Product Claims Testing
Claims Test ADPC0009
NCS Global

Author: Professor Andrew Blyth,
University of South Wales

Revision 1.3
Date: December 4th 2014
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

04/12/2014	Revision 1.0 issued to Steve Mellings
08/12/2014	Revision 1.1 issued to Steve Mellings
09/12/2014	Revision 1.2 issued to Shiva Nanda
10/12/2014	Revision 1.3 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 5th December 2014. The target of the test was ECO Erase. The test was conducted in accordance with the ADISA Claims Test Methodology. The claim made by NCS Global, is that:ADPC00

> "EcoErase when implemented as per EcoErase Quick Start Guide Revision 2014-08-01, will run an Automated Overwriting Script which will overwrite existing data held on all addressable Logical Block Addresses (0 to Max LBA) plus Device Configuration Overlay, the Host Protected Area and Remapped Sectors on a sample of randomly selected ATA and SCSI electro-magnetic drives from different manufacturers and different generation of disk. " - *Claim Number ADPC0009.*

The subject of the tests were a sample of TEN hard drives.

Five IDE/SATA 3.5"computer hard drives.

Model	***Model No***	***Capacity***
Western Digital	WD5000AAKX-00ERM	500 GB
Seagate Baracuda	ST250824AS	250 GB
Samsung 80 GB	HD082G5	80 GB
Hitachi Deskstar	HDS721010KLA330	1 TB
Western Digital	WD1600AAJS-00L7A	160 GB

Five SCSI computer hard drives.

Model	***Model No***	***Capacity***
IBM DCAS 32160	0010752-9713554747	2.19 GB
HP BD146863B3	B8F73ASM	146.8 GB
Seagate (Cheetah)	ST34501WC	4.3 GB
Compaq BD0186398C	BD0186398C	18.2 GB
Compaq BD01864552	BD01864552	18.2 GB

After testing it is confirmed that the NCS Global claim is true for all drives tested up to Test Level 2.

2.0 Test Level 1 Testing

2.1 Methodology

The basic test methodology is outlined below.

- ADISA Threat Level 1 Test Methodology.
    - The Device is first placed into a forensically stable state.
    - Structured data is placed on the drive in a forensically sound manner.
    - The ECO Erase Appliance was executed in acordance the standard operational guidance given in the user manual. The sanitization method used/tested was the *DOD x4 Over Write* method.
    - Forensic tools such as dd/UNIX and mount/UNIX and, in accordance to the ADISA threat levels 1 are applied to the drive in an attempt to recover data.
    - The contents of downloaded data is examine for the presence of the Structured data.

Five IDE/SATA 3.5" computer hard drives where selected and each drive was forensically wiped multiple times, in accordance with the ACPO forensic guidelines. The makes and models of the five drives are listed below:

Model	***Model No***	***Capacity***
Western Digital	WD5000AAKX-00ERM	500 GB
Seagate Baracuda	ST250824AS	250 GB
Samsung 80 GB	HD082G5	80 GB
Hitachi Deskstar	HDS721010KLA330	1 TB
Western Digital	WD1600AAJS-00L7A	160 GB

Five SCSI computer hard drives where selected and each drive was forensically wiped multiple times, in accordance with the ACPO forensic guidelines. Each hard-drive was wide ultra SCSI. The makes and models of the five drives are listed below:

Model	***Model No***	***Capacity***
IBM DCAS 32160	0010752-9713554747	2.19 GB
HP BD146863B3	B8F73ASM	146.8 GB
Seagate (Cheetah)	ST34501WC	4.3 GB
Compaq BD0186398C	BD0186398C	18.2 GB
Compaq BD01864552	BD01864552	18.2 GB

Upon completion of the sanitization job each hard drive was connected to a forensic analysis workstation and in accordance with the ADISA Threat Matrix, forensic analysis techniques where applied to recover data from the hard-drive.

2.2 Test Results

Test Level 1 replicated an attck on these devices 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 following are the results related to the ADISA threat matrix.

The Results of Test Level 1.

IDE / Sata Magnetic Hard Drive	***Result***
Western Digital - WD5000AAKX-00ERM	Pass
Seagate Baracuda - ST250824AS	Pass
Samsung 80 GB - HD082G5	Pass
Hitachi Deskstar - HDS721010KLA330	Pass
Western Digital - WD1600AAJS-00L7A	Pass
SCSI Magnetic Hard Drive	***Result***
IBM DCAS 32160 - 0010752-9713554747	Pass
HP BD146863B3 - B8F73ASM	Pass
Seagate (Cheetah) - ST34501WC	Pass
Compaq BD0186398C - BD0186398C	Pass
Compaq BD01864552 - BD01864552	Pass

3.0 Test Level 2 Testing

3.1 Methodology

The basic test methodology is outlined below.

- ADISA Threat Level 1/2 Test Methodology.
    - The Device is first placed into a forensically stable state.
    - Structured data is placed on the drive in a forensically sound manner.
    - The ECO Erase Appliance was executed in acordance the standard operational guidance given in the user manual. The sanitization method used/tested was the *DOD x4 Over Write* method.
    - Forensic and Data Recovery tools in accordance to the ADISA threat levels 1 and 2 are applied to the drive in an attempt to recover data.
    - The contents of downloaded data is examine for the presence of the Structured data.

Five IDE/SATA 3.5" computer hard drives where selected and each drive was forensically wiped multiple times, in accordance with the ACPO forensic guidelines. The makes and models of the nine drives are listed below:

Model	***Model No***	***Capacity***
Western Digital	WD5000AAKX-00ERM	500 GB
Seagate Baracuda	ST250824AS	250 GB
Samsung 80 GB	HD082G5	80 GB
Hitachi Deskstar	HDS721010KLA330	1 TB
Western Digital	WD1600AAJS-00L7A	160 GB

Five SCSI computer hard drives where selected and each drive was forensically wiped multiple times, in accordance with the ACPO forensic guidelines. Each hard-drive was wide ultra SCSI. The makes and models of the nine drives are listed below:

Model	***Model No***	***Capacity***
IBM DCAS 32160	0010752-9713554747	2.19 GB
HP BD146863B3	B8F73ASM	146.8 GB
Seagate (Cheetah)	ST34501WC	4.3 GB
Compaq BD0186398C	BD0186398C	18.2 GB
Compaq BD01864552	BD01864552	18.2 GB

3.2 Test Results

Test Level 2 replicated an attck on these devices being made by an aggressor with capabilities outlined below

Risk Level	Threat Actor and Compromise Methods	Test Level
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

The Results of Test Level 2.

IDE / Sata Magnetic Hard Drive	***Result***
Western Digital - WD5000AAKX-00ERM	Pass
Seagate Baracuda - ST250824AS	Pass
Samsung 80 GB - HD082G5	Pass
Hitachi Deskstar - HDS721010KLA330	Pass
Western Digital - WD1600AAJS-00L7A	Pass
SCSI Magnetic Hard Drive	***Result***
IBM DCAS 32160 - 0010752-9713554747	Pass
HP BD146863B3 - B8F73ASM	Pass
Seagate (Cheetah) - ST34501WC	Pass
Compaq BD0186398C - BD0186398C	Pass
Compaq BD01864552 - BD01864552	Pass

4.0 Summary and Conclusions

All forensic data recovery techniques up to, and including, ADISA Test Level 2 failed to recover any data from all of the SATA/SCSI hard disk drives listed once they had had the DOD 4 Over-Write method appliance applied to them via the ECO Erase Appliance.

Name: Professor Andrew Blyth, PhD.

Signature: 

Date: 5th December 2014.

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