University of South Wales
Prifysgol De Cymru

ADISA
ASSET DISPOSAL & INFORMATION SECURITY ALLIANCE

Products Claims Testing
Claims Test ADPC0042
eDR

Author: Professor Andrew Blyth,
University of South Wales

Revision 1.0
Date: February 27, 2018
Distribution: Confidential

DISCLAIMER

The Product Claims Test is presented as the outcome of a specific test ran in laboratory environment under controlled conditions. Use of this certified product for the purpose of sanitizing data from devices tested needs to be done so after a risk assessment process. ADISA reserves the right to review the validity of this award upon changes in threat landscape.

LIABILITY

ADISA accepts no liability for any claims resulting from the use of the product tested.

REVISION HISTORY

23/02/2018 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, London, W1K 5DR, United Kingdom

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 a preliminary report detailing the findings in relation to the execution of the ADISA Testing Methodology on Claims Test ADPC0042 submitted by eDR Europe in February 2018.

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 magnetic hard drive and solid-state drive was:

> *"A hard disk drive will be destroyed in less than 15 seconds to the extent that any data contained on it is unrecoverable (Risk Level 4 on the Threat Matrix).*
>
> *A solid state drive will be destroyed in less than 10 seconds such that each NAND cell is physically damaged to the extent that any data containing on it is unrecoverable (Risk level 4 on the Threat Matrix).- Claim Number ADPC0042."*

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

Device	***Test Level***
Samsung SSD – P/N 717353-002	1 and 2
DeskStar HDD – P/N 0A33535	1 and 2

After testing it is confirmed that the eDR **claim is true** for the devices tested up to Test Level 1 and 2 results. Those devices are:

- Samsung SSD – P/N 717353-002
- DeskStar HDD – P/N 0A33535

2.0 Test Level 1 Testing Solid State and Electromagnetic Drives

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. Structured data, the string "ISRG", was written to every logical block address on the hard drive.
2. The device was then imaged using Access Data / FTK to create a base-line forensic image.
3. The Device was then destroyed using the eDR crusher, in accordance with the manufacturer's instructions.
4. We then attempt analyse the device use using the following tools to create a second forensic image:
    a. Standard commercial tools and techniques such as Access Data/FTK and Encase.
5. Where possible 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***
Samsung SSD – P/N 717353-002	PASS
DeskStar HDD – P/N 0A33535	PASS

Pass means that eDR Disk Crusher 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. A key element to the claims test is that the software has to be used in accordance with the manufacturers user manual.

3.0 Test Level 2 Testing Solid State and Electromagnetic Drives

3.1 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. Cellebrite). For each device, the following methodology is performed.

1. Structured data, the string "ISRG", was written to every logical block address on the hard drive.
2. The device was then imaged using Access Data / FTK to create a base-line forensic image.
3. The Device was then destroyed using the eDR crusher, in accordance with the manufacturer's instructions.
4. NAND chips and Disk patters are then extracted from the crusher drive and via hard attack methods data is extracted. Key technologies such in Level 2 testing include a Magnetic Force Microscope, and IC Test/debug test Rigs.
5. If stage 4 results in any meaningful data being extracted then then claim is said to have failed level 2 testing

3.2 Test Results.

Test Level 2 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.	2
2 (Low)	Commercial data recovery organisation able to mount non-invasive and non-destructive software attacks and hardware attacks.	2

The Results of Test Level 2

Hard Drive/Model	***Result***
Samsung SSD – P/N 717353-002	PASS
DeskStar HDD – P/N 0A33535	PASS

Pass means that the eDR Disk Crusher mitigates 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.

The two devices passed the claims test as all-forensic data recovery techniques up to and including ADISA Test Level 1 and 2 failed to recover any data. The hardware device tested was the eDR Disk Crusher.

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

Test Facility: University of South Wales

Signature: 

Date: 23rd February 2018