Products Claims Testing
Application Number ADPC151

Author: Godfred Badu
ADISA Research Centre

Revision 1.0
Date: July 25, 2022
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

25.07.2022 Revision 1.0 issued to Michael Ben-Oliel

ADISA Research Centre

Phone: +44 (0) 1582 361743

Web: www.adisa.global
Web: www.adisarc.com

Registration Number: 07390092
Registered Office: Ground Floor, 5
Kinsbourne Court, Harpenden, AL5 3BL,
United Kingdom

Contents

1.0 Executive Summary 4
2.0 Test Level 1 Testing Smart Phones and Tablets 5
3.0 Summary and Conclusions 7

1.0 Executive Summary

This is a report detailing the findings in relation to the execution of the ADISA Testing Methodology on Claims Test ADPC0151 submitted by Michael Ben-Oliel in July 2022.

The claims test was carried out in accordance with ADISA Claims Testing (ACT) v1.0 and supporting document ADISA Testing Methodology v1.12, both of which are available from ADISA.

The claim made for the phone was:

> *"MCE software with Wipe Engine 12.4.73, when used in accordance with on-screen instructions for Wipe process will sanitize user-generated data from smart phones and tablet within this test to protect from a forensic attack equivalent to test level 1 of the ADISA threat matrix."*

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

Device	***Test Level***
Apple iPhone 11 (MWLT2B/A) running iOS 15.5	1
Samsung Galaxy S20 (SM-G980F/DS) running Android 12	1
Apple iPad 8th Generation (MYLD2LL/A) running iOS 15.5	1

After testing it is confirmed that the ADPC151 **claim is True** for the devices tested up to Test Level 1 results. Those devices are:

- Apple iPhone 11 running iOS 15.5
- Samsung Galaxy S20 running Android 12
- Apple iPad running iOS 15.5

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;
    g. Email/Gmail account.
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 these devices being made by an aggressor with capabilities outlined below.

Test Level	Threat Actor	Compromise Methods	Sanitisation Method
1	Casual or opportunistic threat actor only able to mount high-level non-invasive and non-destructive software attacks utilizing freeware, COTS and OS tools	Keyboard attacks from a motivated individual or professional organisation. Typical attack could be using open-source forensic tools or commercial tools	Aligned to Clear

The Results of Test Level 1

Make and Model	Operating System	Result
Apple iPhone 11	iOS 15.5	PASS
Samsung Galaxy S20	Android 12	PASS
Apple iPad 8th Generation	iOS 15.5	PASS

PASS means that *ADPC0151* mitigate the threat posed by the Threat Actors holding the capabilities outlined by Test Level 1.

3.0 Summary and Conclusions

Claims Test Result: Pass on all devices tested.

The two devices passed the claims test as forensic data recovery techniques up to and including ADISA Test Level 1 did not recover data from the devices after the software was executed. The software tested was the *MCE Wipe Engine v12.4.73*

Claims Test Carried Out By: Godfred Badu

Test Facility: ADISA Research Centre

Signature: 

Date: 25th July 2022