



Certification Report: Onsite Repair System v 9.1.W01.6474
Application Reference Number: ADPC190

Author: Paul Stretch
ADISA Research Centre

Date: June 26, 2023
Distribution: Client Confidential

Foreword

ADISA Certification is an independent certification body specialising in product and service certification. Product Certification is undertaken by the ADISA Research Centre (ARC) which is the test laboratory operated by ADISA Certification.

This certification report is for the verification of a claim made under the Product Claims Test (PCT) service offered by the ARC. This service is where a claim is made about the suitability of a data sanitisation product to render the data on a target set of media unretrievable using a range of data recovery techniques aligned to the ADISA Threat Matrix within this document.

The testing process is undertaken following the ADISA Product Claims Test Methodology for the target media identified during each specific test and this report contains information regarding an application which is permitted to be released into the public domain.

All companies whose products have passed the testing undertaken by the ARC are required to sign a Licence Agreement and must comply with ADISA Brand Guidelines when using the ADISA marks.

A certification awarded by ADISA Certification is not an endorsement of the product.

Disclaimer

The PCT is presented as the outcome of a specific test conducted in the laboratory environment under controlled conditions. Use of this certified product for the purpose of sanitising 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 makes no warranty of any kind with regards to this evaluated product and shall not accept any liability for incidental or consequential damages resulting from the use of the product.

Report Revision History

<i>Issue</i>	<i>Date</i>	<i>Detail of changes</i>
0.1	21.06.2023	Draft for review
0.2	22.06.2023	Draft for review
0.3	23.06.2023	Draft for review
1.0	23.06.2023	Initial release

ADISA Research Centre trading name of ADISA Certification Limited.

Registration Number: 07390092

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

Web: www.adisa.global

Web: www.adisarc.com

Phone: 0044 (1) 1582 361743

Contents

Executive Summary	4
Certification.....	4
1. Target of Evaluation (TOE)	5
1.1 Claim	5
1.2 Identification.....	5
1.3 Test Media	5
2. Testing Methodology	6
2.1 Overview	6
2.2 Threat Matrix	6
2.2 Procedure.....	6
3. Summary	7
3.1 Results of Evaluation.....	7
3.2 Observations	7
3.3 Conclusions	7
Appendix A – TOE Information	8
Appendix B – Devices Tested.....	8
Appendix C – Post-Wipe	10
Appendix D – ARC Testing Equipment	22

Executive Summary

This report details the findings in relation to the Target of Evaluation (TOE) listed below against the ADISA Product Claims Test (PCT) scheme application ADPC190 submitted by Storage Recovery Migration Services Ltd. The PCT scheme examines the outcome of TOE sanitisation on specified test devices. The evaluation was completed at the ARC on 21 June 2023. This Certification Report only applies to the version of the product evaluated.

The details for the product under evaluation.

<i>Name</i>	<i>Version Number</i>
Onsite Repair System (ORS)	9.1.W01.6474

Table 1 – Target of evaluation

As part of the evaluation, the vendor submitted documents to be used as guidance documents and these are listed in the table below.

<i>Document Name</i>	<i>Version Number</i>
NORS Operating Manual	1.4

Table 2 – List of Guidance Documents

Certification

After testing it is confirmed that the ADPC190 **claim is true** for the devices tested up to ADISA Test Level 1.

1. Target of Evaluation (TOE)

1.1 Claim

On the 13 April 2023 Storage Recovery Migration Services Ltd submitted their Onsite Repair System (ORS) to the ADISA Research Centre Forensic Laboratory to conduct a Product Claims Test (PCT) in a controlled lab environment on three devices. The claims test was carried out in accordance with ADISA Test Methodology document, which is available from ADISA.

The claim made for the TOE was:

Onsite Repair System software 9.1.W01.6474 when used in accordance with user manual and using NIST Wipe IPSV algorithm, will sanitise all user data on Test Media(s) such that forensic techniques aligned to Test Level 1 cannot recover data.

