Products Claims Testing
Claims Test ADPC000076
Stellar Data Recovery Inc

Author: Dr Andrew Blyth,

Revision 1.0
Date: December 12, 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

12/12/20019 v1.0 issued to Steve Mellings

ADISA ASSET DISPOSAL & INFORMATION SECURITY ALLIANCE

Asset Disposal and Information Security Alliance Limited

Phone: 0044 845 557 7726

Registration Number: 07390092

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

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

Contents

1.0 Executive Summary

This is a final report detailing the findings in relation to the execution of the ADISA Testing Methodology on Claims Test ADPC000076 which was submitted by Ashiishek Jain of Stellar Data Recovery in November 2019.

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 and p was:

> *"Stellar software called BitRaser Drive Eraser v3.0 and BitRaser Mobile Eraser & Diagnostics v3.0 when used in accordance with User Manuel 3.0 and using NIST 800-88 Purge Algorithm will overwrite all user data on the hardware sample within this test to protect to a forensic attack equivalent to test level 1 of the ADISA threat matrix." ADPC0076*

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

Device	***Test Level***
SanDisk 250GB SSD / SDSSH11 Sata 2.5	1
iPhone 8 / MRRM2B/A	1

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

- SanDisk 250GB SSD Model: SDSSH11 Sata 2.5
- iPhone 8 Model: MRRM2B/A

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 place 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 use 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
SanDisk 250GB SSD	SDSSH11 Sata 2.5	PASS

Pass means that the BitRaser Drive Eraser 3.0 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 1 Testing Smart Phones and Tablets

3.1 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. (e.g. Oxygen). For each device the following methodology is performed.

1. The applicant software was configured in accordance with the manufacturer's instructions.
2. A factory reset is performed on each device in accordance with the device manufacturers instructions.
3. A SIM was inserted into the device and the device connected to a Wi-Fi network.
4. The following data is placed on each device:
    a. A standard pin to unlock the device '123456'
    b. WIFI credentials;
    c. Pictures and Movies;
    d. SMS, MMS, Phone Calls;
    e. Contact Details and Diary Events
    f. Internet Browsing and Internet Email.
5. To create a Base Image for comparison the device was then imaged using Oxygen.
6. The device was then erased using applicant's software in accordance with the manufacturer's instructions.
7. The device was then imaged using Oxygen to create the test image.
8. The test image was then data carved to identify any images and the results compares with the base-image constructed in step 5.

3.2 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 (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

Product	Operating System	Result
Apple iPhone 8	iOS 11.3	PASS

Pass means that the BitRaser Mobile Eraser and Diagnostics 3.0 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.

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 failed to recover any data. The software tested was the BitRaser Drive Eraser 3.0 and BitRaser Mobile Eraser and Diagnostics 3.0.

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

Test Facility: ADISA Research Centre

Signature: 

Date: 12/12/2019

