Standard Testing Report: Shredding Solution
Application Number: ADPC130A

Author: Godfred Badu
ADISA Research Centre

Revision 1.0
Date: January 28, 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

28/01/2022 Revision 1.0 issued to Ross Hayburn

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 4
1.1 Test Objectives 4
1.2 Test Media used in test 4
2.0 Testing for Shredding Solutions (MHD and SSD) 5
2.1 Test Method for Objective 1 – Level 1 5
2.2 Test Method for Objective 1 – Level 2 5
2.3 Test Method for Objective 2 6
3.0 Summary of Findings 7
3.1 Objective 1 Test Level 1 7
3.2 Objective 1 Test Level 2 7
3.3 Objective 2 7
4.0 Conclusions 8
Appendix A ISO 21964-2 Shred particle size 9
Appendix B Table of Shred Measurement 10
Appendix C Graph of Shred Measurement 11

1.0 Executive Summary

This report details the findings in relation to the execution of the ADISA Testing Methodology on Product Claims Test *ADPC130A – Ulster Shredders*.

On the *15th of December 2021, Ulster Shredders* submitted a Product Claims Test application for their shredding solution ***U-15 Shredder*** 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 v1.7, both of which are available from ADISA.

The claim made for the drives were:

> *Ulster Shredder U15 when used in accordance with User Manual U15 Standard, and using a 15mm screen, will destroy SSD and MHD, such that forensic techniques aligned to Test Level 2 cannot recover data and compliance to ISO 21964 E3 (SSD) and H5 (MHD) is confirmed.*

After testing, it was confirmed that the ADPC130A **claim is true** for the devices tested up to Test Level 1 and Level 2.

1.1 Test Objectives

Ulster Shredders submitted *U-15 Shredder* solution to be tested against two test objectives:

First that no data can be recover while using Level 1 and Level 2 forensic attacks.

Secondly, that the shred particulate meets the requirements laid out in ISO 21964 E3 (for SSD) and H5 (for magnetic hard drives. (See Appendix A)

Details of the hardware used for testing is in table below:

Manufacturer	***Model Number***	***Screen Size (mm)***
Ulster Shredders	U-15	15

1.2 Test Media used in test

Make	***Model***	***Serial Number***	***Media Interface Type***
Seagate	ST3500413AS	5VMX04F9	SATA HDD
Intel	SSD DC 5320	PHDV65330A0N150MGN	SATA SSD

2.0 Testing for Shredding Solutions (MHD and SSD)

2.1 Test Method for Objective 1 – Level 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 shredding process. Shredding is done under the supervision of the Analyst.
7. The shredders 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 shred 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. Shred 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 for Objective 1 – Level 2

If Stage 10 is successful, ie 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, ie 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.

2.3 Test Method for Objective 2

The requirements for ISO 21964 output are listed in Appendix A. To verify this the following method was followed:

Stages 1 to 9 are carried out as per 2.1.

1. Each forensic bag of test particulate was weighed in digital scales. 10% of the particulate was separated to be assessed as the output sample.
2. Test particulate is then measured using digital callipers with the longest and shortest dimensions recorded.
3. The average dimension was used to determine the typical output from the shred.

3.0 Summary of Findings

3.1 Objective 1 Test Level 1

After following the method listed in 2.1 the findings were

Device Description	*Media Interface Type*	*Test Result*
Seagate ST3500413AS	SATA HDD	PASS
Intel SSD DC 5320	SATA SSD	PASS

3.2 Objective 1 Test Level 2

After following the method listed in 2.1 the findings were

Device Description	*Media Interface Type*	*Test Result*
Seagate ST3500413AS	SATA HDD	PASS
Intel SSD DC 5320	SATA SSD	PASS

3.3 Objective 2

The requirements are listed in Appendix A and the findings listed in Appendix B.

U-15	*Length (mm)*	*Width (mm)*
Max	28.03	13.61
Min	6.10	3.20
Total of 10%	512.34	275.19
Average	12.81	6.88
Average mm2	88.13mm^2	

Media	*Requirement*	*Test Result*
SSD	Medium broken into pieces.	PASS
SSD	Particle size less than or equal to 160mm^2	PASS
SSD	Less than 10% can exceed 480mm^2 in size	PASS
MHD	Data Carrier Broken into several pieces and deformed	PASS
MHD	Particle size less than or equal to 320mm^2	PASS
MHD	Less than 10% can exceed 3800mm^2 in size	PASS

4.0 Conclusions

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

The shredder presented passed the claims test as all-forensic data recovery techniques up to and including ADISA Test Level 2 failed to recover any data. We can also confirm compliance to the requirements of E3 for SSD and H5 for MHD.

The shredder tested was the Ulster Shredder U15 from the Confidential Destruction Range using a 15mm screen.

Claims Test Carried Out By: Godfred Badu

Test Facility: ADISA Research Centre

Signature: 

Date: 28th January 2022

Appendix A ISO 21964-2 Shred particle size.

Table 5 – Information on hard drives with magnetic data carriers

Information on hard drives with magnetic data carriers		
Security level	**Condition, shape and size after destruction**	**Tolerance**
H-1	Hard drive physically/electronically unusable	
H-2	Data carrier damaged	
H-3	Data carrier deformed	
H-4	Data carrier broken into several pieces and deformed and Particle size ≤ 2 000 mm^2	10% of the material may exceed the specified particle size, but shall not be more than 3 800 mm^2 in size.
H-5	Data carrier broken into several pieces and deformed and Particle size ≤ 320 mm^2	10% of the material may exceed the specified particle size, but shall not be more than 800 mm^2 in size.

Table 6 – Information on electronic data carriers

Information on electronic data carriers (solid-state drives) e.g.: memory sticks, chip cards, solid-state drives (SSD), mobile communication equipment		
Security level	**Condition, shape and size after destruction**	**Tolerance**
E-1	Medium physically/electronically unusable	
E-2	Medium broken into pieces	
E-3	Medium broken into pieces and Particle size ≤ 160 mm^2	10% of the material may exceed the specified particle size, but shall not be more than 480 mm^2 in size.

Appendix B Table of Shred Measurement

	Length (Longest Side)	Width (Shortest Side)
	mm	mm
1	18.57	6.85
2	15.60	8.66
3	12.10	5.24
4	16.62	9.95
5	12.53	8.15
6	13.02	7.07
7	12.34	4.64
8	7.73	4.80
9	19.98	4.94
10	19.05	5.87
11	14.57	5.41
12	14.58	13.61
13	12.60	7.68
14	7.82	5.67
15	9.76	5.41
16	15.57	10.80
17	16.38	5.83
18	19.42	10.95
19	13.83	7.99
20	13.57	13.57
21	8.44	7.95
22	10.99	9.99
23	21.28	11.02
24	28.03	4.15
25	12.84	5.25
26	13.93	5.73
27	10.96	7.15
28	10.35	8.86
29	18.30	6.01
30	8.30	6.59
31	14.83	5.95
32	10.89	4.92
33	11.20	6.74
34	6.91	6.05
35	6.52	5.03
36	6.20	3.80
37	6.10	5.27
38	6.98	4.14
39	6.36	3.20
40	7.29	4.30
Total	**512.34**	**275.19**
Average	**12.81**	**6.88**
Max	**28.03**	**13.61**
Min	**6.10**	**3.20**

Appendix C Graph of Shred Measurement