

Monday, January 13, 2020

Erase Verification Report

Media ID: 6209730\_A1

Level 1 Erase Verification Result: **Passed**

Level 2 Erase Verification Result: **Passed**

This document contains the summary and detailed report of the Erase Verification Services provided by Ontrack to Stellar Information Technology Pvt. Ltd.

Ontrack Erase Verification Services provide an in-depth analysis and verification of customer provided sanitized media. Using advanced laboratory techniques and state-of-the-art proprietary data recovery tools, Ontrack inspects the media to confirm that the target data has been effectively sanitized to the standards of NIST Special Publication 800-88 Rev. 1.

Specific technical and procedural details are included in the remainder of this document.

### **Ontrack Media Preparation Process**

To verify the effectiveness of the sanitization, Ontrack strongly advises preparation by writing two separate unique byte patterns to all logically accessible blocks of the media to simulate user data. This process ensures the entire media, including over provisioned areas, contain identifiable target data. Once prepared, the sanitization process is performed per the customer's specifications. If preparation is not possible, Ontrack performs verification to align with the NIST 800-88 r1 standard for Cryptographic Erase as outlined in section 4.7.3. This standard suggests searching the entire media for several strings to verify that no file system structures, operating system files, or common files exist.

### **Ontrack Verification Process and Levels of Verification**

**Level 1 Verification** analyzes the contents of all sectors which are accessible to the user via the device interface through a Full Verification method as described in the NIST 800-88 r1 document. Ontrack uses proprietary data recovery software tools to perform this verification.

**Level 2 HDD Verification** analyzes the contents of all sectors that have been remapped by the G-List or hidden in a protected area like HPA/DCO/AMAC.

**Level 2 SSD Verification** analyzes the media at a raw NAND level. The NAND chips are removed from the controller so that all sectors of each NAND chip can be imaged. The images are then analyzed for any remnants of target data that may exist in any portion of the media including user-accessible portions, but also any bad or defective blocks, spare pool areas, or areas otherwise protected by the controller chip or hidden from the standard interface.

The Ontrack® verification is intended to evidence the independent recognition of a well-known industry leader in Erase Verification Services for Stellar Information Technology Pvt. Ltd. This information is provided on an 'as is' basis. Ontrack assumes no direct, indirect or consequential liability to any third party for the information contained in this report. This report does not constitute a recommendation, endorsement or approval of any kind with respect to any product or service, and should not be relied upon as such under any circumstances.

#### **About Ontrack**

Ontrack provides technology-driven services and software to help legal, corporate and government entities as well as consumers manage, recover, search, analyze, and produce data efficiently and cost-effectively. In addition to its award-winning suite of software, Ontrack provides data recovery, data destruction, electronic discovery and document review. For more information about Ontrack and its offerings please visit: [www.ontrack.com](http://www.ontrack.com) or follow @Ontrack on Twitter.

Customer Information			
Company name	Stellar	Service Order Number	6209730_B1
Media Information			
Make / Vendor	Samsung	Model Number	MZ-7LN128D
Serial Number	S1ZUNXAGC05959	Firmware Version	EMT03D0Q
Media Type	SSD	Media Interface	SATA
Capacity	128GB	LBA	250,069,680
Media Preparation			
Tool Used	N/A	Revision / Build	N/A
Pattern Used 1 <sup>st</sup> Pass	STELLAR!	Pattern Used 2 <sup>nd</sup> Pass	None
Sanitization Details			
Method Type	<input checked="" type="checkbox"/> Clear <input type="checkbox"/> Purge <input type="checkbox"/> Damage <input type="checkbox"/> Destruct		
Method Used	<input type="checkbox"/> Degauss <input checked="" type="checkbox"/> Overwrite <input type="checkbox"/> Block Erase <input type="checkbox"/> Crypto Erase <input type="checkbox"/> Other:		
Tool Vendor	BitRaser	Revision/Build	3.0
Erasure Verification Details			
Verification Method	Full	Erasure Pattern	0x00
Percent Matching Pattern	100%	Percent Not Matching Pattern	0%
Was HPA/DCO Identified on Device?			N/A
Data Found	<input type="checkbox"/> File System Structures <input type="checkbox"/> Simulated User Data <input checked="" type="checkbox"/> No Data Found <input type="checkbox"/> Other (See engineer comments)		
Engineer Comments			
<p><b>Level 1 Erasure Verification Result: Passed per NIST 800-88r1 standard</b></p> <p>Stellar prepared the media by writing an ASCII "STELLAR!" pattern to simulate user data and then executed their sanitization process on the above identified media that was sent to Ontrack for erasure verification.</p> <p>The media was then analyzed by Ontrack as part of the erasure verification process. Upon completion of verification, the drive was found to have 100% of the user accessible sectors filled with the 0x00 erasure pattern. No remnants of the ASCII "STELLAR!" prep pattern was found on the disk.</p>			

NAND Removal Details					
Controller Details					
Controller Manufacturer	Samsung	Controller Model	S4LN062X01		
Chip Type #1					
Chip Manufacturer	Samsung	Chip Model	K90KGY8S7C		
Pin layout	BGA316	Number of Chips	1	Chip Capacity	128GB
Chip Type #2					
Chip Manufacturer	N/A	Chip Model	N/A		
Pin layout	N/A	Number of Chips	N/A	Chip Capacity	N/A
Chip Type #3					
Chip Manufacturer	N/A	Chip Model	N/A		
Pin layout	N/A	Number of Chips	N/A	Chip Capacity	N/A
Search Results Breakdown (In Percent of Pages)					
0xFF	0.77%	0x00	<0.1%	Encrypted	99.13%
User Data	0%	File System	0%	SSD System Area	0%
Engineer Comments					
<p><b>Level 2 Erasure Verification Result: <span style="color: green;">Passed per NIST 800-88r1 standard</span></b></p> <p>The raw NAND data was examined and was found to contain the following:</p> <ul style="list-style-type: none"> <li>• 0.77% of the media contained a 0xFF byte pattern</li> <li>• &lt;0.1% of the media contained a 0x00 byte pattern</li> <li>• 99.13% contained what appears to be encrypted data</li> </ul> <p>The device was examined for evidence of standard reversible scrambling methods, such as pseudo-random data generated by a Linear Feedback Shift Register, no evidence was found.</p> <p>The ASCII "STELLAR!" simulated data pattern was not found on the raw images taken from the NAND media. No identifiable user data was found.</p>					

### Media Analyzed – B1

