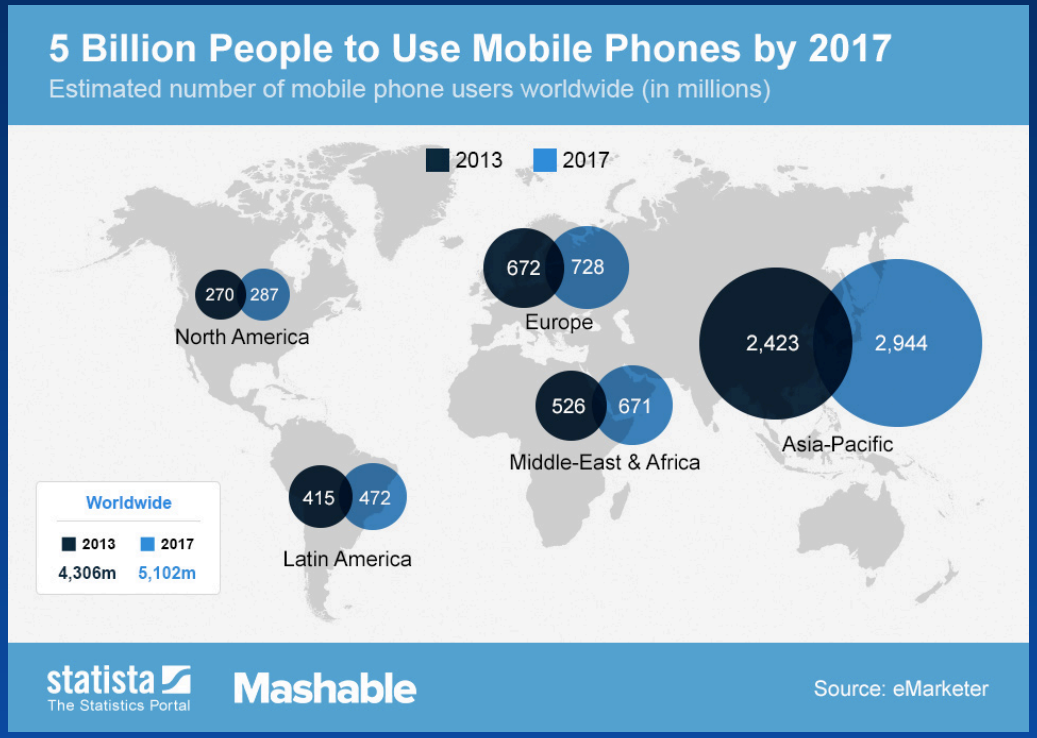
- Why Data Recovery from Smartphones?
- Lab Processes & Challenges
- Case Study
- Looking Forward



Why Smartphone Data Recovery?

- 1 billion Apple iPhones sold
  - But recently flat sales
- Billions of Android phones sold
  - 400+ manufacturers, 4000+ models
  - Activation rate 6:1 over iOS

Why Smartphone Data Recovery?



Why Smartphone Data Recovery?

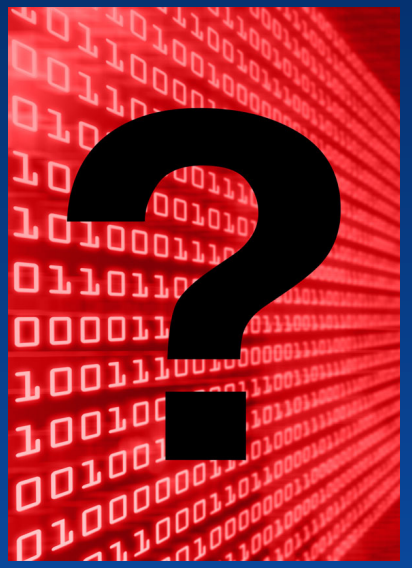
- User and device are in motion
  - Phones get dropped, smashed, submerged, lost
- Most recent data will be on phone only
  - Photos, videos, contacts, personal information
- Passcodes and security
  - People forget passcodes
  - In the event of death, family or estate wants data
  - For forensic, legal and law enforcement

Why Smartphone Data Recovery?

