ADISA

ASSET DISPOSAL & INFORMATION
SECURITY ALLIANCE

Product Claims Test
Application Number ADPC0041
IMEI Limited

Author: Professor Andrew Blyth

Revision 1.2
Date: May 21, 2018
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

26.03.2018	Revision 1.0 issued to Steve Mellings (ADISA)
06.04.2018	Revision 1.1 issued to Andrew Blyth
21.05.2018	Revision 1.2 issued by 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

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 ADPC0041 submitted by IMEI Limited. 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:

> *"IMEI Ltd's MobiWIPE software v1.0, when used in accordance with the developer user guidance provided for version v1.00 in February 2018 - will erase the user data on the smartphones and tablets within this test to protect from forensic attack equivalent to risk level 2 (test level 1) of the ADISA Threat Matrix" – Claim Number ADPC0041.*

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

Family	***Model***	***Test Level***
Apple iPhone 6 Plus	A1634	1
Samsung S7 Edge	SM-G935	1

Table 1 – Devices Tested

After testing it is confirmed that the IMEI claim is as follows for the test devices:

- The claim **is** true for the Apple iPhone 6 Plus device tested up to Test Level 1 attacks.
- The claim **is** true for the Samsung S7 Edge device 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 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. 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 the 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 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
Apple iPhone 6 Plus	A1634	**PASS**
Samsung S7 Edge	SM-G935	**PASS**

- Pass means that IMEI Ltd's MobiWIPE software v1.0 mitigates the threat posed by the Threat Actors holding the capabilities outlined by Test Level 1.

3.0 Summary and Conclusions

The Samsung S7 Edge device 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 IMEI Ltd's MobiWIPE software v1.0.

The Apple iPhone 6 Plus Edge device 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 IMEI Ltd's MobiWIPE software v1.0.

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

Signature:

Date: 14th May 2018

Appendix A Claims Test Application Form

Form Number ADPC0041

Section 1 – Applicant Information

Company Name: IMEI Ltd
Address: Unit 4, Eastcote Industrial Estate, Field End Road, Eastcote, Middlesex, HA4 9XG

General Contact
Name: Paul Harris
Phone: ______
Mobile: 07872 515665
E-Mail: ph@mobicode.co.uk

Section 2 – Applicant Software Information

Manufacturer IMEI Ltd
Version of software MobiWIPE Version 1.00

Background (Explanation of the company and software)

IMEI Ltd, based in the UK, are a solutions provider to the mobile phone industry, specialising in the pre-owned market. Working with Recyclers, Operators, Retailers, Insurers and Law Enforcement, IMEI Ltd offer end to end / turn key solutions to deliver best practice and compliance to the sector.

Technical / physical architecture of claims test applicant software.

MobiWIPE, is a Windows-Based PC Application, that will operate on Windows 7 Professional and Windows 10 Operating System. The application will be installed using a purpose-built installer to ensure correct installation. User will require sufficient Administrator rights on the PC to allow the installation and storing of application data during use.

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

A full user guide will be provided with the hardware

For our testing we added the following data to the devices:
Photo
Video
Email Account & Sent Email
Contacts
Calendar Entry
Notes
Web History
Call Log
SMS
User Installed Application from official app store

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

We will be providing the following for the Test:

1 x Windows 10 Laptop (HP) with UK mains charger (ensure charging during test)
1 x Apple iPhone 6 Plus
1 x Samsung S7 Edge
1 x Apple iPhone 5 Plus USB Cable

1 x Samsung S7 Edge USB Cable

*Devices will be charged before shipping but ensure charged to 25% minimum before test (incase turned on in transit)

Section 3 – Test Hardware Information

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

iPhone 6 Plus (supplied)

Samsung S7 Edge (supplied)

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

IMEI Ltd's MobiWIPE software v1.0, when used in accordance with the developer user guidance provided for version v1.00 in February 2018 - will erase the user data on the smartphones and tablets within this test to protect from forensic attack equivalent to risk level 2 (test level 1) of the ADISA Threat Matrix.