ASSET DISPOSAL & INFORMATION SECURITY ALLIANCE

Solid State Testing
Blancco Phase 1

Author: Steve Mellings, ADISA
Editor: Professor Andrew Blyth, University of South Wales

Revision 1.3
Date: October 7, 2013
Distribution: Confidential

DISCLAIMER

The content of this document is based on information shared to date and will be subject to change or modification as requirements are amended, clarified or additional requirements are indicated at a later stage. For this reason this document should be viewed as a discussion document with further qualification and refinement required.

Whilst we make every endeavour to ensure the accuracy of the information provided here and that the recommendations are made to the best of our ability they may be subject to inaccuracies or change.

REVISION HISTORY

07/11/2012	Revision 1.0 issued to Jonathan Brew.
16/11/2012	Revision 1.1 issued to Jonathan Brew.
06/12/2012	Revision 1.0 of FINAL Report issued to Jonathan Brew.
11/02/2013	Revision 1.1 of FINAL Report issued to Jonathan Brew.
07/10/2013	Revision 1.3 of FINAL Report issued to Jonathan Brew

Asset Disposal and Information Security Alliance Limited

Phone: 0845 557 7726

Web: www.adisa.org.uk

Registration Number: 07390092
VAT Number: 105 6457 26
Registered Office: Hamilton House, 1 Temple Avenue, London, EC4Y 0HG

Contents

1.0 Executive Summary

This is the final report detailing the findings in relation to the execution of the ADISA Solid State Testing Methodology on Solid State Drives submitted for testing by Blancco in February 2013. The relevant testing methodology v1.0 and claims forms can be reviewed on the ADISA website at http://www.adisa.org.uk/solid-state-sanitisation.

The claim made for each of the drives was:

"The software writes blocks of data to the SSD totalling the full capacity of the device; verification that the blocks have been successfully written is performed; an additional round of writing data blocks to the SSD is performed, again filling the logical capacity of the disk; additional verification is performed along with a firmware level sanitization command"

The testing was structured into 2 phases which are outlined in the methodology.

Phase 0 Summary Results

Phase 0 was discounted from this testing project as SSD have no factory reset capability and phase 0 was designed for use when testing SSD within phones and other devices.

Phase 1 Summary Results

Phase 1 (Test Level 1) replicated an attack on these device being made by an aggressor with capabilities outlined below.

Risk Level	Threat Actor and Compromise Methods	Test Level
1 (Very Low)	Casual or opportunistic threat actor only able to mount high-level non-invasive and non-destructive software attacks utilising freeware, OS tools and COTS products.	1
2 (Low)	Commercial data recovery organisation able to mount non-invasive and non-destructive software attacks and hardware attacks.	1

The Results of Test Phase 1.

Drive	Result
Micron SSD	Pass
Crucial SSD	Pass
Intel SSD	Pass
Kingston SSD	Pass
Samsung SSD	Pass

Pass means that the Blancco tool mitigates the threat posed by the Threat Actors holding the capabilities outlined by risk level 1 and 2.

2.0 Phase 1 Testing.

2.1 Simple Methodology.

This test phase is designed to evaluate the claim made by recreating an attack by a threat adversary utilising standard COTS forensic tools and techniques. (E.g. encase and access data / FTK)

During this phase structured data was written to each of the drives and then each drive was forensically imaged in accordance with legal guidelines. Blancco Software was executed onto the drive and the resulting drive was forensically imaged in accordance with legal guidelines.

The two forensic images were then compared and contrasted to ensure that all structured data had been removed.

For this test there is no tolerance for remnant structured data and the result is a straight Pass or Fail.

2.2 Test Results.

Drive	Result
Micron SSD	Pass
Crucial SSD	Pass
Intel SSD	Pass
Kingston SSD	Pass
Samsung SSD	Pass

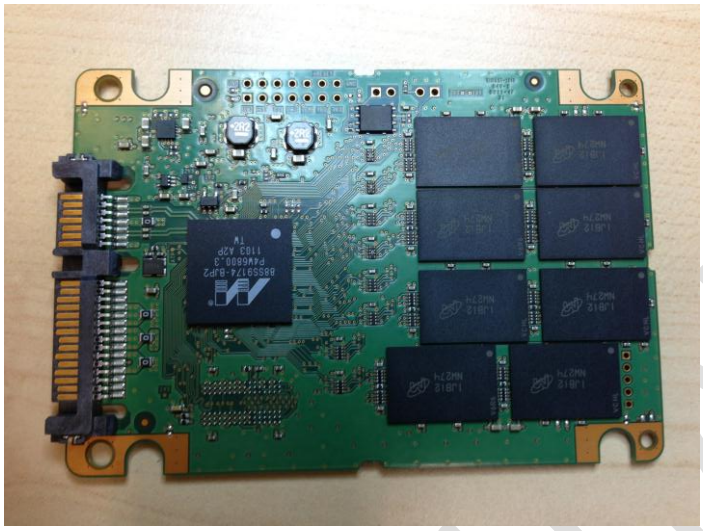
2.3 Observations.

All drives functioned as standard drives and complied with ATA standards.

All of the drives allowed standard forensic imaging tools to be used. This enabled the lab to confirm that Blancco Software wrote to every available logical block address (LBA) on the drive.

