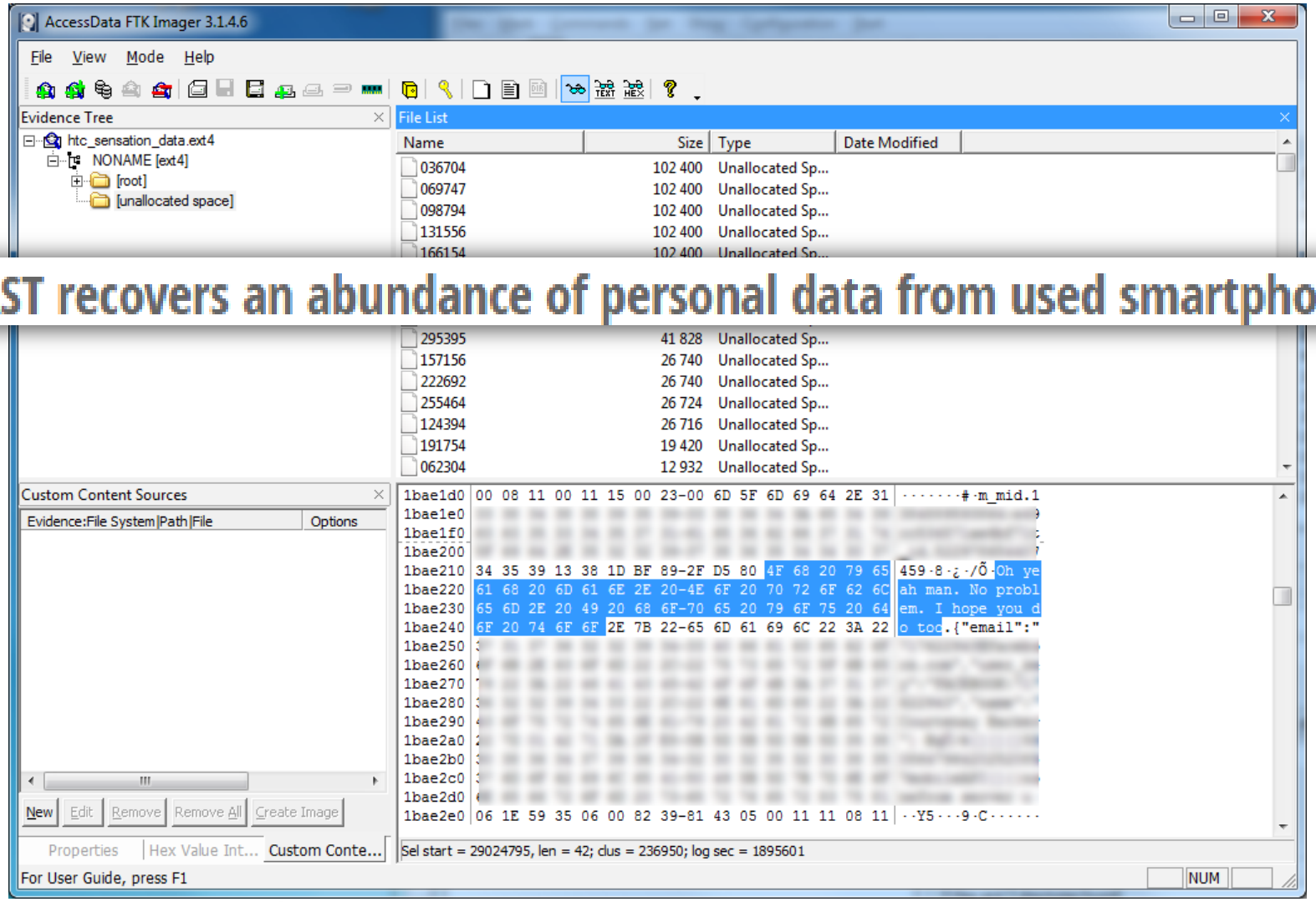
Data Destruction of Mobile Devices

…did it really wipe all data?

