



Product Claims Test
Application Number ADPC0051
Blanco Technology Group

Author: Professor Andrew Blyth

Revision 1.1
Date: August 3, 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

13.07.2018	Revision 1.0 issued to Andrew Blyth
17.07.2018	Revision 1.1 issued by Andrew Blyth
03.08.2018	Revision 1.2 issued by Steve Mellings



**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	4
2.0	Test Level 1 Testing Smart Phones and Tablets	5
3.0	Summary and Conclusions	6

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 ADPC0051 submitted by Blancco Technology Group. 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:

“Blancco Mobile Device Eraser, when used in accordance with the user manual provided for v. 3.6.0, will erase all user data from the smartphones listed in Section 3. All user data will be unrecoverable using the techniques corresponding to ADISA Threat Matrix Level 1. Erasure report will be automatically generated upon erasure completion.” – Claim Number ADPC0051.

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

Family	OS	Test Level
Apple iPhone 6	iOS 11.3	1
Apple iPhone 8	iOS 11.3	1
Apple Tablet iPad 2	iOS 11.3	1
Samsung Galaxy S8	Android 8.0	1

Table 1 – Devices Tested

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

- Apple iPhone6
- Apple iPhone 8
- Apple iPad 2
- Samsung Galaxy S8

2.0 Test Level 1 Testing Smart Phones and Tablets

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. Cellebrite). 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 types of data are placed on each device:
 - a. Pictures and Movies;
 - b. SMS, Phone Details and Contact Details;
 - c. Internet Browsing and Internet Email;
 - d. Applications such as What's App and Skype.
5. To create a Base Image for comparison the device was then imaged using Cellebrite.
6. The device was then erased using applicant's software in accordance with the manufacturer's instructions.
7. The device was then imaged using Cellebrite 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.

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	OS	Result
Apple iPhone 6	iOS 11.3	PASS
Apple iPhone 8	iOS 11.3	PASS
Apple Tablet iPad 2	iOS 11.3	PASS
Samsung Galaxy S8	Android 8.0	PASS

- Pass means that *Blancco Mobile Device Eraser* mitigates the threat posed by the Threat Actors holding the capabilities outlined by Test Level 1.

3.0 Summary and Conclusions

All devices tested 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 Blancco Mobile Erasure 3.6.0.

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

Signature:

A handwritten signature in black ink, appearing to read 'A. Blyth', written over a horizontal line.

Date: 17th July 2018