ASSET DISPOSAL & INFORMATION SECURITY ALLIANCE

Product Claims Test
Application Number ADPC0073
Jetico Inc Oy.

Author: Dr Andrew Blyth PHD,

Revision 1.0
Date: January 16, 2020
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

02.01.2020 Revision 1.0 issued to Steve Mellings (ADISA) by Dr Andrew Blyth (ADISA)

CONFIDENTIAL

Asset Disposal and Information Security Alliance Limited

Phone: 0044 845 557 7726

Web: www.adisa.global

Registration Number: 07390092

©Copyright ADISA 2020

Contents

1.0 Executive Summary 4
2.0 Test Level 1 Testing 5
3.0 Summary and Conclusions 6

CONFIDENTIAL

©Copyright ADISA 2020

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 ADPC0073 submitted by Jetico Inc Oy. 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:

> *"JETICO software called BCWipe Total WipeOut V.4.1.0, when used in accordance with User Manual included within the software will overwrite using Algorithm 3-Pass US DoD 5220-22M(E) all user data, DCO and HPA, on the sample drives listed within this claim to ensure data cannot be recovered from a forensic attack equivalent to test level 1 of the ADISA threat matrix.." – Claim Number ADPC0073.*

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

Family	***Model***	***Test Level***
SanDisk SSD	SDSSDHII-250G	1
Kingston SSD NOW 300	SV300S37A/240G	1
Hitachi Deskstar MHD	HDS728080PLA380	1
Western Digital MHD	WD10EARX-00N0YB0	1

Table 1 – Devices Tested

After testing it is confirmed that the Jetico Inc Oy claim is true for these four devices tested up to Test Level 1 attacks only.

CONFIDENTIAL

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. 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. The drive is checked for the presence of DCO and HPA. If the DCO/HPA are not represent on the Drive, then they are placed/created on the drive.
4. Structured data, the string "ADISA", was written to every logical block address on the hard drive.
5. The device was then imaged using standard imaging techniques to create a base-line forensic image.
6. The device was then erased using the applicant's software in accordance with the manufacturer's instructions.
7. 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.
8. 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 this 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

Family	***Model***	***Result***
SanDisk SSD	SDSSDHII-250G	Pass
Kingston SSD NOW 300	SV300S37A/240G	Pass
Hitachi Deskstar MHD	HDS728080PLA380	Pass
Western Digital MHD	WD10EARX-00N0YB0	Pass

Pass means that the *JETICO software called BCWipe Total WipeOut V.4.1.0* 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.

©Copyright ADISA 2020

3.0 Summary and Conclusions

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

The device tested 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 *BCWipe Total WipeOut V.4.1.0*

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

Test Facility: ADISA Research Centre

Signature: 

Date: 02.01.2020

CONFIDENTIAL

©Copyright ADISA 2020