Data Destruction of Mobile Devices
...did it really wipe all data?
The Problem

AVAST recovers an abundance of personal data from used smartphones
## The Problem

Common data found on smartphones:

<table>
<thead>
<tr>
<th>Email</th>
<th>Web History</th>
</tr>
</thead>
<tbody>
<tr>
<td>Text Messaging</td>
<td>Call History</td>
</tr>
<tr>
<td>Photos</td>
<td>Application Data</td>
</tr>
<tr>
<td>Video</td>
<td>eBooks</td>
</tr>
<tr>
<td>Audio</td>
<td>Maps/GPS</td>
</tr>
</tbody>
</table>
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

Myriad of storage locations and form factors
+ Solid State Storage Technology
+ Firmware
+ Operating System
= %^&?*#@!!
Data Storage Complexity

- Myriad of storage locations and form factors
- Solid State Storage Technology
- Firmware
- Operating Systems

%^&?*#@!!
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?
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)

<table>
<thead>
<tr>
<th>Apple</th>
<th>Google</th>
<th>Samsung</th>
<th>Blackberry</th>
<th>Microsoft</th>
</tr>
</thead>
<tbody>
<tr>
<td>iOS 7 &amp; 8</td>
<td>Android 4</td>
<td>Android 4+ SAFE</td>
<td>BlackBerry 10 + BES 10</td>
<td>Windows Phone 8 &amp; 8.1</td>
</tr>
<tr>
<td>AES 256</td>
<td>AES 128</td>
<td>AES 256</td>
<td>AES 256</td>
<td>AES 256</td>
</tr>
<tr>
<td>User disable option = No</td>
<td>User disable option = No</td>
<td>User disable option = Yes</td>
<td>User disable option = Yes</td>
<td>User disable option = No</td>
</tr>
</tbody>
</table>

*Not all devices support encryption*
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)
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
@TJBareIlmann