University of South Wales
Prifysgol De Cymru

ADISA
ASSET DISPOSAL & INFORMATION SECURITY ALLIANCE

Products Claims Testing
Claims Test ADPC0037
Future Dial

Author: Professor Andrew Blyth,
University of South Wales

Revision 1.0
Date: February 27, 2018
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

23/02/2018 Revision 1.0 issued to Steve Mellings

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, United Kingdom

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

This is a preliminary report detailing the findings in relation to the execution of the ADISA Testing Methodology on Claims Test ADPC0037 submitted by Future Dial in January 2018.

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 magnetic hard drive and solid-state drive was:

> *"FutureDial's Data Storage Eraser (DSE), when used in accordance with User Manual version 3.0 will sanitize the solid state and magnetic hard drives listed in Section 3 of this claims test application, such that the all user data is unrecoverable using techniques aligned to ADISA Risk Levels 1 and 2 as outlined in Section 3. Upon successful sanitization, a Certification of Sanitisation will be produced to validate this.- Claim Number ADPC0037."*

The claim made for IoS and Android Smart Phones was:

> *"FutureDial Lean One-touch 4.11.0, when used in accordance with User Manual 4.0 will sanitize the smart phones listed in Section 3 of this claims test application, such that the all user data is unrecoverable using techniques aligned to ADISA Risk Levels 1 and 2 as outlined in Section 3. Upon successful sanitization, a Certification of Sanitisation will be produced to validate this.- Claim Number ADPC0037."*

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

Device	***Test Level***
WestGate WD5000LPLX-66ZNTT1 – SATA HDD	1
Kingston SKC400S37256G – SATA - SSD	1
iPhone 7 running iOS 11.2	1
Samsung Galaxy S7 G930T running Android 7.0	1

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

- WestGate Model WD5000LPLX-66ZNTT1 – SATA HDD
- Kingston Model SKC400S37256G – SATA - SSD
- iPhone Model iPhone 7 running iOS 11.2
- Samsung Model Galaxy S7 G930T running Android 7.0

2.0 Test Level 1 Testing Solid State and Electromagnetic Drives

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.

For each computer hard drive device, the following methodology is performed:

1. Structured data, the string "ISRG", was written to every logical block address on the hard drive.
2. The device was then imaged using Access Data / FTK to create a base-line forensic image.
3. The device was then erased using the Data Storage Eraser (DSE), in accordance with the manufacturer's instructions.
4. The device was then analysed use using the following tools to create a second forensic image:
    a. Standard commercial tools and techniques such as Access Data/FTK and Encase.
5. The two forensic images (Stage 3 and Stage5) were then compared and contrasted to ensure that all structured data had been removed.
    a. For this test, there is no tolerance for remnant structured data and the result is a straight Pass or Fail.

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.

Hard Drive/Model	***Result***
WestGate WD5000LPLX-66ZNTT1 – SATA HDD	PASS
Kingston SKC400S37256G – SATA - SSD	PASS

Pass means that FutureDial's Data Storage Eraser (DSE), 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 Test Level 1 Testing Smart Phones

3.1 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 FutureDial Lean One-touch 4.11.0 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 FutureDial Lean One-touch 4.11.0 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.

3.2 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

Hard Drive/Model	***Result***
WestGate WD5000LPLX-66ZNTT1 – SATA HDD	PASS
Kingston SKC400S37256G – SATA - SSD	PASS

Pass means that the FutureDial Lean One-touch 4.11.0 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.

4.0 Summary and Conclusions.

Claims Test Result: Pass on all devices tested.

The two devices 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 FutureDial Lean One-touch 4.11.0 and FutureDial's Data Storage Eraser (DSE).

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

Test Facility: University of South Wales

Signature: 

Date: 23rd February 2018