Product Claims Test
Application Number ADPC0038
Blackbelt Smartphone Defence Ltd

Author: Professor Andrew Blyth,
University of South Wales

Revision 1.0
Date: December 21, 2017
Distribution: Confidential

DISCLAIMER

The content of this document is based on information shared to date and will be subject to change or modification as requirements are amended, clarified or additional requirements are indicated at a later stage. For this reason this document should be viewed as a discussion document with further qualification and refinement required.

Whilst we make every endeavour to ensure the accuracy of the information provided here and that the recommendations are made to the best of our ability they may be subject to inaccuracies or change.

REVISION HISTORY

19/12/2017 Revision 1.0 issued to Steve Mellings (ADISA)

ADISA ASSET DISPOSAL & INFORMATION SECURITY ALLIANCE

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

University of South Wales Prifysgol De Cymru

University of South Wales

Phone: 0044 845 576 0101

Web: www.southwales.ac.uk

Contents

1.0 Executive Summary 4
2.0 Test Level 1 Testing. 5
3.0 Summary and Conclusions 6
Appendix A Claims Test Application Form 7

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 ADPC0038 submitted by Blackbelt Smartphone Defence Ltd. 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:

> *"BlackBelt Smartphone Defence software 3.8.37, when used in accordance with User Manual "BB Installation Guide – ADISA 0811" will overwrite all available data on the hardware sample within this test to protect to a forensic attack equivalent to test level 1 of the ADISA threat matrix" – Claim Number ADPC0038.*

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

Family	***Model***	***Test Level***
Samsung Galaxy S8 Plus	SM-G955F	1
Apple iPhone 8 Plus	MQ8L2B/A	1

Table 1 – Devices Tested

After testing it is confirmed that the Blackbelt Smartphone Defence Ltd claim is true for all devices tested up to Test Level 1 attacks.

2.0 Test Level 1 Testing

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 Blackbelt Smartphone Defence Software 3.8.37 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. Pictures and Movies;
    b. SMS, Phone Details and Contact Details;
    c. Internet Browsing and Internet Email.
5. To create a Base Image for comparison the device was then imaged using Cellebrite.
6. The device was then erased using Blackbelt Smartphone Defence Software 3.8.37 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 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 these devices 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
Samsung Galaxy S8 Plus	SM-G955F	Pass
Apple iPhone 8 Plus	MQ8L2B/A	Pass

Pass means that the Blackbelt Smartphone Defence Software 3.8.37 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.

3.0 Summary and Conclusions

Both 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 the Blackbelt Smartphone Defence Software 3.8.37.

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

Test Facility: University of South Wales

Signature: 

Date: 18th December 2018

Appendix A Claims Test Application Form

ASSET DISPOSAL & INFORMATION SECURITY ALLIANCE

Claims Testing Application Form
Form Number ADPC0038

Section 1 – Applicant Information

Company Name: Blackbelt Smartphone Defence Ltd
Address: Helm Bank, Natland, Kendal, Cumbria. LA9 7PS

General Contact
Name: Brejesh Chauhan
Phone: 07968280916
Mobile: 07968280916
E-Mail: brejesh.chauhan@blackbeltdefence.com

Section 2 – Applicant Software Information

Manufacturer Blackbelt Smartphone Defence Ltd
Version of software Datawipe 3.8.37

Background (Explanation of the company and software)

Based in the UK, BlackBelt Smartphone Defence was founded in 2004, and has been providing Mobile security products ever since. Datawipe has been independently tested, to ensure the software is compatible with the latest devices, also providing a full audit trail, which is available real time from your user controlled dashboard. Datawipe will safely remove all user data, restoring your smart device back to an out of box state. This software is used by industry and corporate clients.

Technical/physical architecture of claims test applicant software

This section describes how the product is deployed, on what hardware it runs and any other technical aspect of using the product.

