ASSET DISPOSAL & INFORMATION SECURITY ALLIANCE

Product Claims Test
Application Number ADPC0078
iMT Co Ltd

Author: Dr Andrew Blyth PHD,

Revision 1.0
Date: January 16, 2020
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

15.01.2020 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 / www.adisarc.com

Registration Number: 07390092

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 ADPC0078 submitted by iMT Co 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:

> *"iMT Co. Ltd. Software called iMT Cleaner 2.0 when used in accordance with the user manual iMT-Cleaner 2.0 and using algorithm DoD 5220.22 M will overwrite all user data on the hardware sample within this test to protect against a forensic attack equivalent to test level 1 of the ADISA threat matrix – Claim Number ADPC0078.*

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

Family	***Model***	***Test Level***
Apple iPhone 8	MRRM2B/A	1
Samsung Galaxy S9	SM-G960F	1

Table 1 – Devices Tested

After testing it is confirmed that the iMT Co Ltd **claim is true** for these devices tested up to Test Level 1 attacks.

2.0 Test Level 1 Testing Smart Phones

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. Cellebrite or 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. 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 or Oxygen
6. The device was then erased using applicant software in accordance with the manufacturer's instructions.
7. The device was then imaged using Cellebrite or Oxygen 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 (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	*Model*	Result
Apple iPhone 8	MRRM2B/A	1
Samsung Galaxy S9	SM-G960F	1

Pass means that the iMT Co Ltd Software iMT-Cleaner 2.0 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 Summary and Conclusions

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

The 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 the iMT Co Ltd Software iMT-Cleaner 2.0

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

Test Facility: ADISA Research Centre

Signature: 

Date: 15th January 2020