- But Cloud backup is (almost) FREE!
  - Hard to backup all data all the time to one location
  - “Freemium” pricing can get expensive
- It can be confusing to manage
  - What data is where on what cloud service?
- People are lazy
  - You have to turn it on, configure and leave it on!

Lab Process & Challenges

- Initial analysis and diagnosis
  - Determine if physical failure
    - External trauma
    - Liquid exposure
    - Electronic issues
  - Or logical issue
    - Passcode lockout & encryption
    - File Deletion
    - OS or file system corruption

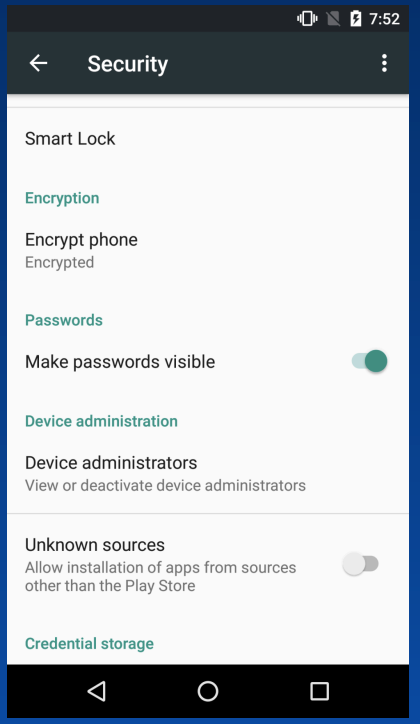


Logical Recovery Process

- Passcode lockout is a common problem
  - User forgets code or fingerprint needs to be reconfigured
  - Phone disabled from too many attempts and user risks factory reset

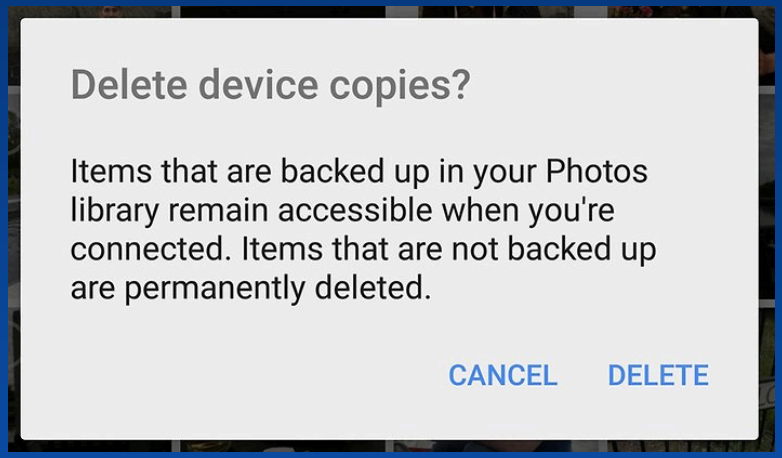
Logical Recovery Process

- Encryption
  - iOS always on since 3GS model
    - Hardware/software combination
    - Very difficult to exploit
  - Android
    - ~10% with encryption enabled
    - Performance suffers due to software encryption
    - Easier to exploit



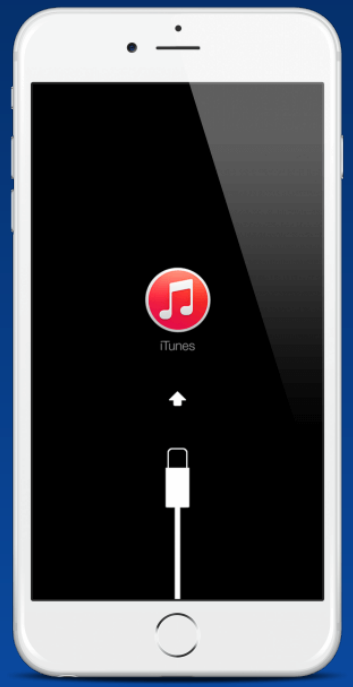
Logical Recovery Process

- File deletion
  - User deletes local copy of data before it is backed up or synced to cloud



