Jeff Hedlesky – Forensic Evangelist
Forensic Business Unit – GSI

Overcoming the Unique Challenges of Digital Forensics
Just a Little About Me…

Santa Clara, CA
August 2015
## Just a Few of our Customers…

<table>
<thead>
<tr>
<th>Government</th>
<th>Energy / Utilities</th>
<th>Insurance</th>
<th>Banking/ Finance</th>
<th>Technology</th>
<th>Telecom</th>
<th>Retail/CPG</th>
<th>Manufacturing &amp; Industrial</th>
<th>Pharma/ Biotech</th>
</tr>
</thead>
<tbody>
<tr>
<td>State Dept.</td>
<td>Exelon</td>
<td>Aetna</td>
<td>Bank of America</td>
<td>Intel</td>
<td>AT&amp;T</td>
<td>Hershey Co.</td>
<td>UTC</td>
<td>Amgen</td>
</tr>
<tr>
<td>IRS</td>
<td>Chevron</td>
<td>Liberty Mutual</td>
<td>Wells Fargo</td>
<td>Dell</td>
<td>Comcast</td>
<td>Coca Cola</td>
<td>GE</td>
<td>Genentech</td>
</tr>
<tr>
<td>Treasury</td>
<td>Koch</td>
<td>Allstate</td>
<td>Citigroup</td>
<td>Motorola</td>
<td>Cox</td>
<td>P &amp; G Lowe’s</td>
<td>Rolls-Royce</td>
<td>Roche</td>
</tr>
<tr>
<td>DOJ</td>
<td>Halliburton</td>
<td>Nationwide</td>
<td>Deutsch Bank</td>
<td>McAfee</td>
<td>Verizon</td>
<td>Wal-Mart</td>
<td>Toyota</td>
<td>Novartis</td>
</tr>
<tr>
<td>Energy Dept.</td>
<td>DTE</td>
<td>USAA</td>
<td>JPMorgan Chase</td>
<td>Sony</td>
<td>Sprint</td>
<td>Target</td>
<td>Ford</td>
<td>Pfizer</td>
</tr>
<tr>
<td>DHS</td>
<td>El Paso</td>
<td>Am. Fam.</td>
<td>KeyBank</td>
<td>Microsoft</td>
<td>Vodafone</td>
<td>Home Depot</td>
<td>Textron</td>
<td>Merck</td>
</tr>
<tr>
<td>HHS</td>
<td>Anadarko</td>
<td>CIGNA</td>
<td>HSBC</td>
<td>RIM</td>
<td>Disney</td>
<td>Disney</td>
<td>CSC</td>
<td>Merck</td>
</tr>
<tr>
<td>DOD</td>
<td>PSEG</td>
<td>Hartford</td>
<td>Barclays</td>
<td>Symantec</td>
<td>Best Buy</td>
<td>Best Buy</td>
<td>Diebold</td>
<td>Novartis</td>
</tr>
<tr>
<td>CIA</td>
<td>SoCal Edison</td>
<td>Kaiser</td>
<td>Barclays</td>
<td>eBay</td>
<td>Staples</td>
<td>Staples</td>
<td>Boise- Cascade</td>
<td>Pfizer</td>
</tr>
<tr>
<td>FBI</td>
<td>Dominion</td>
<td>UnitedHealth</td>
<td>First American</td>
<td>Cisco</td>
<td>OfficeMax</td>
<td>OfficeMax</td>
<td>Eaton</td>
<td>Merck</td>
</tr>
<tr>
<td>NSA</td>
<td>Shell</td>
<td>UnitedHealth</td>
<td>Visa</td>
<td>EMC</td>
<td>Big Lots</td>
<td>Big Lots</td>
<td>Fluor</td>
<td>Purdue Phar.</td>
</tr>
<tr>
<td>UK MOD</td>
<td></td>
<td></td>
<td>MasterCard</td>
<td>HP</td>
<td>Mattel</td>
<td>Mattel</td>
<td>Gen. Dynamics</td>
<td>Watson</td>
</tr>
<tr>
<td>UK FCO</td>
<td></td>
<td></td>
<td>UBS</td>
<td>NetApp</td>
<td>McDonald’s</td>
<td>McDonald’s</td>
<td>Northrop</td>
<td>Wyeth</td>
</tr>
<tr>
<td>NATO</td>
<td></td>
<td></td>
<td>Vanguard</td>
<td>Intuit</td>
<td>SuperValu</td>
<td>SuperValu</td>
<td></td>
<td></td>
</tr>
<tr>
<td>UN</td>
<td></td>
<td></td>
<td>Fidelity</td>
<td>Oracle</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Yahoo!</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Qualcomm</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Santa Clara, CA</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>August 2015</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Just a few of our Forensic Hardware Products

