Product Claims Testing

Claims Test ADPC0018

SoftThinks S.A.

Author: Professor Andrew Blyth,
University of South Wales

Revision 1.0

Date: 24th April 2015

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

24/04/2015	Revision 1.0 issued to Steve Mellings.
27/04/2015	Revision 1.0p issued to Laurent Kitzinger

ADISA ASSET DISPOSAL & INFORMATION SECURITY ALLIANCE

Asset Disposal and Information Security Alliance Limited

Phone: 0044 845 557 7726
Web: www.adisa.org.uk
Registration Number: 07390092
Registered Office: Hamilton House, 1 Temple Avenue, London, EC4Y 0HG

University of South Wales Prifysgol De Cymru

University of South Wales
Phone: 0044 845 576 0101
Web: www.southwales.ac.uk

Contents

1.0 Executive Summary 4

2.0 Test Level 1 5

2.1 Method 5

2.2 Results 5

3.0 Summary and Conclusions 6

Appendix 1. 0 The ADISA Threat Matrix. 7

1.0 Executive Summary

This report documents the findings of a forensic test that was conduction on behalf of ADISA on the 24th April 2015. The target of the test was the SoftThinks S.A. product and it was conducted in accordance with the ADISA Claims Test Methodology. The claim made by SoftThinks, is that:

> *"*SoftThinks software called SDS, when used in accordance with the User Manual will overwrite all available data on the SSD provided and also the MHD provided within this test to protect from a forensic attack equivalent to test level 1 of the ADISA threat matrix*."* – *Claim Number ADPC0018.*

The subject of the tests was one specified soild state computer hard drive (SSD) and one specified magnetic hard drive. (MHD)

Manufacturer	***Model***	***Model No***	***Capacity***
Samsung	Samsung SSD 850 EVO	MZ-75E500	500GB
Western Digital	WD Blue 500Gb	WD5000AAKX	500GB

After testing it is confirmed that the SoftThinks S.A. claim is true for all drives tested up to Test Level 1.

2.0 Test Level 1

2.1 Method

The basic test method for ADISA Test Level 1 is outlined below:

- The device is first placed into a forensically stable state.
- Structured data is placed on the drive in a forensically sound manner.
- The SoftThinks S.A. product is executed in accordance with the standard operational guidance given in the user manual.
- Forensic tools to replicate the capabilitiy specified in accordance to the ADISA test level 1 are applied to the drive in an attempt to recover data.
- An image of the contents of the device is taken and examined for the presence of the structured data.

2.2 Results

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

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

The computer hard drives underwent the test method outlined in 2.1 with the following results attributed to the claim being made.

The Results of Test Level 1.

Manufacturer	*Model*	*Model No*	*Result*
Samsung	Samsung SSD 850 EVO	MZ-75E500	Pass
Western Digital	WD Blue 500Gb	WD5000AAKX	Pass

3.0 Summary and Conclusions

All forensic data recovery techniques, up to and including, ADISA Test Level 1 failed to recover any data from the SSD/MHD hard disk drives listed once the SoftThinks S.A. SDS product had been applied to them.

Name: Professor Andrew Blyth, PhD.

Signature: 

Date: 24th April 2015

Appendix 1.0 The ADISA Threat Matrix.

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
3 (Medium)	Commercial computer forensics organisation able to mount both non-invasive/non-destructive and invasive/non-destructive software and hardware attack, utilising COTS products.	2
4 (High)	Commercial data recovery and computer forensics organisation able to mount both non-invasive/non-destructive and invasive/destructive software and hardware attack, utilising both COTS and bespoke utilities.	2
5 (Very High)	Government-sponsored organisations or an organisation with unlimited resources and unlimited time capable of using advanced techniques to mount all types of software and hardware attacks to recover sanitised data.	3