Products Claims Testing
Application Number ADPC0075
Deep Mobile

Author: Dr. Andrew Blyth,
ADISA Research Centre

Revision 1.1
Date: January 9, 2020
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

18/12/2019	Revision 1.0 issued to Steve Mellings
09/01/2020	Revision 1.1 issued to Steve Mellings

ADISA ASSET DISPOSAL & INFORMATION SECURITY ALLIANCE

www.adisa.global
www.adisarc.com

Asset Disposal and Information Security Alliance Limited

Registration Number: 07390092
Registered Office: 31 Thrales End Business Centre, Thrales End Lane, Harpenden, AL5 3NS

Phone: 0044 845 557 7726

Contents

1.0 Executive Summary

This is a report detailing the findings in relation to the execution of the ADISA Testing Methodology on Claims Test ADPC0075 submitted by Jordan Schwartz of Deep Mobile 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 phone was:

> *"DeepMobile Eraser™ 1.0 when used in accordance with User Manuel 1.0 and using NIST 800-88 Rev 1 or Cryptographic 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.*
>
> *On Android:*
> *For encrpyted androids - Cryptographic erasure is performed to pass level 1 testing.*
> *For unencrypted devices - Data erasure using method stated in NIST 800-88 Rev 1 is performed to pass level 1 testing.*
>
> *On Ios:*
> *Cryptographic erasure is performed to pass level 1 testing*
> *Cryptographic erasure + firmware upgrade to pass level 1 testing" ADPC0074*

Three devices were submitted as part of this test with the two Android devices being tested in both encrypted and unencrypted modes. These are listed below:

Device			***Test Level***
iPhone 8	Model:	MRRM2B/A	1
Samsung Galaxy S9	Model:	SM-G960F Unencrypted	1
Samsung Galaxy S9	Model:	SM-G960F Encrypted	1
Sony Xperia	Model:	C1505 Unencrypted	1
Sony Xperia	Model:	C1505 Encrypted	1

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

- iPhone 8 Model: MRRM2B/A
- Samsung Galaxy S9 Model: SM-G960F
- Sony Xperia Model: C1505

2.0 Test Level 1 Testing Smart Phones and Tablets

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. (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.

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 (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

Family	Operating System	Result
Apple iPhone 8	ISO 13.2.3	PASS
Samsung Galaxy S9 Encrypted	Android OS: 8.0.0	PASS
Samsung Galaxy S9 Unencrypted	Android OS: 8.0.0	PASS

Sony Xperia	Encrypted	Android OS: 4.1.1	PASS
Sony Xperia	Unencrypted	Android OS: 4.1.1	PASS

Pass means that DeepMobile Eraser™ 1.0 mitigates the threat posed by the Threat Actors holding the capabilities outlined by Test Level 1.

2.3 Encrypted and Unencrypted Modes in Android Handsets.

Within the Android Operating System encryption is enabled via the security options within the Apps Screen. The encryption algorithm is by Android is 128 Advanced Encryption Standard (AES) with a key length of 128 bits, and with a cipher-block chaining (CBC) and SHA256. The master key is encrypted with 128-bit AES used by the phone is also encrypted. Disk Encryption was first support in Android Version 4.

3.0 Summary and Conclusions

Claims Test Result: **Pass on all devices tested.**

The three devices all 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 DeepMobile Eraser™ 1.0.

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

Test Facility: ADISA Research Centre

Signature: 

Date: 10th December 2019