Products Claims Testing
Claims Test ADPC0069B
BRAINSQUARE

Author: Dr Andrew Blyth

Revision 2.0
Date: January 15, 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

30/09/2019	Revision 1.0 issued to Andrew Blyth
03/01/2020	Revision 2.0 issued to Steve Mellings
14/01/2020	Revision 3.0 issued to Steve Mellings

ADISA ASSET DISPOSAL & INFORMATION SECURITY ALLIANCE

Asset Disposal and Information Security Alliance Limited

Phone: 0044 845 557 7726

Web: www.adisa.global

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

Contents

1.0 Executive Summary

This is a final report detailing the findings in relation to the execution of the ADISA Testing Methodology on Claims Test ADPC0069 submitted by Brainzsquare Inc. This report documents the execution of claim with the revised software. 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:

> *"*Brainzsquare Co's software Secudrive Drive Eraser 6.0, when used in accordance with user guide 1.0, will overwrite using algorithm NIST 800-88-3-Pass, all user data on the sample media to ensure that data cannot be recovered using forensic techniques aligned ADISA Test Level 2.*"*

One device was submitted as part of this test and these are listed below:

Device	***Test Level***
Hitachi 3.5" MHD 500GB / 647466-001	1 and 2

After testing it is confirmed that the ADPC0066 **claim is true** for the devices tested up to Test Level 1 and 2 results. Those devices are:

- Hitachi 3.5" MHD 500GB Model: 647466-001

2.0 Test Level 1 Testing Magnetic Hard 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 the device 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***
Hitachi 3.5" MHD 500GB / 647466-001	PASS

Pass means that the SecuDrive Drive Eraser 6.0 mitigates the threat posed by the Threat Actors holding the capabilities outlined by Test Level 1 on the tested device 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 manufacturer's user manual.

3.0 Test Level 2 Testing Magnetic Hard Drives

3.1 Methodology.

This test phase is designed to evaluate the claim made by recreating an attack by a threat adversary utilising standard Advanced and Invasive 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. PCB analysis for IC identification and validation.
    b. JTAG and SPI data extraction techniques such as Chip-Off and Pin Identification.
    c. Advanced tools and techniques such as PC3000 UDMA, PC3000 SSD and Rusolut.
    d. Hardware based JTAG/SPI debuggers such as J-Link.
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.

3.2 Test Results.

Test Level 2 Summary Results

Test Level 2 replicated an attack on this device 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***
Hitachi 3.5" MHD 500GB / 647466-001	PASS

Pass means that the SecuDrive Drive Eraser 6.0 mitigates the threat posed by the Threat Actors holding the capabilities outlined by Test Level 2 on the tested device 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 manufacturer's user manual.

4.0 Summary and Conclusions.

Claims Test Result: Pass on Test Level 1 and 2

The device tested, Hitachi 3.5" MHD 500GB / 647466-001, passed the claims test for all-forensic data recovery techniques up to and including ADISA Test Level 2. The software tested was SecuDrive Drive Eraser 6.0.

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

Test Facility: ADISA Research Centre

Signature: 

Date: 13th Jan 2020

