



**Products Claims Testing
Claims Test ADC0071
Toolhouse DV-Systeme GmbH & Co.KG**

Author: Dr Andrew Blyth,

Revision 1.0

Date: October 30, 2019

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

30/10/2019 Revision 1.0 issued to Steve Mellings



**Asset Disposal and Information Security
Alliance Limited**

Phone: 0044 845 557 7726

Web: www.adisa.global

Registration Number: 07390092

Registered Office: 31 Thrales End Business
Centre, Thrales End Lane, Harpenden, AL5 3NS

Contents

1.0	Executive Summary	4
2.0	Test Level 1 Testing Solid State and Electromagnetic Drives	5
2.1	Methodology.....	5
3.0	Test Level 2 Testing Solid State Drive.....	6
3.1	Methodology.....	6
4.0	Test Level 2 Testing Electromechanical Drive.....	8
4.1	Methodology.....	8
5.0	Summary and Conclusions.....	10

CONFIDENTIAL

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 ADPC0071 submitted by Volker Denkhaus of toolhouse DV-Systeme GmbH & Co.KG in October

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:

“toolstar®testLX Version 5.11 with shredderLX-module, when used in accordance with inbuilt manual and help function will overwrite all user data on the sample media when algorithm BSI-3 is selected for HDD and algorithm Overwrite plus Enhanced Secure Erase SSD for SSD are selected, such that no user data cannot be recovered using forensic techniques aligned ADISA Test Level 2..” ADPC0071

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

Device	Test Level
Western Digital HDD WD2500AAKX SATA	1 and 2
Samsung 860 EVO V-NAND SATA 250Gb	1 and 2

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

- Western Digital Model: WD2500AAKX
- Samsung Model: 860 EVO V-NAND SATA 250Gb

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

- Western Digital Model: WD2500AAKX
- Samsung Model: 860 EVO V-NAND SATA 250Gb

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. The device is connected to a target PC and placed in a stable state.
2. The applicant software was configured in accordance with the manufacturer's instructions.
3. Structured data, the string "ADISA", was written to every logical block address on the hard drive.
4. The device was then imaged using standard imaging techniques to create a base-line forensic image.
5. The device was then erased using the applicant's software in accordance with the manufacturer's instructions.
6. The device was then analysed using the following tools to create a second forensic image:
 - a. Standard commercial tools and techniques such as Access Data/FTK, Forensic Explorer and Encase.
7. The two forensic images (Stage 4 and Stage 6) 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 (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

The Results of Test Level 1.

Hard Drive/Model	Result
Western Digital HDD WD2500AAKX SATA	PASS
Samsung 860 EVO V-NAND SATA 250Gb	PASS

Pass means that the software toolstar@testLX with shredderLX-module 5.10 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 manufacturer's user manual.

3.0 Test Level 2 Testing Solid State Drive

3.1 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 device, the following methodology is performed:

1. The device is connected to a target PC and place in a stable state.
2. The applicant software was configured in accordance with the manufacturer's instructions.
3. If present on the test device the DCO and HPA are removed.
4. Structured data, the string "ADISA", was written to every logical block address on the hard drive.
5. The device was then imaged using standard imaging techniques to create a base-line forensic image.
6. The device was then erased using the applicant's software in accordance with the manufacturer's instructions.
7. 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.

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
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

The Results of Test Level 2.

<i>Hard Drive/Model</i>	<i>Result</i>
Western Digital HDD WD2500AAKX SATA	PASS
Samsung 860 EVO V-NAND SATA 250Gb	PASS

Pass means that the software toolstar@testLX with shredderLX-module 5.10 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. A key element to the claims test is that the software has to be used in accordance with the manufacturers user manual

CONFIDENTIAL

4.0 Test Level 2 Testing Electromechanical Drive

4.1 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 device, the following methodology is performed:

1. The device is connected to a target PC and place in a stable state.
2. The applicant software was configured in accordance with the manufacturer's instructions.
3. If present on the test device the DCO and HPA are removed.
4. Structured data, the string "ADISA", was written to every logical block address on the hard drive.
5. The device was then imaged using standard imaging techniques to create a base-line forensic image.
6. The device was then erased using the applicant's software in accordance with the manufacturer's instructions.
7. 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 UDMA/SAS;
 - iii. Hardware debugging techniques such as JTAG, I3C and SPI;
 - iv. Customer designed data recovery software.

4.2 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
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

The Results of Test Level 2.

<i>Hard Drive/Model</i>	<i>Result</i>
Western Digital HDD WD2500AAKX SATA	PASS
Samsung 860 EVO V-NAND SATA 250Gb	PASS

Pass means that the software toolstar@testLX with shredderLX-module 5.10 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. A key element to the claims test is that the software has to be used in accordance with the manufacturers user manual

CONFIDENTIAL

5.0 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 software tested was the toolhouse DV-Systeme GmbH & Co.KG toolstar@testLX with shredderLX-module 5.10

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

Test Facility: ADISA Research Centre

Signature:



Date: 30th October 2019

CONFIDENTIAL