Jeff Hedlesky – Forensic Evangelist

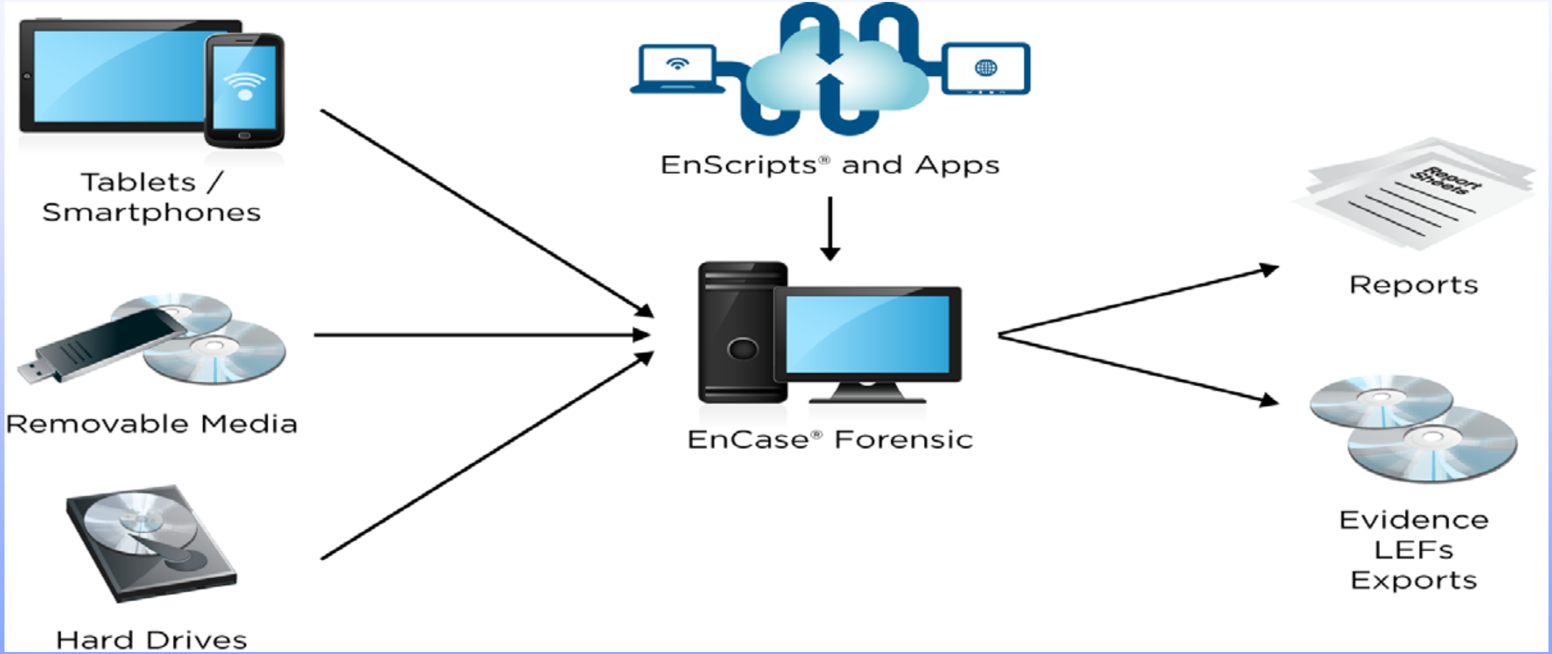
Forensic Business Unit – GSI

Overcoming the Unique Challenges of Digital Forensics

Santa Clara, CA
August 2015

Just a Little About Me…

EnCase Forensic



Just a Few of our Customers…

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

Just a few of our Forensic Hardware Products

T35u

T8u

T3iu

UltraBay 3d™

T35689iu

TD2u

TD3

Santa Clara, CA
August 2015

Digital Forensics – Best Practices

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”

Flash Memory SUMMIT

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- Encrypted or unpublished ATA commands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