ARC | ADISA RESEARCH CENTRE

Products Claims Testing
Claims Test ADPC0118
U-Reach Data Solutions Inc.

Author: Godfred Badu

Revision 1.0
Date: September 16, 2021

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

16.09.2021   Revision 1.0 Issued to Justin Dobrusky

Contents

1.0   Executive Summary

This is a final report detailing the findings in relation to the execution of the ADISA Testing Methodology on Claims Test ADPC0118 submitted by Justin Dobrusky of U-Reach Data Solutions in August 2021.

The claims test was carried out in accordance with ADISA Claims Testing (ACT) v1.0 and supporting document ADISA Testing Methodology v1.4, both of which are available from ADISA.

The claim made for the test was:

> *"MTS400-SAS (SAS and SATA duplicator and sanitizer) running firmware Controller HD3970SAS firmware version 2.4X.XX and when used in accordance with User Manual UM-UR&USA-EN-MTS-SAS-20200902 VA.01.2 and using algorithm Full Erase, will sanitise all user data on media listed in Section 3, such that forensic techniques aligned to Test Level 1 cannot recover user data."ADPC118*

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

Device	Test Level
Seagate Momentus XT (ST500LX003) 500GB 2.5" SATA HDD	1
Hitachi HTS725025A9A364 250 GB 2.5" SATA HDD	1

After testing it is confirmed that the U-Reach Data Solutions claim **is true** for the devices tested up to Test Level 1 results.

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. The device is connected to a target PC and place in a stable state.
2. The applicant software was configured in accordance with the manufacturer's instructions.
3. Structured data, the string "ADISA", was written to every logical block address on the hard drive.
4. The device was then imaged using standard imaging techniques to create a base-line forensic image.
5. The device was then erased using the applicant's software in accordance with the manufacturer's instructions.
6. 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, Forensic Explorer and Encase.
7. The two forensic images (Stage 4 and Stage 6) 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 (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.

Hard Drive/Model	Result
Seagate Momentus XT (ST500LX003) 500GB 2.5" SATA HDD	PASS
Hitachi HTS725025A9A364 250 GB 2.5" SATA HDD	PASS

Pass means that the *MTS400-SAS (SAS and SATA duplicator and sanitizer) running firmware Controller HD3970SAS firmware version 2.4X.XX* mitigates the threat posed by the Threat Actors holding the capabilities outlined by Test Level 1 on the tested devices.

3.0   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 *MTS400-SAS (SAS and SATA duplicator and sanitizer) running firmware Controller HD3970SAS firmware version 2.4X.XX*

Claims Test Carried Out By: Godfred Badu

Test Facility: ADISA Research Centre

Signature:

Date: 15th September 2021