Operator PC Minimum Specification: Standard desktop/laptop running Windows 7, 8 or 10. i5 machine with full internet access. Each Operator PC must have at least: • 8GB RAM • 250GB+ SSD drive or Magnetic drive • 2 USB host controllers.

System Access
C:\Program Files (x86)\BlackBelt SmartPhone Defence\ BlackBelt DataWipe\DataWipe.exe"
C:\Program Files (x86)\BlackBelt SmartPhone Defence\ BlackBelt DataWipe\MobileDevice\idevicerestore.exe
C:\Program Files (x86)\BlackBelt SmartPhone Defence\ BlackBelt DataWipe\BBAppleFirmwareService.exe
C:\ProgramData\BlackBelt SmartPhone Defence\

Firewall Access
https://dashboard.blackbeltdefence.com/(88.208.233.202)

http://ax.phobos.apple.com.edgesuite.net (184.25.157.104)
http://appldnld.apple.com.edgesuite.net (77.67.87.89)
http://appldnld.apple.com (17.253.15.206)
phobos.apple.com deimos3.apple.com
albert.apple.com
gs.apple.com
gg*.apple.com*
itunes.apple.com
ax.itunes.apple.com*

NB: if you have Anti-virus running, please also add to the exceptions list.

Blackbelt uses propriety methods for different operating systems

Blackbelt Device Clean

The BlackBelt propriety application and/or secure commands are sent to the connected device to remove all customer data, including; contacts, call logs, calendars, photographs, videos and user alarms. This process ensures we remove all user accessible data.

Data overwrite

BlackBelt offer both standard and secure wipe, when secure is selected the software will overwrite the storage on the device using a bespoke algorithm to ensure that data is not recoverable using specialist software to rebuild user data.

The BlackBelt Datawipe software allows admin-controlled configuration to set number of cycles and passes, to ensure the datawipe process can be configured to meet customer required standards.

Manufacturer Factory Reset

As part of the Data wipe process BlackBelt will always perform a manufacturer factory reset to put the device into an out of box state.

Device Reset Check

To ensure the device is left in a factory reset state, BlackBelt perform a device reset check to complete the process, this ensures the device is left in an out of box state and removes the risk of a false positive response.

Best practice usage guide for usage of software being tested. (Please enclose any manuals)

This is a critical part as the software will be executed by the test lab as per a particular guidance document.

See attached document – BB Installation Guide – Adisa 0811.

Host Information for claims test applicant software to run on. To be shipped by test claimant.

What Hardware (if any) is to be shipped to the test lab in order to run the software?

Do we need to provide a laptop? If yes do we pre-install?

Section 3 – Test Hardware Information

What is the sample of hardware that is to be used during the test?

iPhone 8+

Samsung S8+

ADISA Threat Matrix

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
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
5 (Very High)	Government-sponsored organisations or an organisation with unlimited resources and unlimited time capable of using advanced techniques to mount all types of software and hardware attacks to recover sanitised data.	3

Section 4 – The Claim

BlackBelt Smartphone Defence software 3.8.37, when used in accordance with User Manual "BB Installation Guide – ADISA 0811" will overwrite all available data on the hardware sample within this test to protect to a forensic attack equivalent to test level 1 of the ADISA threat matrix.

Claim Technical Contact at applicant.

Name: Brejesh Chauhan
Phone:
Mobile: 07968280916
E-Mail: Brejesh@blackbeltdefence.com

Acceptance

I, Brejesh Chauhan of BlackBelt Defence confirm that the information outlined in this document is an accurate and true reflection of the claims made by our product wishing to undergo the ADISA testing method.

Signed on behalf of BlackBelt Defence

SIGNED: B Chauhan

NAME: Brejesh Chauhan

TITLE: Head of Product

DATE: 11.12.2017

Claim Accepted by:

Signed on behalf of University of South Wales

SIGNED:

NAME: Andrew Blyth

TITLE: Professor

DATE: 19.12.2017

Signed on behalf of ADISA

SIGNED:

NAME: Steve Mellings

TITLE: Director

DATE: 19.12.2017