ICRS – November 12, 2014

The Problem



AVAST recovers an abundance of personal data from used smartphones

The Problem

Common data found on smartphones:

- Email
- Text Messaging
- Photos
- Video
- Audio
- Web History
- Call History
- Application Data
- eBooks
- Maps/GPS

CASCADE ASSET MANAGEMENT, LLC

Forensic methods can retrieve data

Not all smart phones are the same

Not all smart phones are the same

Hardware
Firmware
Software
OS
Apps

Data Storage Complexity

Hardware Factors

- Many manufacturers of devices and firmware
- Fragmentation with hardware implementation
- Support for encryption & other security varies
- Rooted devices

Data Storage Complexity

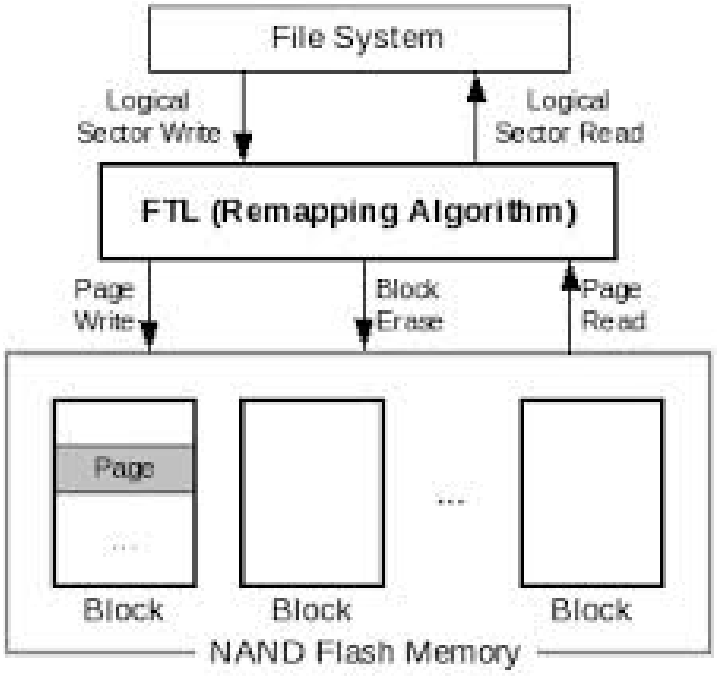
Software Factors

- **Different OS platforms and versions available**
- **Implementation can be different - effectiveness of OS varies with hardware/firmware**

