Product Claims Test
Application Number ADPC0045
SoftThinks

Author: Professor Andrew Blyth

Revision 1.0
Date: August 13, 2018
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

13.08.2018 Revision 1.0 issued by Andrew Blyth

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: 50 Brook Street, London,
W1K 5DR

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 ADPC0045 submitted by SoftThinks. 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 baseline used to proof/disprove a claim in relation to data erasure/sanitization of mobile phone is that of a factory reset on the device.

The claim made for the drive was:

> *"SoftThinks software SDS v17.0, when used in in accordance with User Manuel 17.0 will overwrite all user data on the MHD provided in this test using Basic 0 algorithm to protect from a forensic attack equivalent to test level 1 of the ADISA threat matrix" – Claim Number ADPC0045.*

In addition, this claims was made for SSD:

> *"SoftThinks software SDS v17.0, when used in in accordance with User Manuel 17.0 will overwrite all user data on the SSD provided in this test using the Secure Erase (NIST 800-88) algorithm to protect from a forensic attack equivalent to test level 1 of the ADISA threat matrix" – Claim Number ADPC0045.*

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

Family	***Model***	***Test Level***
Western Digital 500GB	WD5000BEVT	1
HP S700 Pro	SSD-25SE	1

Table 1 – Devices Tested

After testing it is confirmed that the SoftThinks claim is TRUE for both drives tested.

2.0 Test Level 1 Testing

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. Structured data, the string "ISRG", was written to every logical block address on the hard drive.
2. The device was then imaged using Access Data / FTK to create a base-line forensic image.
3. The device was then erased using the applicant's software in accordance with the manufacturer's instructions.
4. 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 and Encase.
5. The two forensic images (Stage 3 and Stage5) 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 this 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 Level 1

Family	*Model*	Result
Western Digital 500GB	WD5000BEVT	**PASS**
HP S700 Pro	SSD-25SE	**PASS**

- Pass means that SoftThinks software SDS v17.0 mitigates the threat posed by the Threat Actors holding the capabilities outlined by Test Level 1.

3.0 Summary and Conclusions

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

The two drives passed the claims test as all-forensic data recovery techniques up to and including ADISA Test Level 1 failed to recover any data. The software tested was the SoftThinks software SDS v17.0

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

Signature: 

Date: 13th August 2018