Products Claims Testing

Claims Test ADPC155

SDS Shredder v1.0.0.180

Author: Godfred Badu

Revision 1.0
Date: September 14, 2022
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

02/09/2019 Revision 1.0 issued to Steve Mellings

ADISA Research Centre

Phone: 0044 (1) 1582 361743

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

Registration Number: 07390092
Registered Office: Ground Floor, 5 Kinsbourne Court, Harpenden, AL5 3BL, United Kingdom

Contents

1.0 Executive Summary

This is a preliminary report detailing the findings in relation to the execution of the ADISA Testing Methodology on Claims Test ADPC155 submitted by Roni Karmineke of SoftThinks S.A in September 2022.

The claims test was carried out in accordance with ADISA Claims Testing (ACT) v1.0 and supporting document ADISA Testing Methodology v1.12, both of which are available from ADISA.

The claim made for the drive was:

> *"SoftThinks software SDS Shredder Version - 1.0.0.180, when used in accordance with user manual SoftThinks Adisa User Guide version 22.0.doc will overwrite all user data on the sample media in Section 3 by selecting the appropriate algorithm option as listed in Section 2 to ensure that user data cannot be recovered using forensic techniques aligned ADISA Test Level 2."*

Two devices were submitted as part of this test, and these are listed below:

Device	***Test Level***
Toshiba MK5065GSXF 500GB 2.5" SATA HDD 500GB	2
Intel SSD 320 SSDSA2BW120G3H 2.5" SATA SSD 120GB	2

After testing it is confirmed that the SoftThinks **claim is true** for the devices tested up to Test Level 2 results. Those devices are:

- Toshiba MK5065GSXF 500GB 2.5" SATA HDD 500GB
- Intel SSD 320 SSDSA2BW120G3H 2.5" SATA SSD 120GB

2.0 Test Level 2 Testing Solid State Drive

2.1 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 "ADISAARC", was written to every logical block address on the hard drive and verified using ARC tools.
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 the following tools and techniques to verify and 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. ARC proprietary tools
        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.

2.2 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.

Test Level	Threat Actor	Compromise Methods	Sanitisation Method
1	Casual or opportunistic threat actor only able to mount high-level non-invasive and non-destructive software attacks utilizing freeware, COTS and OS tools.	Keyboard attacks from a motivated individual or professional organisation. Typical attack may be the use of open-source forensic tools or commercial tools.	Aligned to Clear
2	Commercial data recovery and computer forensics organisation able to mount invasive/destructive software and hardware attack, utilising both COTS and bespoke hardware and software.	Laboratory attacks from commercial data recovery experts or specialist forensic scientists. Typical attack may be the use of advanced data recovery software, Chip Readers and protocol decoders. Typical attack would involve analysis of individual hardware components as well as protocol structures.	Aligned to Purge

3.0 Results

Hard Drive/Model	*Result*
Toshiba MK5065GSXF 500GB 2.5” SATA HDD 500GB	PASS
Intel SSD 320 SSDSA2BW120G3H 2.5” SATA SSD 120GB	PASS

Pass means that the software SDS Shredder v1.0.0.180 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.

4.0 Summary and Conclusions.

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

The two devices passed the claims test as all-forensic data recovery techniques up to and including ADISA Test Level 1 and 2 failed to recover any data. The software tested was the SoftThinks Development Suite Shredder v1.0.0.180

Claims Test Carried Out By:

Test Facility: ADISA Research Centre

Signature: 

Date: 12/09/2022

