Product Claims Test
Application Number ADPC0046
Horizon Technology, LLC

Author: Professor Andrew Blyth

Revision 1.2
Date: June 15, 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

23.05.2018	Revision 1.0 issued to Andrew Blyth
13.06.2018	Revision 1.1 issued to Andrew Blyth
15.06.2018	Revision 1.2 issued to Andrew Blyth

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

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 ADPC0046 submitted by Horizon Technology, LLC. 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 baseline used to proof/disprove a claim in relation to data erasure/sanitization of mobile phone is that of a factory reset on the device.

The claim made for the drive was:

> *"Prosoft Engineering Inc.'s product called 'Media Tools Wipe Version 1.2.1' when used in accordance with the Use Manual Media Tools 1.2.1 Wipe Guide will overwrite all user data on the hardware sample within this test to protect from forensic attack equivalent to test level 2 of the ADISA Threat Matrix" – Claim Number ADPC0046.*

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

Family	***Model***	***Test Level***
BiWIN SSD – C1001 480 GB	CSE25GS2474-480	1
Seagate Barracuda MHD - 500GB	ST500LM030	1

Table 1 – Devices Tested

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

- BiWIN SSD – C1001 480 GB device Model CSE25GS2474-480
- Seagate Barracuda MHD 500GB device. Model ST500LM030

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

- BiWIN SSD – C1001 480 GB device. Model CSE25GS2474-480
- Seagate Barracuda MHD 500GB device. Model ST500LM030

2.0 Test Level 1 Testing Solid State and Electromagnetic Drives

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. (e.g. Encase V7.12.01 and Forensic Explorer V4). For each device the following methodology is performed.

1. The Software was configured in accordance with the manufacturer's instructions.
2. If present the DCO and HPA are removed from the test devices
3. Structure data of a known type is written to ever positive logical block address (LBA)
4. To create a Base Image for comparison the device is then forensically images.
5. The device was then erased using the software in accordance with the manufacturer's instructions.
6. The device was then imaged to create the test image.
7. The test image was then data carved to identify any images and the results compares and contrasted with the base-image constructed in step 5.

2.2 Test Results.

Test Level 1 Summary Results

Test Level 1 replicated an attack on this device 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

Family	*Model*	Result
BiWIN SSD – C1001 480 GB	CSE25GS2474-480	**PASS**
Seagate Barracuda MHD - 500GB	ST500LM030	**PASS**

- Pass means that Media Wiping Tools V1.2.1 mitigates the threat posed by the Threat Actors holding the capabilities outlined by Test Level 1.

3.0 Test Level 2 Testing Solid State Drives

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. 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 test applicant's software 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 data recovery tools such as PC3000 SSD;
        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 and Rusolut;
        iii. 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
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.

Family	*Model*	**Result**
BiWIN SSD – C1001 480 GB	CSE25GS2474-480	**PASS**

- Pass means that Media Wiping Tools V1.2.1 mitigates the threat posed by the Threat Actors holding the capabilities outlined by Test Level 2.

4.0 Test Level 2 Testing Electromagnetic 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. 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 applicants software 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 data recovery tools such as PC3000 UDMA/SAS;
        iii. 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
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.

Family	*Model*	Result
Seagate Barracuda MHD - 500GB	ST500LM030	**PASS**

- Pass means that Media Wiping Tools V1.2.1 mitigates the threat posed by the Threat Actors holding the capabilities outlined by Test Level 2.

5.0 Summary and Conclusions

The BiWIN SSD – C1001 480 GB device tested passed the claims test as all-forensic data recovery techniques up to and including ADISA Test Level 2 failed to recover any data. The software tested was Media Wiping Tools V1.2.1.

The Seagate Barracuda 500GB device tested passed the claims test as all-forensic data recovery techniques up to and including ADISA Test Level 2 failed to recover any data. The software tested was Media Wiping Tools V1.2.1.

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

Signature: 

Date: 13th June 2018