3.0 SSD Architecture / Chip Types

3.1 Micron SSD – Claims Test ADPC0001



From the following picture we can observe that:

- The USB controller chip is a Micron 88SS9174-BJP2

- The NAND chips are 1 JB12 NW274

3.2 Crucial SSD – Claims Test ADPC0002

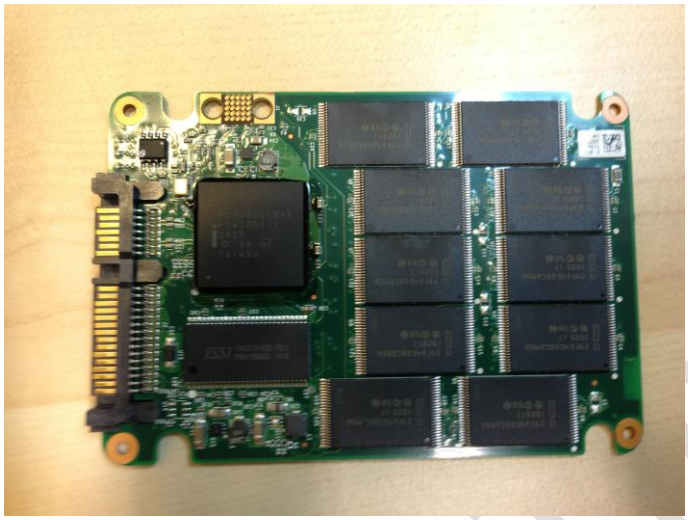
From the following picture we can observe that:

- The USB controller chip is a Micon 88SS9174-BLD2

- The NAND chips are 29F64G08CFACB

3.0 SSD Architecture / Chip Types (cont.)

3.3 Intel SSD – Claims Test ADPC0003

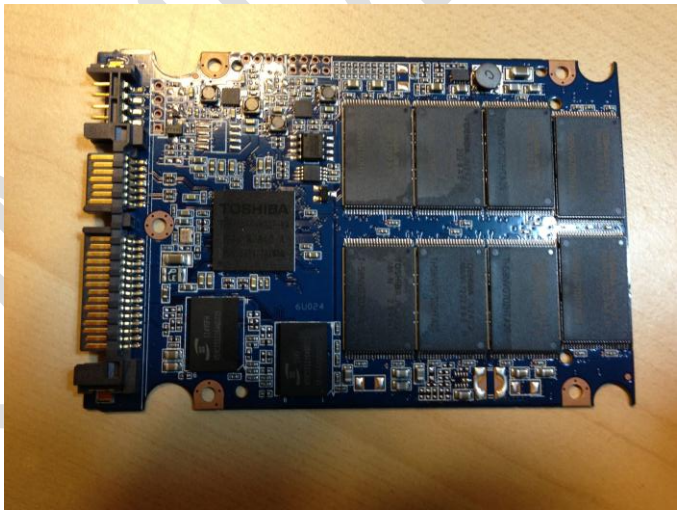


From the following picture we can observe that:

- The USB controller chip is an Intel PO29A5218A

- The NAND chips are 29F64G08CAMDA

3.4 Kingston SSD – Claims Test ADPC0004



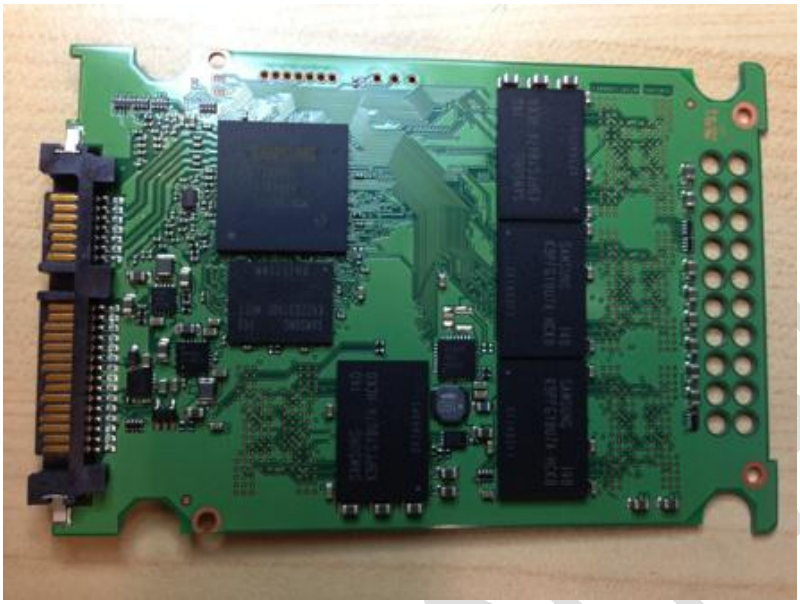
From the following picture we can observe that:

- The USB controller chip is a Toshiba TC58NCF6686DT-BB

- The NAND chips are TH58NVG7D2HTA20

3.0 SSD Architecture / Chip Types (cont.)

3.5 Samsung SSD – Claims Test ADPC0006



From the following picture we can observe that:

- The USB controller chip is a Samsung K9PFGY8U7A-HCKO

- The NAND chips are 54L-J204XQ1-Y040

4.0 Project Summary

SSD architecture is clearly evolving and the use of encryption is now increasing with every device tested implementing NAND cell encryption. This is creating a set of challenges for testing overwriting on this type of product as a result. There are also a wide variety of chip sets being utilised by the manufacturers.

These significant challenges were not altogether unexpected, but to find encryption on all devices tested was. It should be noted that the technology is evolving and therefore the threat landscape is still immature. This will change overtime as standard architectures and approached to SSD manufacturing emerge and SSD technology converges. Forensic capability will also evolve and COTS products will become more capable of mounting forensic attacks on these devices.

To summarise; at this point in time, February 2013, it can be confirmed that the Blancco product submitted for testing can be used on the SSD with chip sets provided to protect against threat capabilities equivalent to test levels 1.