1.2 Identification

Details of the software submitted for testing is in table below:

	<i>Description</i>
TOE and version	Onsite Repair System software 9.1.W01.6474
Manufacturer	Storage Recovery Migration Services Ltd
Test Level	Level 1

Table 3 – Product Details

The product under evaluation requires additional components (i.e. software/hardware/firmware) for its operation. These components include:

	<i>Description</i>
Host Operating System	Not applicable
Hardware Requirements	Not applicable
Deployment	Hardware appliance

Table 4 – Operational Requirements

1.3 Test Media

The TOE is executed on the device(s) specified in the PCT Application Form completed by the applicant whilst following the user manual. The details of the device(s) used as part of this test are listed below:

<i>Media Type</i>	<i>Device Description</i>	<i>Serial Number</i>	<i>Media Interface Type</i>
Magnetic	HGST HUS722T2TALA604 MHD-ATA3	WMC6N0H5A56W	SATA
Magnetic	IBM VPBA146C3ETS11 MHD-SCSI1	JFYKMR9C	SAS
Solid-State	SanDisk X300-SD7SB6S-128G-1012 SSD-ATA1	163093400853	SATA

Table 5 – Test Media

2. Testing Methodology

2.1 Overview

This section defines the ADISA Threat Matrix and the Test Levels associated with it and provides a high-level overview of the test procedure undertaken.

2.2 Threat Matrix

The threat matrix defines three test levels which in turn define a series of capabilities that a threat actor/agent may wish to bring against an asset either by direct access to the asset or access via its location within a device.

Test Level	Threat Actor and Compromise Methods	Attack Examples
1	Casual or opportunistic threat actor only able to mount unsophisticated attacks.	Keyboard attacks using the standard device interface using commercial off the shelf (COTS) or open-source forensic tools.
2	Motivated, targeted threat actor such as organised crime or journalists or hackers applying laboratory methods.	Advanced attacks using specialist hardware and software to interrogate the device / storage media using the device interface and component attacks.
3	State-sponsored organisations using sophisticated techniques with unlimited time and resources.	Typical attack may involve proprietary hardware and software techniques not available on the general commercial market.

Table 6. ADISA Threat Matrix v4.1

2.2 Procedure

For each device the TOE is tested against, the following general methodology is performed:

1. The device is prepared and verified with known test data in accordance with the ADISA Test Methodology. Appendix D lists the ARC hardware utilised during the preparation and verification procedure.
2. The device is then sanitised in accordance with the TOE user manual. Should the TOE fail to operate in accordance with the instructions the ARC will liaise with the client to determine the cause of the issues.
3. On successful completion of the sanitisation process, the device is then analysed using tools and techniques commensurate with the respective Test Level undertaken. This will be a combination of commercial forensic and data recovery tools and proprietary ADISA ARC tools, techniques and methods.
4. The results are analysed with no tolerance for remnant data.
5. On successful completion a report is produced and issued to applicant.

3. Summary

3.1 Results of Evaluation

The table below shows the findings of the PCT carried out on the device(s) listed.

<i>Device Description</i>	<i>Media Interface Type</i>	<i>Test Level</i>	<i>Test Result</i>
MHD-ATA3	SATA	1	Pass
MHD-SCSI1	SAS	1	Pass
SSD-ATA1	SATA	1	Pass

Pass means that ADPC190 mitigates the threat posed by the Threat Actors holding the capabilities outlined by Test Level 1.

3.2 Observations

TOE version number is not displayed in the online management portal screen, only on the sanitisation report.

The algorithm is displayed in the online management portal as 'NIST Wipe 1PSV' but as 'NIST Clear' on the sanitisation report.