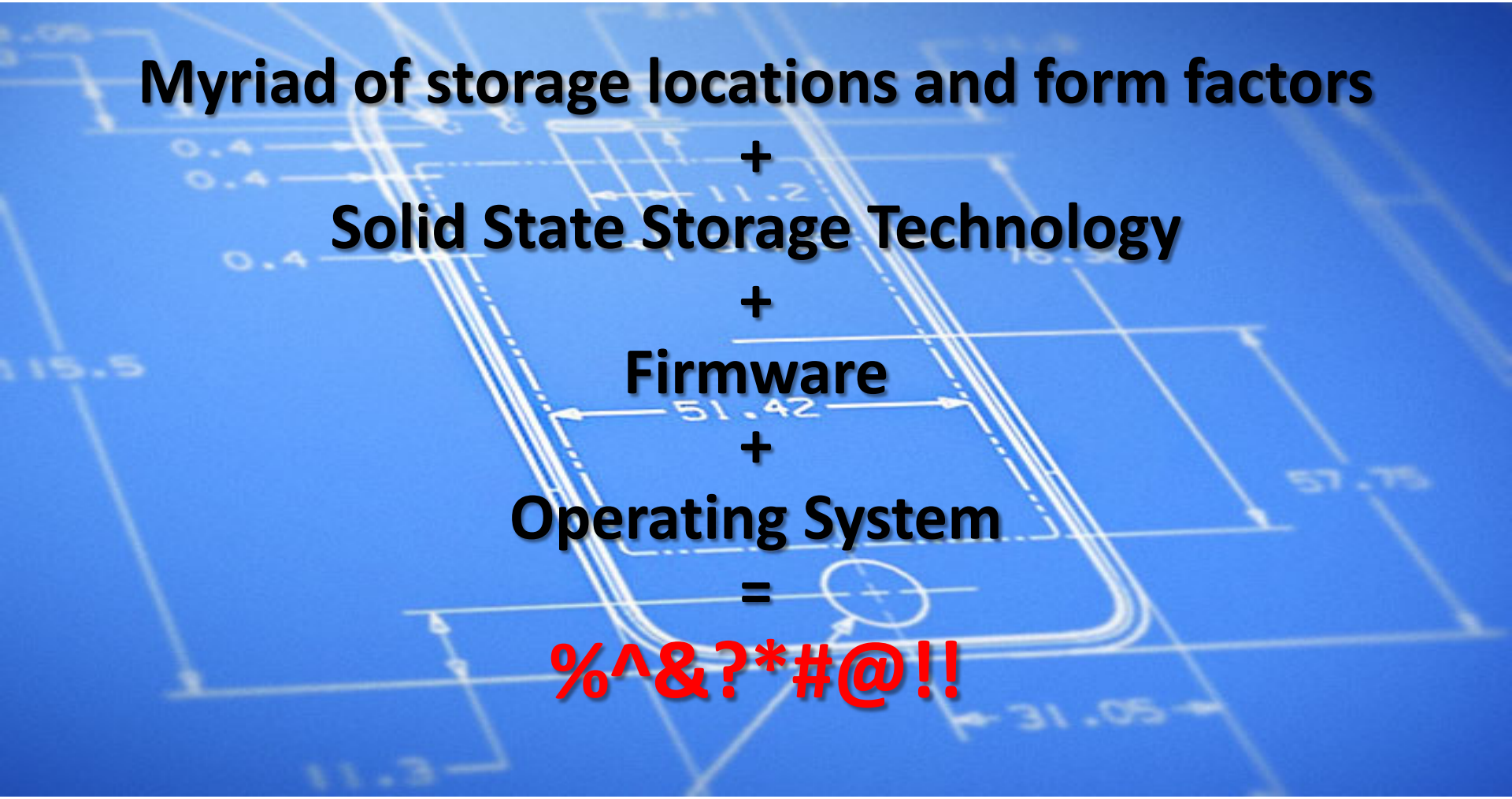
Data Storage Complexity

Solid State Storage Technology

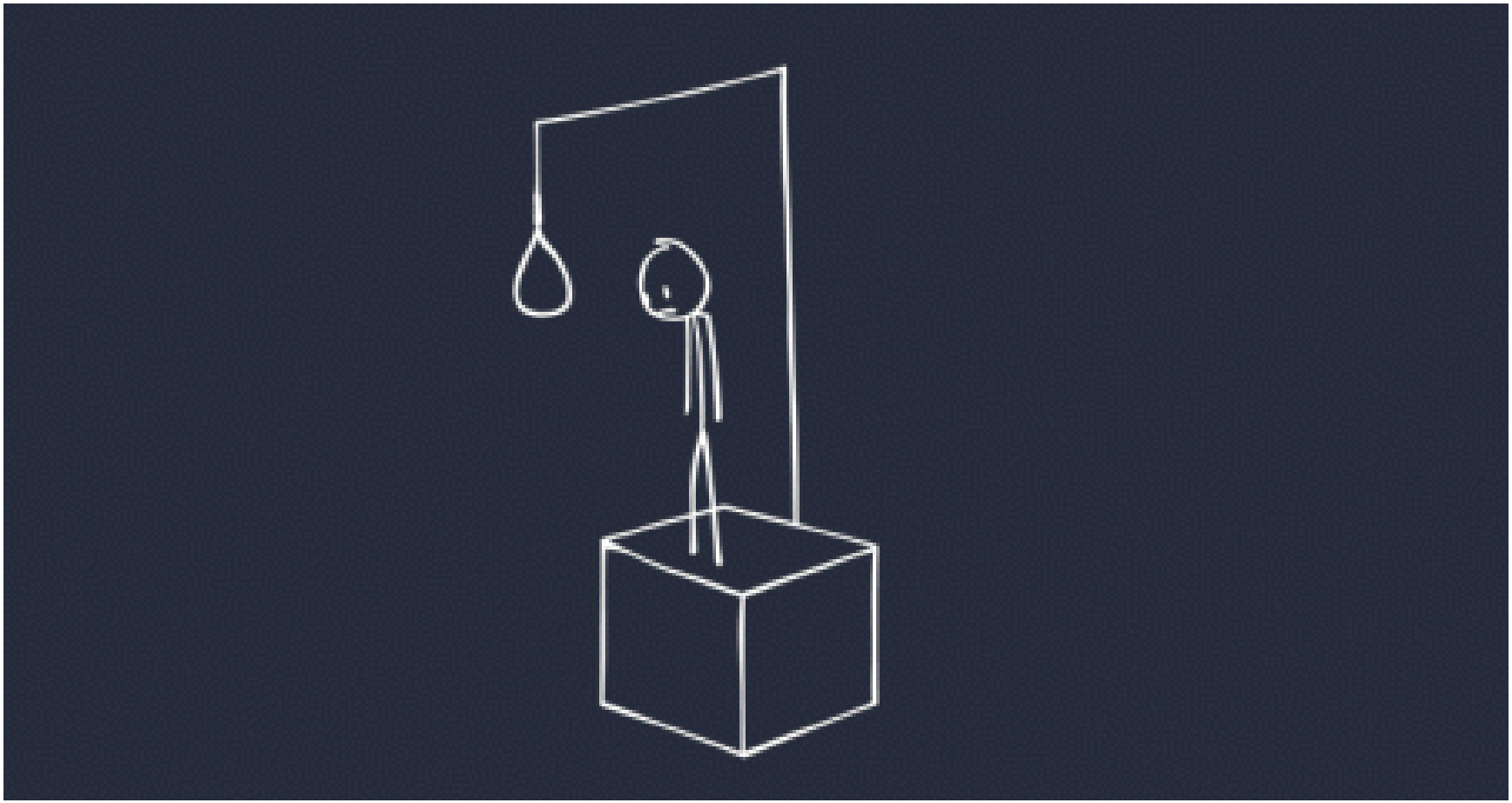
- **Limitations for access, validation of data storage areas:**
  - **Wear leveling**
  - **Over-provisioning**
  - **SIM/SD cards**



