ASSET DISPOSAL & INFORMATION SECURITY ALLIANCE

Product Claims Test
Application Number ADPC0081
iMT Co Ltd

Author: Dr Andrew Blyth PHD,

Revision 1.0
Date: February 21, 2020
Distribution: Confidential

DISCLAIMER

The Product Claims Test is presented as the outcome of a specific test ran in laboratory environment under controlled conditions. Use of this certified product for the purpose of sanitizing data from devices tested needs to be done so after a risk assessment process. ADISA reserves the right to review the validity of this award upon changes in threat landscape.

LIABILITY

ADISA accepts no liability for any claims resulting from the use of the product tested.

REVISION HISTORY

21.02.2020 Revision 1.0 issued to Steve Mellings (ADISA)

Asset Disposal and Information Security Alliance Limited

Phone: 0044 845 557 7726

Web: www.adisa.global
Web: www.adisarc.com

Registration Number: 07390092
Registered Office: 31 Thrales End Business Centre, Thrales End Lane, Harpenden, AL5 3NS

Contents

1.0 Executive Summary

This is the final report detailing the findings in relation to the execution of the ADISA Testing Methodology on Claims Test ADPC0081 submitted by iMT Co Ltd. The claims test was carried out in accordance with ADISA Claims Testing (ACT) v1.0 and supporting document ADISA Testing Methodology v1.0, both of which are available from ADISA.

The claim made for the drive was:

> *"iMT Co Ltd software called iMT-Cleaner 2.0 when used in accordance with user manual iMT-Cleaner 2.0 and using algorithm DoD 5220.22 M, will overwrite all user data on the hardware sample within this test to protect against a forensic attach equivalent to test level 2 of the ADISA Threat Matrix. ". ADPC0081*

A device was submitted as part of this test and this is listed below:

Device	***Test Level***
SanDisk SSD Model: SDSSDA-240G	1 and 2

After testing it is confirmed that the iMT Co Ltd. **claim is true** for the devices tested up to Test Level 1 and 2 results. The device tested was:

- SanDisk SDSSA-240G Model: SDSSA-240G

2.0 Test Level 1 Testing Solid State Drives

2.1 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.

For each computer hard drive device, the following methodology is performed:

1. The device is connected to a target PC and place in a stable state.
2. The applicant software was configured in accordance with the manufacturer's instructions.
3. Structured data, the string "ADISA", was written to every logical block address on the hard drive.
4. The device was then imaged using standard imaging techniques to create a base-line forensic image.
5. The device was then erased using the applicant's software in accordance with the manufacturer's instructions.
6. The device was then analysed use using the following tools to create a second forensic image:
    a. Standard commercial tools and techniques such as Access Data/FTK, Forensic Explorer and Encase.
7. The two forensic images (Stage 4 and Stage 6) were then compared and contrasted to ensure that all structured data had been removed.
    a. For this test, there is no tolerance for remnant structured data and the result is a straight Pass or Fail.

2.2 Test Results.

Test Level 1 Summary Results

Test Level 1 replicated an attack on these devices being made by an aggressor with capabilities outlined below.

Risk Level	Threat Actor and Compromise Methods	Test Level
1 (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. Commercial data recovery organisation able to mount non-invasive and non-destructive software attacks and hardware attacks.	1

The Results of Test Level 1.

Hard Drive/Model	***Result***
SanDisk SSD Model: SDSSDA-240G	PASS

Pass means that the iMT Co Ltd Software iMT-Cleaner 2.0 mitigates the threat posed by the Threat Actors holding the capabilities outlined by Test Level 1 on the tested devices and the claim made can be confirmed. A key element to the claims test is that the software has to be used in accordance with the manufacturers user manual.

3.0 Test Level 2 Testing Solid State Drives

3.1 Methodology.

This test phase is designed to evaluate the claim made by recreating an attack by a threat adversary utilising standard intrusive/destructive testing tools designed to read data directly off the device at the platter/chip level.

For each computer hard drive device, the following methodology is performed:

1. The device is connected to a target PC and place in a stable state.
2. The applicant software was configured in accordance with the manufacturer's instructions.
3. If present on the test device the DCO and HPA are removed.
4. Structured data, the string "ADISA", was written to every logical block address on the hard drive.
5. The device was then imaged using standard imaging techniques to create a base-line forensic image.
6. The device was then erased using the applicant's software in accordance with the manufacturer's instructions.
7. The device was then analysed use the following tools and techniques to create a series of forensic images that are compared and contrasted with the base-line forensic image to ensure that all structured data has been removed. For this test, there is no tolerance for remnant structured data and the result is a straight Pass or Fail.
    a. Software based forensic tools/techniques such as:
        i. Standard commercial tools and techniques such as Access Data/FTK, Forensic Explorer and Encase;
        ii. State of the art data recovery tools such as PC3000 SSD, PC3000 UDMA/SAS;
        iii. Customer designed data recovery software.
    b. Hardware/Chip based forensic tools/techniques such as:
        i. Flash/NAND TSOP/BGA chip readers;
        ii. State of the art data recovery tools such as PC3000 FLASH, PC3000 SSD and Rusolut;
        iii. Hardware debugging techniques such as JTAG, I3C and SPI;
        iv. Customer designed data recovery software/hardware.

3.2 Test Results.

Test Level 2 Summary Results

Test Level 2 replicated an attack on these devices being made by an aggressor with capabilities outlined below.

Risk Level	Threat Actor and Compromise Methods	Test Level
2 (Medium)	Commercial computer forensics organisation able to mount both non-invasive/non-destructive and invasive/non-destructive software and hardware attack, utilising COTS products. Commercial data recovery and computer forensics organisation able to mount both non-invasive/non-destructive and invasive/ non-destructive software and hardware attack, utilising both COTS and bespoke utilities.	2

The Results of Test Level 2.

Hard Drive/Model	*Result*
SanDisk SSD Model: SDSSDA-240G	PASS

Pass means that the iMT Co Ltd Software iMT-Cleaner 2.0 mitigates the threat posed by the Threat Actors holding the capabilities outlined by Test Level 2 on the tested devices and the claim made can be confirmed. A key element to the claims test is that the software has to be used in accordance with the manufacturers user manual.

4.0 Summary and Conclusions.

Claims Test Result: **Pass on all devices tested.**

The device tested passed the claims test as all-forensic data recovery techniques up to and including ADISA Test Level 2 failed to recover any data. The software tested was the iMT Co Ltd Software iMT-Cleaner 2.0

Claims Test Carried Out By: Dr Andrew Blyth, PhD.

Test Facility: ADISA Research Centre

Signature: 

Date: 17.02.2020