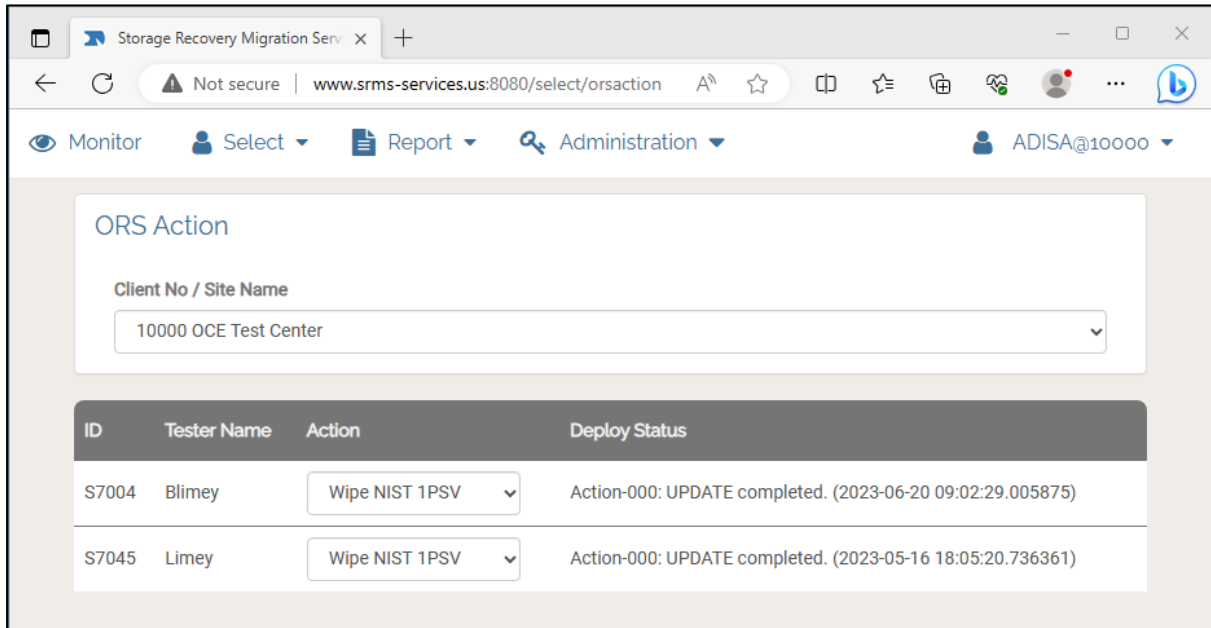
3.3 Conclusions

Claims Test Result: Pass on all devices tested.

The TOE passed the claims test as all forensic data recovery techniques up to and including ADISA Test Level 1 failed to recover any data from the three devices tested.

Appendix A – TOE Information

Photographs of TOE screen showing overwrite method options:



Appendix B – Devices Tested

Photographs of devices tested:

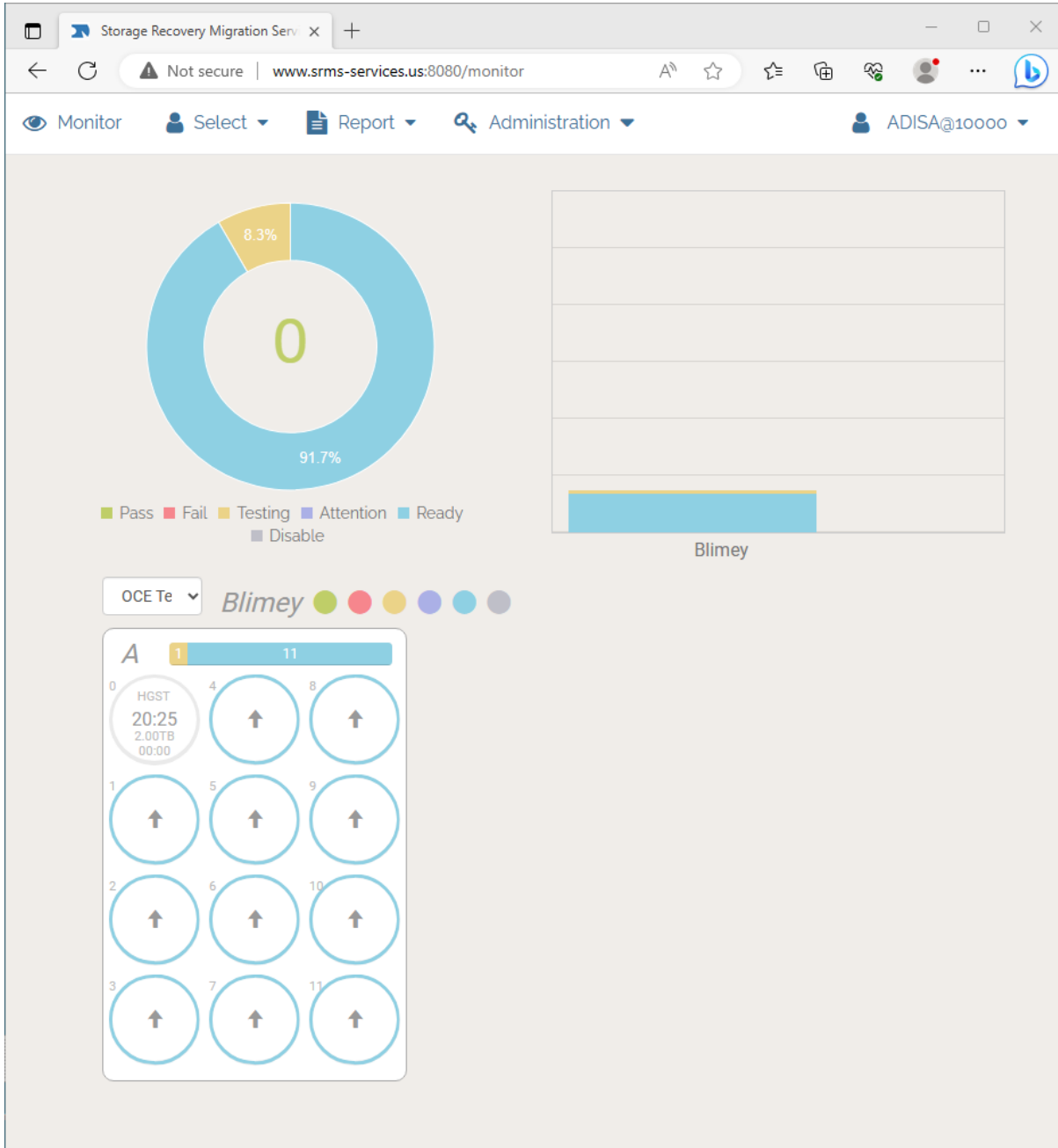




Appendix C – Post-Wipe

Screenshots of Post-Wipe and Post-Wipe images

MHD-ATA3



Storage Recovery Migration Serv x New tab

Not secure | www.srms-services.us:8080/monitor

Monitor Select Report Administration ADISA@10000

8.3%

1

Blimey A - 0

Repair Level	Test Time
4	03:56
Manufacturer	Model
HGST 2.00TB	HUS722T2TALA604
Serial Number	WWN
WMC6N0H5A56W	50014EE059A955AB

HDD-SATA

Pass Fail Test

OCE Te

A 1

0 HGST 2.00TB 03:56

1 4

2 5

3 6 10

7 11

CERTIFICATE OF HDD SANITIZATION

HDD INFORMATION		
Vendor: HGST	Model: HUS722T2TALA604	Capacity: 2000 GB
Serial Number: WMC6N0H5A56W		
World Wide Name: 50014EE059A955AB		
Reference Number:		
SANITIZATION INFORMATION		
Method Type: NIST Clear	Date(UTC): 20-Jun-23 14:17	
Method Used: Overwrite	Key: 318YWSMASJDLE3WK	
Method Details: 1 Pass Overwrite		
Equipment Used: SRMS ORS Version 9.1.W01.6474		
Verification Method: Sample Verify		
Post Sanitization Classification:		
Notes:		
OPERATOR INFORMATION		
Name:	Title:	
Group:	Location:	
Signature:		
Website:	Phone:	
VALIDATION INFORMATION		
Name:	Date:	
Organization:	Location:	



```

/dev/sg0 - HGST HUS722T2TALA604 - WMC6N0H5A56W - RR03 - ATA
*** Full Verification ***
Reference Sector : 0
Device LBA size : 512
Device MaxLBA : 3907029167
    
```

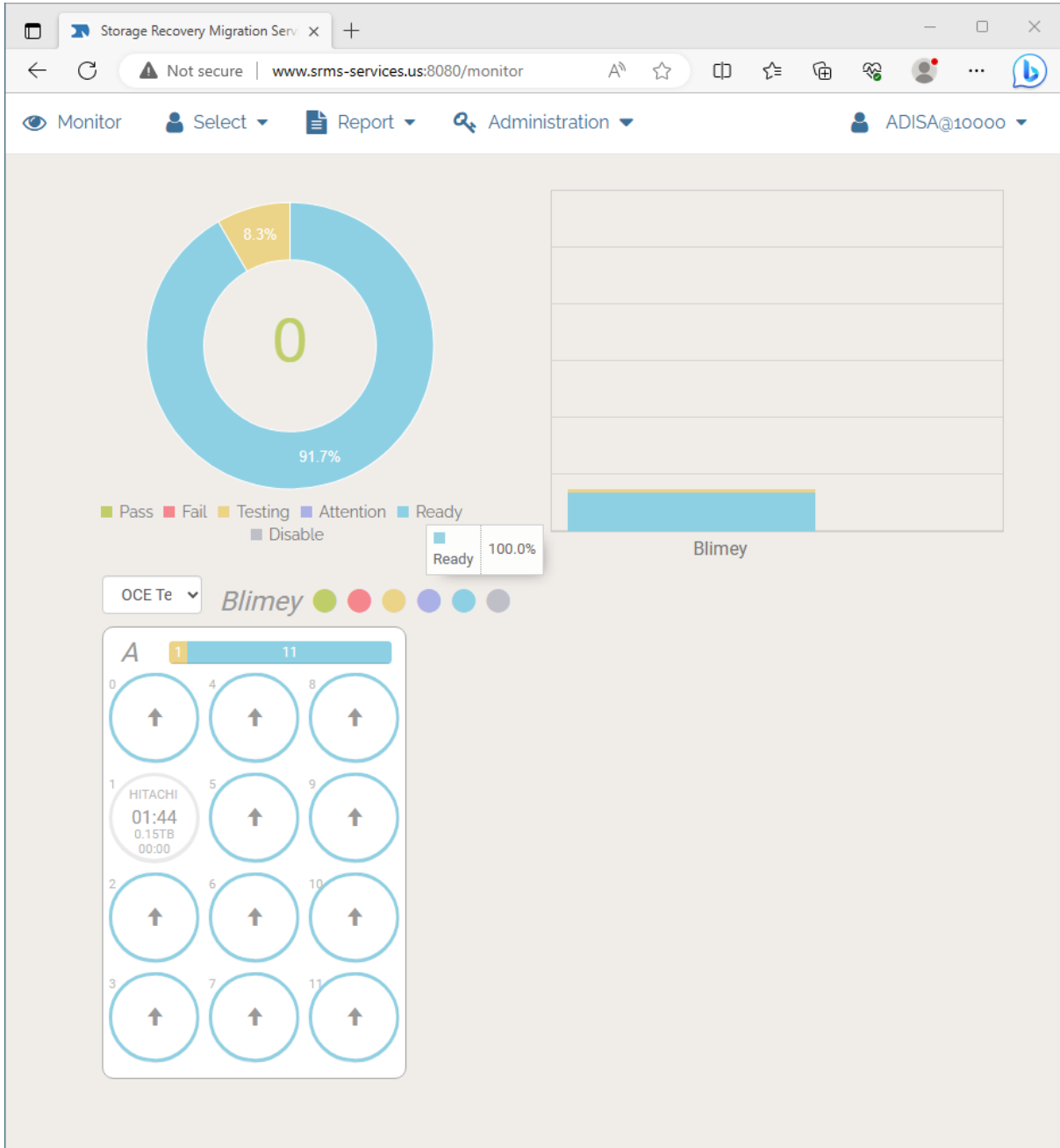
Contents of Reference LBA 0:

