The Past and Current State of Mobile Device Recovery

Steve Hruska, HW R&D Engineer
Ontrack Data Recovery
What is Mobile Data Recovery?
Mobile Device Recovery History

- Early Mobile Recoveries
  - Pros
    - Unencrypted
    - Security a somewhat low concern
    - Logical/Physical memory access
    - Low capacities
  - Cons
    - Custom cables/chargers
    - Proprietary software
    - Unique memory use
What Changed?

- Universal interface adoption
  - Lightning-iOS
  - USB-Android
- Standardized operating systems
  - iOS
  - Android
- Standardized NAND utilization
Current Recovery Options-Logical

- **Logical**
  - OS corruption
    - Can be bypassed in some cases
  - Passcode issues
    - Disabled device
    - Forgotten/unknown passcode
  - Deleted Data
    - Individual assets
    - Factory reset
  - Exploits, exploits, exploits!
Current Recovery Options-Logical

- Factory Reset Devices
  - iOS factory resets
    - Utilized a crypto-shred type reset
    - No access to unallocated data
  - Android
    - Uses File-Based Encryption and Full Disk Encryption
    - Uses similar crypto-shred type reset
    - MicroSD
      - Not the most efficient way to erase removable unless encrypted
Current Recovery Options - Physical

- **Physical**
  - ISP (In-System Programming)
  - Chip-off
    - Removal of eMMC itself and read through adapter
    - Direct NAND access on eMMC
  - Full physical memory dump through device interface
Current Recovery Options - Physical

- Physical cont.
  - Most cases require a booting phone to acquire data
    - Hardware encryption
    - Ability to enter passcodes/home button verification
  - Repair as a path to recovery
    - Devices are not designed with repair in mind
Conclusion

- Mobile device recoveries are still possible
- Physical failures are uncommon for flash memory
- Backup your data!
- If you experience data loss, call an expert

Visit us at Booth 126!