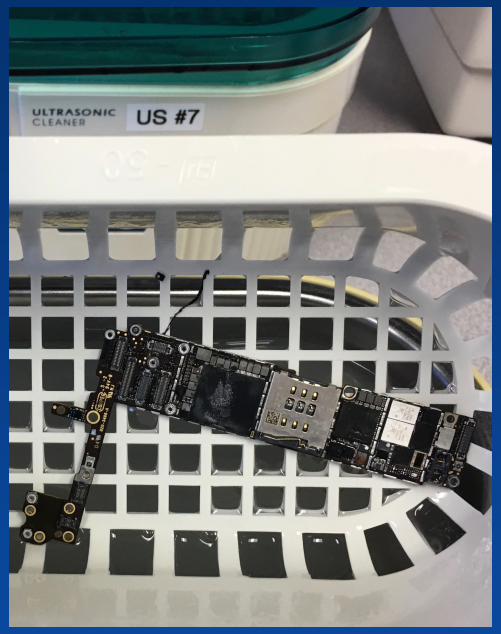
Logical Recovery Process

- OS or file system corruption
  - Phone powers on but will not boot
  - May be stuck in recovery or restore mode
  - Unknown issues



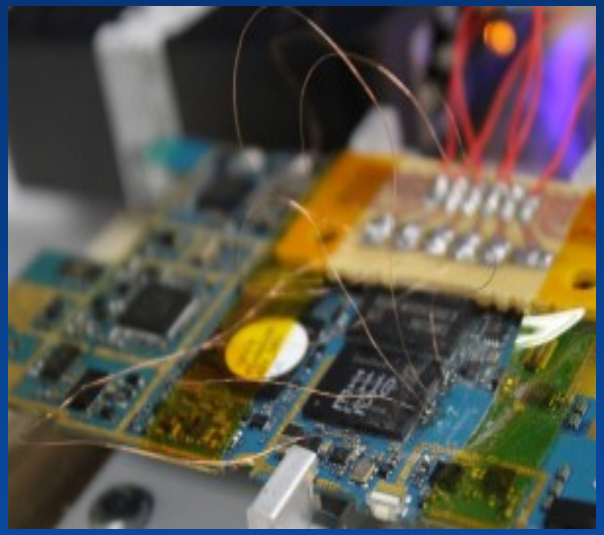
Physical Recovery Process

- Device teardown & cleaning
  - Disassembly of device to component level
  - Inspection and cleaning of any corrosion



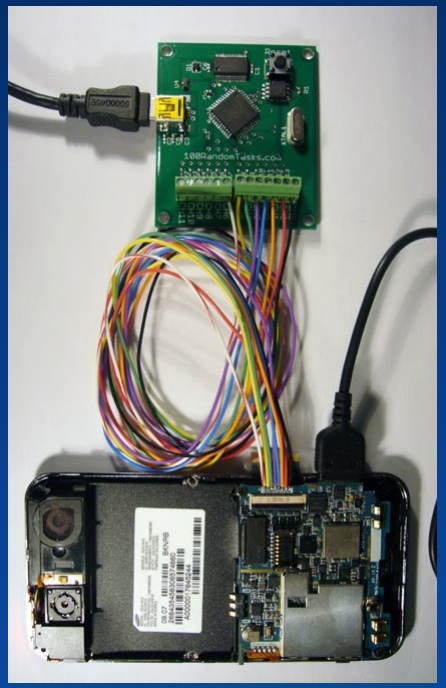
Physical Recovery Process

- PCB diagnosis and repair
  - Test for faults on PCB
  - Remove, reflow and replace components
  - Re-route circuits
  - Rebuild the device and recover



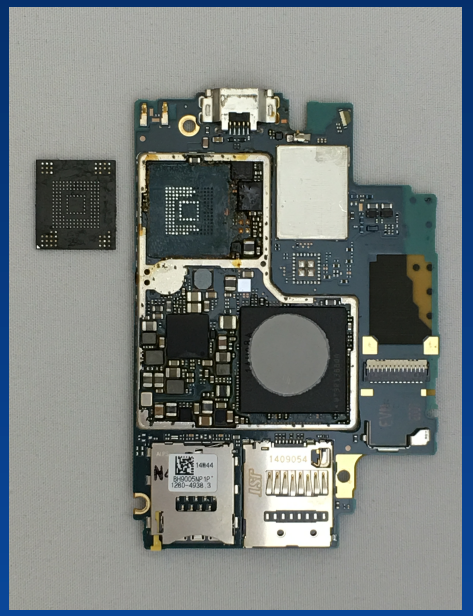
Physical Recovery Process

- JTAG
  - TAPs (test access points) for access
  - Trial and error
  - Not supported or implemented on all devices, never on Apple