Data Storage Complexity



Data Storage Complexity



Wiping methods are inconsistent and sometimes ineffective

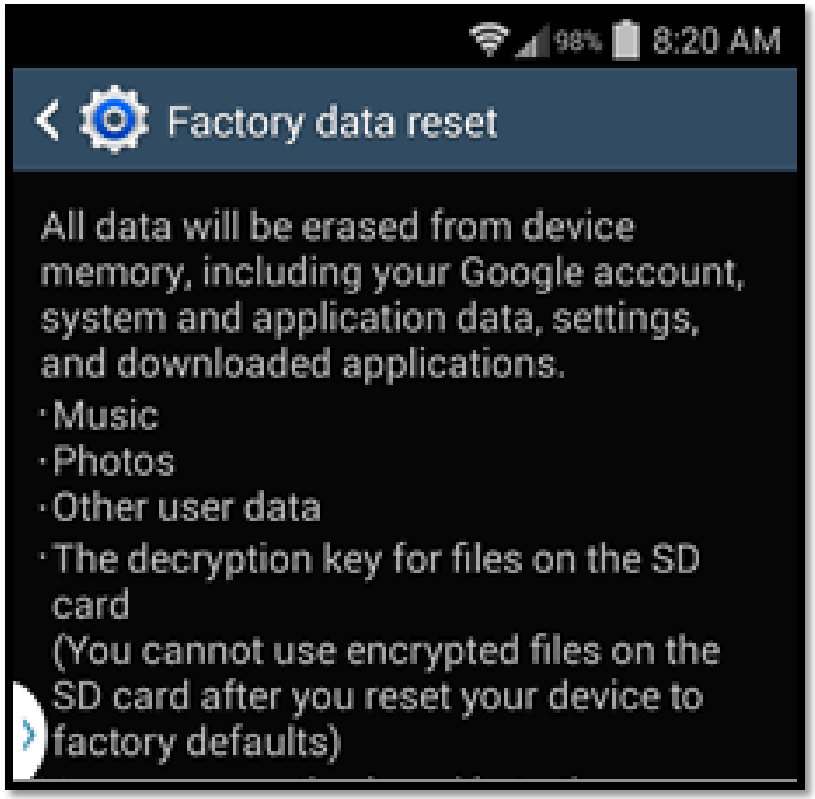
There is no single standard for smartphone sanitization

- **NIST Guidelines 800-88 Rev 1**
- **Manufacturer Recommendations**
- **Scramble and Finally Erase (SAFE)**

Validation is difficult or impossible – can you prove erasure? Can you prove recovery?

