University of South Wales
Prifysgol De Cymru

ADISA
ASSET DISPOSAL & INFORMATION SECURITY ALLIANCE

Products Claims Testing
Claims Test ADPC0024
Jetico

Author: Professor Andrew Blyth,
University of South Wales

Revision 1.2
Date: September 6, 2016
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

09/08/2016	Revision 1.0 issued to Steve M
10/08/2016	Revision 1.1 issued to Tommi Rasila
12/08/2016	Revision 1.2 issued to Tommi Rasila

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: 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 is the final report detailing the findings in relation to the execution of the ADISA Testing Methodology on Claims Test ADPC0024 submitted by JETICO in June 2016. 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 v3.0.3 when used in accordance with the User Manual included within the Software, will overwrite the users data (LBA-0 to LBA-MAX), DCO and HPA on the following list of magnetic and solid state drives to protect from forensic attack equivalent to Test Level 1 of the ADISA Threat Matrix. - Claim Number ADPC0024."*

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

Hard Drive/Model	***Drive Type***	***Test Level***
Samsung SSD850 EVO (mSATA) – 120GB	SSD	1
Kingston 240GB SSDNOW 300	SSD	1
Crucial BX200 2.5 Inch SSD 240GB	SSD	1
WD 2.0TB Blue – WD20EZRZ	MHD	1
Seagate Video 3.5 HDD 2TB	MHD	1
Toshiba 2TB HDWD120 High Performance Hard Drive P300	MHD	1

Table 1 – Devices Tested

After testing it is confirmed that the JETICO claim is true for all devices tested up to Test Level 1 results.

2.0 Test Level 1 Testing.

2.1 Simple 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. (e.g. Access Data and EnCase). For each device the following methodology is performed.

1. The JETICO BCWipe Total WipeOut v3.0.3 was configured in accordance with the manufacturers instructions.
    a. The following wipe algorithm was executed
2. The following data is placed on every logical block address (LBA-0 to LBA-MAX):
    a. ISRG.
3. The device was then erased using JETICO BCWipe Total WipeOut v3.0.3 in acceptance with the manufactures instructions.
    a. The Erasure Algorithm used is: 3-Pass US DOD 5220-22m(e)
4. The device was then imaged using Access Data to create the test image.
5. The test image was then forensically analysed using FTK version 6.0.3.5

2.2 Test Results.

Test Level 1 Summary Results

Test Level 1 replicated an attack on these 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.

Hard Drive/Model	*Drive Type*	*Result*
Samsung SSD850 EVO (mSATA) – 120GB	SSD	PASS
Kingston 240GB SSDNOW 300	SSD	PASS
Crucial BX200 2.5 Inch SSD 240GB	SSD	PASS
WD 2.0TB Blue – WD20EZRZ	MHD	PASS
Seagate Video 3.5 HDD 2TB	MHD	PASS
Toshiba 2TB HDWD120 High Performance Hard Drive P300	MHD	PASS

Pass means that the JETICO BCWipe Total WipeOut v3.0.3 mitigates the threat posed by the Threat Actors holding the capabilities outlined by Test Level 1 on the tested devices and the claim made can be confirmed.

3.0 Summary and Conclusions.

Claims Test Result: Pass on all devices tested.

All six devices 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 the JETICO BCWipe Total WipeOut v3.0.3.

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

Test Facility: University of South Wales

Signature: 

Date: 9th August 2016

Appendix A Claims Test Application Form

ASSET DISPOSAL & INFORMATION SECURITY ALLIANCE

Claims Testing Application Form

Form Number ADPC00024

Section 1 – Applicant Information

Company Name: Jetico Inc. Oy
Address: Tekniikantie 14, 02150 Espoo, Finland

General Contact
Name: Tommi Rasila
Phone: +358 925 173 030
Mobile: +358 407 508 158
E-Mail: Tommi@jetico.com

Section 2 – Applicant Software Information

Manufacturer Jetico Inc. Oy
Version of software BCWipe Total WipeOut v. 3.03

Background (Explanation of the company and software)

Jetico is a data protection company based in Espoo, Finland. Its two product lines consist of products for encryption and wiping, used by small and large companies, public entities and private individuals.

Technical / physical architecture of claims test applicant software.

The software is used to create the wiping agent that can be written to USB stick, optical disc or an ISO image or alternatively loaded from a server. The agent is used to boot the target HW on which the SSD discs, rotating hard drives or removable media can be erased. The agent has its own operating system based on Linux kernel modules and can thus be used for targets systems regardless of their native operating system (DOS, Windows, Linux, Mac, Sparc).

Best practice usage guide for usage of software being tested. (Please enclose any manuals)

BCWipe Total WipeOut is delivered in three different configurations: Home Edition in which Sparc capabilities are blocked, Enterprise Edition with unlimited use that allows creating USB, optical or ISO images and Enterprise Server which has additional capability of loading the wiping agent over the network from server. All these have identical wiping modules and provide similar wiping agents For the ease of evaluation Enterprise Edition should be used.

User manual can be found here: https://www.jetico.com/web_help/bcwipe_total_wipeout_enterprise/

The recommended wiping schemes for testing purposes are 3-pass US DoE M 205.1-2 with 'Replace the last wiping pass with ATA ERASE command' for SSD and US DoD (7-pass) for MHD.

Host Information for claims test applicant software to run on. To be shipped by test claimant.

No special hardware is needed in running the software.

Section 3 – Test Hardware Information

Standard hard drives of different sizes from various manufacturer should be used. Host systems can be any Intel-based computers apart from ARM systems: x86 (BIOS/EFI), x64 (BIOS/EFI, including Intel-based Mac), Itanium and 64-bit SPARC.

Section 4 – The Claim

JETICO software called BCWipe Total WipeOut v. 3.0.3, when used in accordance with the User Manual included within the software, will overwrite the user data (LBA-0 to LBA-MAX), DCO and HPA on the following list of magnetic and solid state hard drives from a forensic attack equivalent to test level 1 of the ADISA threat matrix.

Toshiba 3,5 MHD, Seagate 3,5 MHD, WD 2,5 MDH

Crucial 2,5 SSD, Kingston 2,5 SSD, Samsung mSATA SSD

Acceptance

Claim Technical Contact at applicant.

Name: Alexey Boltunov
Phone: _____
Mobile: _____
E-Mail: _____

I, Tommi Rasila of Jetico Inc. Oy confirm that the information outlined in this document is an accurate and true reflection of the claims made by our product wishing to undergo the ADISA testing method.

Signed on behalf of Jetico Inc. Oy

SIGNED:

NAME: Tommi Rasila

TITLE: Founder and Chairman

DATE: 29th May 2016

Claim Accepted by:

Signed on behalf of University of South Wales

SIGNED:

NAME: Andrew Blyth

TITLE: Professor

DATE:

Signed on behalf of ADISA

SIGNED:

NAME: Steve Mellings

TITLE: Director

DATE: