Standard Testing Report: Shredding Solution
Application Number: ADPC141

Author: Godfred Badu
ADISA Research Centre

Revision 1.0
Date: April 25, 2022
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

25.04.2022 Revision 1.0 issued to Helen Fouche

ADISA Research Centre

Phone: 0044 (1) 1582 361743

Web: www.adisa.global
Web: www.adisarc.com

Registration Number: 07390092
Registered Office: Ground Floor, 5 Kinsbourne Court, Harpenden, AL5 3BL, United Kingdom

Contents

1.0 Executive Summary

This report details the findings in relation to the execution of the ADISA Testing Methodology on Product Claims Test *ADPC141 – eDR Europe*.

On the 29th *of March 2022, eDR Europe* submitted a Product Claims Test application for their shredding solution ***eDR Hard Disk Crusher*** to the ADISA Forensic Laboratory to conduct a Product Claims Test in a controlled lab environment on two storage drives. The claims test was carried out in accordance with ADISA Claims Testing (ACT) v1.0 and supporting document ADISA Testing Methodology v1.8, both of which are available from ADISA.

The claim made for the drives were:

> *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 2 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 contained on it is unrecoverable (Risk Level 2 on the Threat Matrix).*

After testing, it was confirmed that the ADPC141 **claim is true** for the devices tested up to Test Level 1 and Level 2.

1.1 Hardware Submitted

eDR Europe submitted *eDR Hard Disk Crusher* solution to be tested under the premise that when executed on storage media listed in section 1.2, no data can be recover while using Level 1 and Level 2 forensic attacks. Details of the hardware used for testing is in table below:

Manufacturer	***Model Number***	***Serial Number***
eDR	HDC-VX	10145

1.2 Test Media used in test

The solution is executed on the device specified in section 3 of the Claims Testing Application Form completed and signed by the manufacturer whilst following the user manual. The details of the devices used as part of this test are listed below:

Make	***Model***	***Serial Number***	***Media Interface Type***
Ortial	OC-150-128	97236	SATA SSD
Western Digital	WD2500AAKX-07U6AA0	WCC2F2134853	SATA HDD

2.0 Testing for Destruction Solutions (MHD and SSD)

2.1 Test Methodology – Phase 1

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 device, the following methodology is performed:

1. The device was connected to a target PC and placed in a stable state.
2. If present on the test device, DCO and HPA were removed.
3. Structured data, the string "ADISA", was written to every logical block address on the drive.
4. The device was then imaged using standard imaging techniques to create a base-line forensic image.
5. Each drive to be shredded is then placed in an antistatic bag and securely stored forensic bag. The bag is signed and sealed by Analyst.
6. The drives are transported to customer site to undertake physical destruction process and the process is carried out under the supervision of the Analyst.
7. The device being submitted for test must first be inspected by the forensic analyst. They must be clear of any previous particulate and both the feed hopper and particulate bin must be clean. The screen must be inspected and have the aperture verified by the forensic analyst before the test starts. The user manual will be discussed with the applicant's operator and the forensic analyst will verify that the process is carried out as per the manufacturer's manual.
8. When ready the applicant's operator will destroy each drive in turn in accordance with the user manual and the particulate of each drive will be captured for recovery by the forensic analyst.
9. Particulates were captured and placed into an antistatic bag and labelled with the specific drive which was shredded.
10. On return to the lab, the forensic analyst will attempt to find a way of connecting particulate to a forensic PC workstation running Access Data / FTK via a hardware write blocker. If no connection is possible Test Level 1 is a pass.
11. If a connection is possible the device is then forensically imaged using Access Data / FTK to produce a evaluate image. The device is imaged, and saved, in a RAW DD format. T
12. The Images are compared to identify if any of the test data contained in the baseline is present on the second image.
13. Standard commercial tools and techniques such as Access Data/FTK and Encase are used to examine the two forensic images.
14. If no data can be recovered Test Level 1 is a pass.

2.2 Test Method – Phase 2

If Stage 10 is successful, i.e. the normal user connection can be made then the following process takes place:

1. 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, Forensic Explorer and Encase;

ii. State of the art data recovery tools such as PC3000 SSD, PC3000 UDMA/SAS;
iii. Customer designed data recovery software.

b. Hardware/Chip based forensic tools/techniques such as:
i. Flash/NAND TSOP/BGA chip readers;
ii. State of the art data recovery tools such as PC3000 FLASH, PC3000 SSD and Rusolut;
iii. Hardware debugging techniques such as JTAG, I3C and SPI;
iv. Customer designed data recovery software/hardware.

2. If no data can be recovered Test Level 2 is a pass.

If Stage 10 is NOT successful, i.e. the normal user connection cannot be made then the following process takes place:

1. Forensic Analyst inspects particulate and assesses whether there are any NAND cells from SSD or sections of platter which could be attacked using Test Level 2 capabilities can be recovered.
2. If there are complete NAND Cells Hardware/Chip based forensic tools/techniques such as:
i. Flash/NAND TSOP/BGA chip readers.
ii. State of the art data recovery tools such as PC3000 FLASH, PC3000 SSD and Rusolut.
iii. Hardware debugging techniques such as JTAG, I3C and SPI.
iv. Customer designed data recovery software/hardware.
2. If no data can be recovered Test Level 2 is a pass.

2.2 Test Level

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
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
2 (Medium)	Commercial computer forensics organisation able to mount both non-invasive/non-destructive and invasive/non-destructive software and hardware attack, utilising COTS products. 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

3.0 Summary of Findings

3.1 Test Level 1 Results

The table below shows the findings of the Claims Test carried out on the device listed.

Device Description	*Media Interface Type*	*Test Result*
Ortial OC-150-128	SATA SSD	PASS
Western Digital WD2500AAKX	SATA HDD	PASS

3.2 Test Level 2 Results

After following the method listed in 2.2 the findings were;

Device Description	*Media Interface Type*	*Test Result*
Ortial OC-150-128	SATA SSD	PASS
Western Digital WD2500AAKX	SATA HDD	PASS

3.3 Software Used

The details of forensic software used during the testing process are listed in the table below:

Name	*Version Number*	*What it was used for*
FTK Imager	4.5.0.3	Forensic Imaging
HexEdit	19.6	Data verification

3.4 Hardware Used

The details of forensic software used during the testing process is listed in the table below:

Make	*Model Number*	*Serial Number*	*OS Version*	*What it was used for*
HP	Prodesk 600	CZC5332W9T	Windows 10 Pro	Workstation

4.0 Conclusions

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

The hard disk crusher presented passed the claims test as all forensic data recovery techniques up to and including ADISA Test Level 2 failed to recover any data.

Claims Test Carried Out By: Godfred Badu

Test Facility: ADISA Research Centre

Signature: 

Date: 25th April 2022