University of South Wales
Prifysgol De Cymru

ADISA
ASSET DISPOSAL & INFORMATION SECURITY ALLIANCE

Products Claims Testing
Claims Test ADPC0028
ITRenew – Phase 2 – Magnetic Hard Drives

Author: Professor Andrew Blyth,
University of South Wales

Revision 1.0
Date: August 3, 2018
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

12/04/2017 Revision 1.0 issued to Steve Mellings

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: 50 Brook Street, Mayfair, London, W1K 5DR

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 ADPC0028 submitted by ITRenew in December 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:

> *"The Teraware Digital Asset Disposition Platform version 3.0 can, using NIST 800-88 (1-pass) sanitization method and by following instructions within Teraware User Guide v 1.0, forensically sanitise the devices supplied within this claim removing all user data such that it is unrecoverable using techniques aligned to ADISA 2 as outlined in section 3. Upon successful sanitisation, it produces a Certificate of Sanitisation to validate this."*

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

VENDOR	FAMILY	MODEL	CAPACITY	INTERFACE	RISK LEVEL	TEST LEVEL	CERT LISTING NAME
Seagate	Archive HDD	ST8000AS0002	8TB	SATA-HDD	1,2,3,4	2	Seagate Archive SMR 8TB 4K SATA-HDD
HGST	Ultrastar He10	HUH721010AL4200	10TB	SAS-HDD	1,2,3,4	2	HGST Ultrastar He10 10TB SAS-HDD

Table 1 – Devices Tested

After testing it is confirmed that the ITRenew claim is true for the devices tested up to Test Level 2 results. Those devices are:

- Seagate Archive HDD – Model ST8000AS0002
- HGST Ultrastar He10 – Model HUH721010AL4200

2.0 Test Level 1 Testing Magnetic Hard Drive

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.

For each computer hard drive (Seagate and Samsung) device the following methodology is performed:

1. The device is connected to a target PC and place in a stable state.
2. Structured data, the string "ISRG", was written to every logical block address on the hard drive.
3. The device was then imaged using Access Data/FTK to create a base-line forensic image.
4. The device was then erased using the IT Renew Teraware Digital Asset Disposition Platform v3.0 in accordance with the manufacturer's instructions.
5. 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 and ENCase.
6. The two forensic images (Stage 3 and Stage5) 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 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 Results of Test Level 1

Hard Drive/Model	***Result***
Seagate Archive HDD – Model ST8000AS0002	PASS
HGST Ultrastar He10 – Model HUH721010AL4200	PASS

A Pass means that Teraware Digital Asset Disposition Platform version 3.0 can, using the NIST 800-88 sanitisation method and by following instructions within Teraware User Guide v 1.0 mitigate 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 Test Level 2 Testing Magnetic Hard Drive

3.1 Simple Methodology.

This test phase is designed to evaluate the claim made by recreating an attack by a threat adversary utilising standard intrusive/destructive testing tools designed to read data directly off the device at the platter/chip level.

For each computer hard drive (Seagate and Samsung) device the following methodology is performed:

1. The device is connected to a target PC and place in a stable state.
2. Structured data, the string "ISRG", was written to every logical block address on the hard drive.
3. The device was then imaged using Access Data/FTK to create a base-line forensic image.
4. The device was then erased using the IT Renew Teraware Digital Asset Disposition Platform v3.0 in accordance with the manufacturer's instructions.
5. The device was then analysed use the following tools and techniques to create a series of forensic images that are compared and contrasted with the base-line forensic image to ensure that all structured data has been removed. For this test there is no tolerance for remnant structured data and the result is a straight Pass or Fail.
    a. Software based forensic tools/techniques such as:
        i. Standard commercial tools and techniques such as Access Data/FTK and ENCase
        ii. State of the art and customer designed data recovery software;
    b. Hardware/Chip based forensic tools/techniques such as:
        i. Flash and Cache chips used by the PCB to control the HDD.

3.2 Test Results.

Test Level 2 Summary Results

Test Level 2 replicated an attack 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.

Hard Drive/Model	*Result*
Seagate Archive HDD – Model ST8000AS0002	PASS
HGST Ultrastar He10 – Model HUH721010AL4200	PASS

Pass means that Teraware Digital Asset Disposition Platform version 3.0 can, using the NIST 800-88 sanitisation method and by following instructions within Teraware User Guide v 1.0 mitigate the threat posed by the Threat Actors holding the capabilities outlined by Test Level 2 on the tested devices and the claim made can be confirmed.

4.0 Summary and Conclusions

Claims Test Result: **Pass on all devices tested against the test levels submitted.**

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

Test Facility: University of South Wales

Signature: 

Date: 15th April 2017

Appendix A Claims Test Application Form (copy)

ASSET DISPOSAL & INFORMATION SECURITY ALLIANCE

Form Number ADPC0028

Section 1 – Applicant Information

Company Name: **ITRenew Inc.**
Address: 8356 Central Avenue, Newark, CA 9560

General Contact
Name: Matt Mickelson
Phone: 001 408 799 4118
Mobile: 001 408 799 4118
E-Mail: matt.mickelson@itrenew.com

Section 2 – Applicant Software Information

Manufacturer **ITRenew Inc.**
Version of software **Teraware v3.00**

Technical / physical architecture of claims test applicant software.

The Teraware platform discovers the target device and capabilities to formulate a multi-step, forensic-level, sanitization protocol for a hard disk drive based on the guidelines set forth on the NIST 800-88 guidelines for media sanitization. The basic guidelines reference a full overwriting pass across all user LBAs.
STEP 1: OVERWRITE PASS – Teraware shall enumerate all logical block addresses (LBAs) with a 00h pattern.
STEP 2: MEDIA VERIFICATION – Teraware performs a full verification of all LBAs of the device to confirm the absence of any user data or unstructured data patterns using a reference pattern of 00h.

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

Teraware_User_Guide_v1.0.pdf

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

1x Teraware Appliance (contains the application and deployment system)
1x Dell CS24-TY server w/LSI SAS 9211-4i HBA (processing station)
Teraware User Guide

Section 3 – Test Hardware Information

VENDER	FAMILY	MODEL	CAPACITY	INTERFACE	RISK LEVEL	TEST LEVEL	CERT LISTING NAME
Seagate	Archive HDD	ST8000AS0002	8TB	SATA-HDD	1,2,3,4	2	Seagate Archive SMR 8TB 4K SATA-HDD
HGST	Ultrastar He10	HUH721010AL4200	10TB	SAS-HDD	1,2,3,4	2	HGST Ultrastar He10 10TB SAS-HDD

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

Section 4 – The Claim

The Teraware Digital Asset Disposition Platform version 3.0 can, using NIST 800-88 (1-pass) sanitization method and by following instructions within Teraware User Guide v 1.0, forensically sanitise the devices supplied within this claim removing all user data such that it is unrecoverable using techniques aligned to ADISA Risk Levels 1 or 2 as outlined in section 3. Upon successful sanitisation, it produces a Certificate of Sanitisation to validate this.

Claim Technical Contact at applicant.

Name: Matt Mickelson

Phone: 408-799-4118

Mobile: 408-799-4118

E-mail: matt.mickelson@itrenew.com

Acceptance

I, Matt Mickelson of ITRenew 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 ITRenew

SIGNED:

NAME: Matt Mickelson

TITLE: Director, Product Management

DATE: 12/09/2016

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: