Product Claims Testing

Claims Test ADPC0013

NCS Global

Author: Professor Andrew Blyth,
University of South Wales

Revision 1.0

Date: April 7th 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

24/03/2015 Revision 1.0 issued to Steve Mellings
08/04/2015 Revision 1.0 issued to Shiva Nanda

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

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

> *"The EcoErase v. 4.1.35 software when executed using the EcoSanitize SSD method which uses the 4 x DoD (SSD) option and when used in accordance with best practice mitigates all threat as defined by the ADISA Test Level 1 when deployed on the specified solid state storage media listed below." - Claim Number ADPC0013.*

The subject of the tests were FIVE specified SSD computer hard drives.

Model	***Model No***	***Capacity***
EST	MZ-7PC128D	128 GB
Intel	SSDA2BW160G3D	160 GB
ScanDisk	SD6SP1M-128G-1012	128 GB
Crucial	M4-CT512M4SSD2	512 GB
Dell (Micron)	MTFDDAK512MAM-1K1AB	512 GB

After testing it is confirmed that the NCS Global 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 EcoErase v. 4.1.35 was executed in acordance the standard operational guidance given in the Teraware user manual. The sanitization method used/tested was the *4 x DoD SSD* method.
- Forensic tools to replicate the capabilitiy specified in accordance to the ADISA test levels 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 FIVE SSD 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.

SSD	*Result*
EST - MZ-7PC128D	Pass
Intel - SSDA2BW160G3D	Pass
Scandisk - SD6SP1M-128G-1012	Pass
Crucial - M4-CT512M4SSD2	Pass
Dell (Micron) MTFDDAK512MAM-1K1AB	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 all of the SSD hard disk drives listed once they had had the EcoErase v.4.1.35 data sanitization method (4 x DoD) applied to them.

Name: Professor Andrew Blyth, PhD.

Signature: 

Date: 24th March 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/ non-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