T35u
T8u
UltraBay 3d™
T3iu
T35689iu
TD2u
TD3

Santa Clara, CA
August 2015
All ATA write / erase commands are blocked.

Along with the cloning / imaging of suspect drive, a digital fingerprint, or hash is generated for purposes of proving forensic integrity of evidence (from crime scene to courtroom).
SSD Controller Best Practices

We understand that SSD manufacturers have different concerns than the Digital Forensic community.

- Speed
- Durability
- Compatibility
- Privacy / Security
- Price/Performance
- Unique Differentiators
SSD Controller ≠ HD Controller

With an intelligent SSD controller, write-blocking the host computer is no longer sufficient.

- BGC
- TRIM
- Over-provisioning blocks
- File De-duplication
- Other “Special Sauce”
We Need YOUR Help!

What we’re not asking for:

- Universal JTAG / Serial ports, for direct reading of physical layer
- Encrypted or unpublished ATA commands
- Persistent state changes, without end-user knowledge

What we are asking for:

- Universal tools, for all parties to use, in the forensically sound recovery of SSD data
- Additional ATA commands, to reflect the new unique challenges which SSDs present to users, AND to the law enforcement, intelligence and defense communities of the world
Our ‘Asks’:

Deterministic TRIM (DRAT / DZAT) Good.
Non-deterministic TRIM Bad.

- Non-deterministic TRIM is an issue for the forensic imaging of drives.
- If a block has been TRIM’d, and each read has the potential to deliver different data, then forensic hashes will potentially never match. (and forensic integrity / chain-of-custody gets muddied)
- Our ‘Ask’ would be to only support DRAT / DZAT (or other emerging deterministic TRIM approaches) with your future designs, OR to at least give the SSD owner the option of forcing DRAT / DZAT- only operation.
Our ‘Asks’, Continued…

New ATA Command support:

- A command to immediately suspend all GC / Erase operations on unmapped sectors (until the next power cycle)
- A command to get the size / quantity of unmapped sectors (OR just the TRIM’d but not yet erased sectors; reading a bunch of erased sectors probably isn’t all that useful)
- A command to read these unmapped sectors from the drive
- A command to retrieve the previous FTL mapping, so we know what LBA that sector used to be mapped to
- Also: A command to halt all background processes whilst forensically imaging / cloning an SSD (until the next power cycle)
Our ‘Asks’, for the F1000 / Gov Crowd:

For our Enterprise customers, who are purchasing company equipment, and trying to maintain effective security policies:

- A command to delay garbage collection, even if the user has deleted and the OS has TRIM’d
- A command to read data that has been TRIM’d, but not yet garbage collected. (In an active internal investigation, this is likely to be data of great interest)
- Note: These commands could be treated like ATA Security, and password-protected by InfoSec or IT (Employees could not turn this feature off)
- Note: These are not ‘Secret’ or encrypted commands. Any user could check to see the status of their SSD’s GC operation.
Thank You!

Jeff Hedlesky
+1 (314) 702-0009
jeff.hedlesky@guidancesoftware.com