CASCADE ASSET MANAGEMENT, LLC

Wiping methods are inconsistent and sometimes ineffective

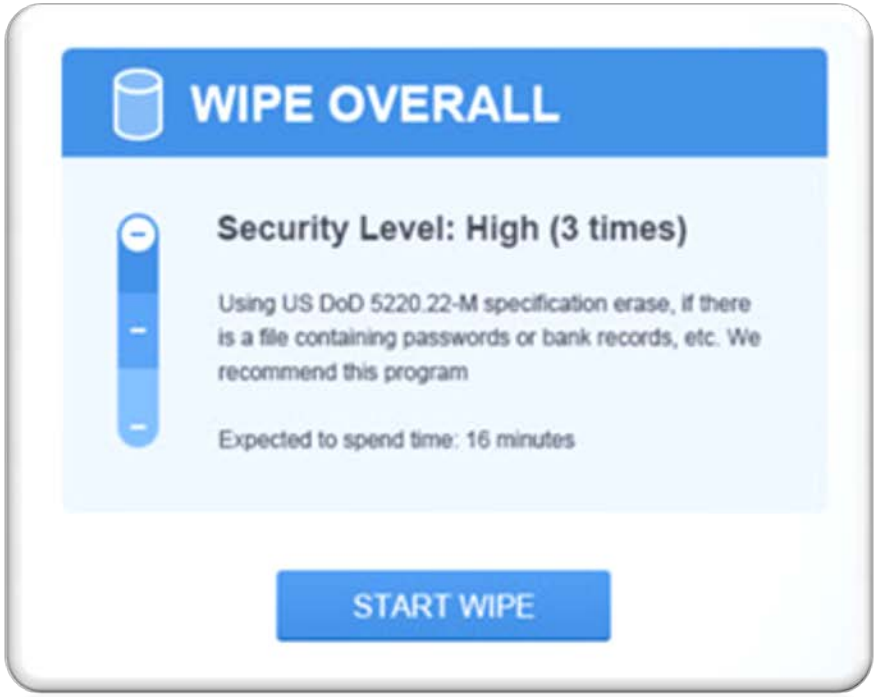


Factory Reset

Manufacturer methods aren't reliable

Removes index

Wiping methods are inconsistent and sometimes ineffective



Overwriting

3rd party / enterprise providers

Verification issues – proving overwrite vs recovery

Application of ill-adapted standards (DoD)

Wiping methods are inconsistent and sometimes ineffective

Crypto Erase

Removal of key - data exists as cipher text

Hardware and software

The new standard for security

Wiping methods are inconsistent and sometimes ineffective

Encryption is now standard (but not always enabled)

Apple	Google	Samsung	Blackberry	Microsoft
iOS 7 & 8	Android 4	Android 4+ SAFE	BlackBerry 10 + BES 10	Windows Phone 8 & 8.1
AES 256 User disable option = No	AES 128 User disable option = No	AES 256 User disable option = Yes **Not all devices support encryption*	AES 256 User disable option = Yes	AES 256 User disable option = No