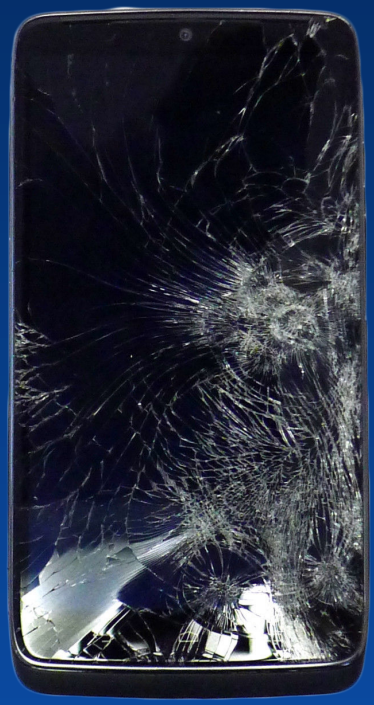
Physical Recovery Process

- Chip-off and raw NAND imaging
  - Typically the last ditch effort
  - Time & labor intensive
  - Not all SSDs are supported
  - Multiple layers to reassemble into LBA image
  - Encryption complicates or makes impossible



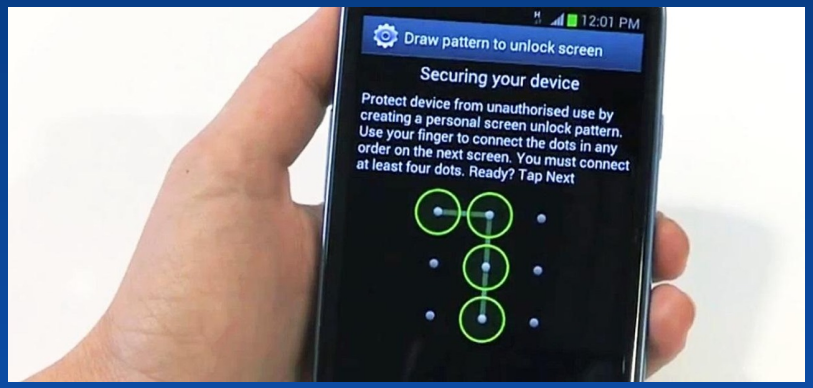
Customer Case Study

- Motorola Droid Turbo XT1254
  - Cracked screen; would not charge or boot
- Army soldier lost in the line of duty
  - Parents wanted data and memories of their lost son



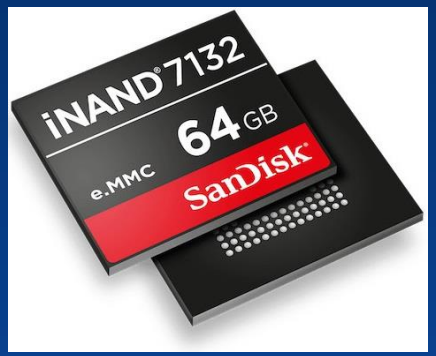
Customer Case Study

- Repaired PCB
  - Rebuilt into a new phone body
- Phone now boots but locked with swipe code
- Chip-off process best chance to get access



Customer Case Study

- SanDisk eMMC NAND
  - Chip removed and cleaned
- Extract NAND raw image
- Decode and create “best effort” LBA
- Recover file system and verify data
- Return recovered data, and son’s memories to the parents



What to Remember

- Mobile devices will become more rugged and more waterproof in the future, but not fail-proof
- The market for Smart devices and wearable technology will continue to expand, and no user will ever be completely backed up
- If you do lose important data, contact a professional recovery lab for assistance

Thank You!

Will DeLisi

will.delisi@drivesavers.com

DriveSavers Data Recovery,
eDiscovery & Digital Forensics