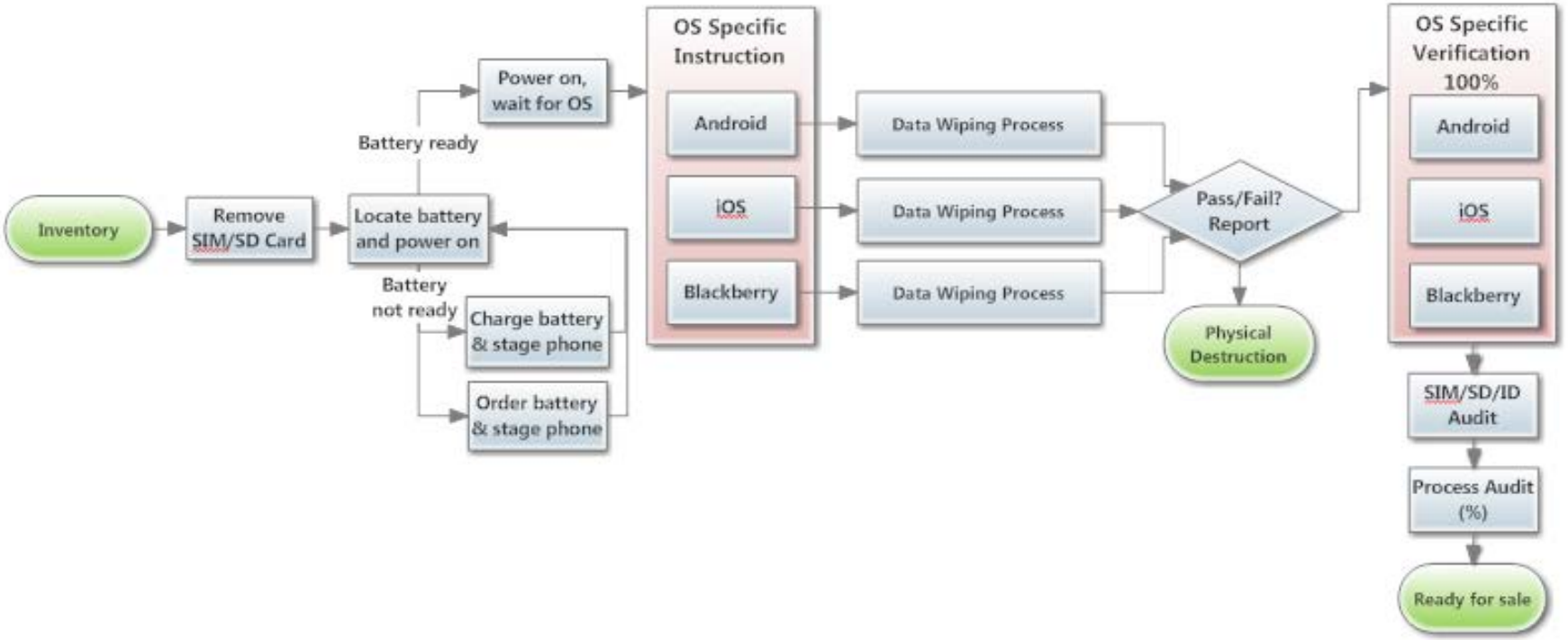
CASCADE ASSET MANAGEMENT, LLC

Wiping methods are inconsistent and sometimes ineffective

FBI blasts Apple, Google for locking police out of phones

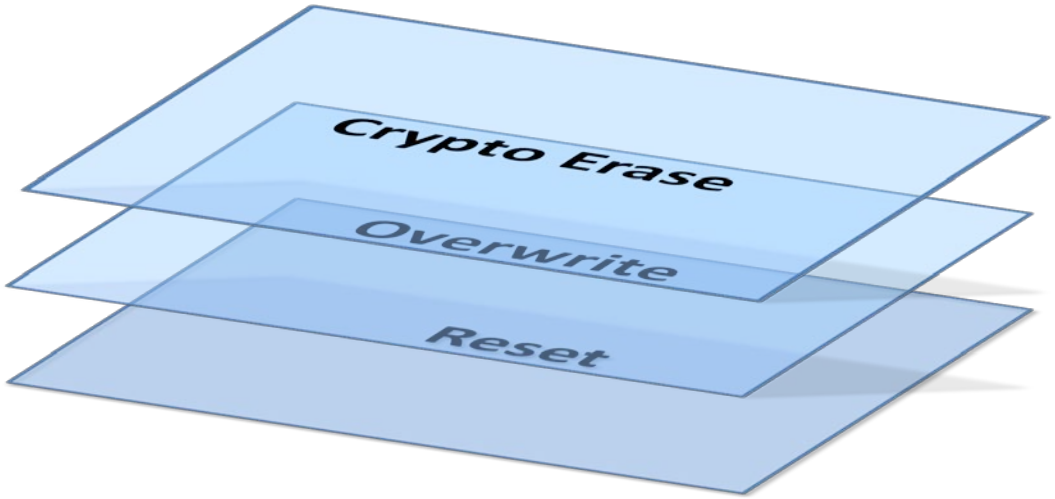
The best defense is a hybrid approach

Evaluate your threat! Then…established procedures and verification are key



The best defense is a hybrid approach

Consider layers of wiping methods (depends on threat level)



CASCADE ASSET MANAGEMENT, LLC

The best defense is a hybrid approach

Enterprise sanitization solutions

Third party forensics…consider the ROI

Thank you!

TJ Barelmann
Cascade Asset Management
tj@cascade-assets.com
608.280.1840
@TJBarelmann

CASCADE ASSET MANAGEMENT, LLC