Client Confidential

	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F		
0x0000	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
0x0010	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
0x0020	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
0x0030	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
0x0040	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
0x0050	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
0x0060	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
0x0070	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
0x0080	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
0x0090	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
0x00A0	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
0x00B0	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
0x00C0	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
0x00D0	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
0x00E0	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
0x00F0	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
0x0100	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
0x0110	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
0x0120	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
0x0130	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
0x0140	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
0x0150	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
0x0160	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
0x0170	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
0x0180	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
0x0190	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
0x01A0	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
0x01B0	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
0x01C0	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
0x01D0	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
0x01E0	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
0x01F0	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00

*** Checking the Whole Disk ***
Verification Complete - Tue Jun 20 19:13:22 2023

MHD-SCSI



The screenshot shows a web browser window with the URL www.srms-services.us:8080/monitor. The page title is "Storage Recovery Migration Serv". The user is logged in as "ADISA@10000". The interface includes a navigation bar with "Monitor", "Select", "Report", and "Administration" options. A donut chart shows a progress of 8.3% with a large number "1" in the center. A detailed view for "Blimey A - 1" is highlighted with a green circle. This view displays the following information:

Repair Level	4	Test Time	00:30
Manufacturer	HITACHI 0.15TB	Model	HUS153014VLS300
Serial Number	JFYKMR9C	WWN	5000CCA00DC92B63

Below this information, it is identified as "HDD-SAS". In the background, a grid of drive icons is visible, with the selected drive (1) showing "HITACHI RL4 0.15TB 00:30".

CERTIFICATE OF HDD SANITIZATION

HDD INFORMATION

Vendor: HITACHI	Model: HUS153014VLS300	Capacity: 147 GB
-----------------	------------------------	------------------

Serial Number: JFYKMR9C

World Wide Name: 5000CCA00DC92B63

Reference Number:

SANITIZATION INFORMATION

Method Type: NIST Clear	Date(UTC): 21-Jun-23 11:26
-------------------------	----------------------------

Method Used: Overwrite	Key: 22V7SKYMJAELJHQP
------------------------	-----------------------

Method Details: 1 Pass Overwrite

Equipment Used: SRMS ORS Version 9.1.W01.6474

Verification Method: Sample Verify

Post Sanitization Classification:

Notes:

OPERATOR INFORMATION

Name:	Title:
-------	--------

Group:	Location:
--------	-----------

Signature:

Website:	Phone:
----------	--------

VALIDATION INFORMATION

Name:	Date:
-------	-------

Organization:	Location:
---------------	-----------



```

/dev/sg1 - HUS153014VLS300 - JFYKMR9C - A410 - SCSI
*** Full Verification ***
Reference Sector : 0
Device LBA size : 512
Device MaxLBA : 287140276

```

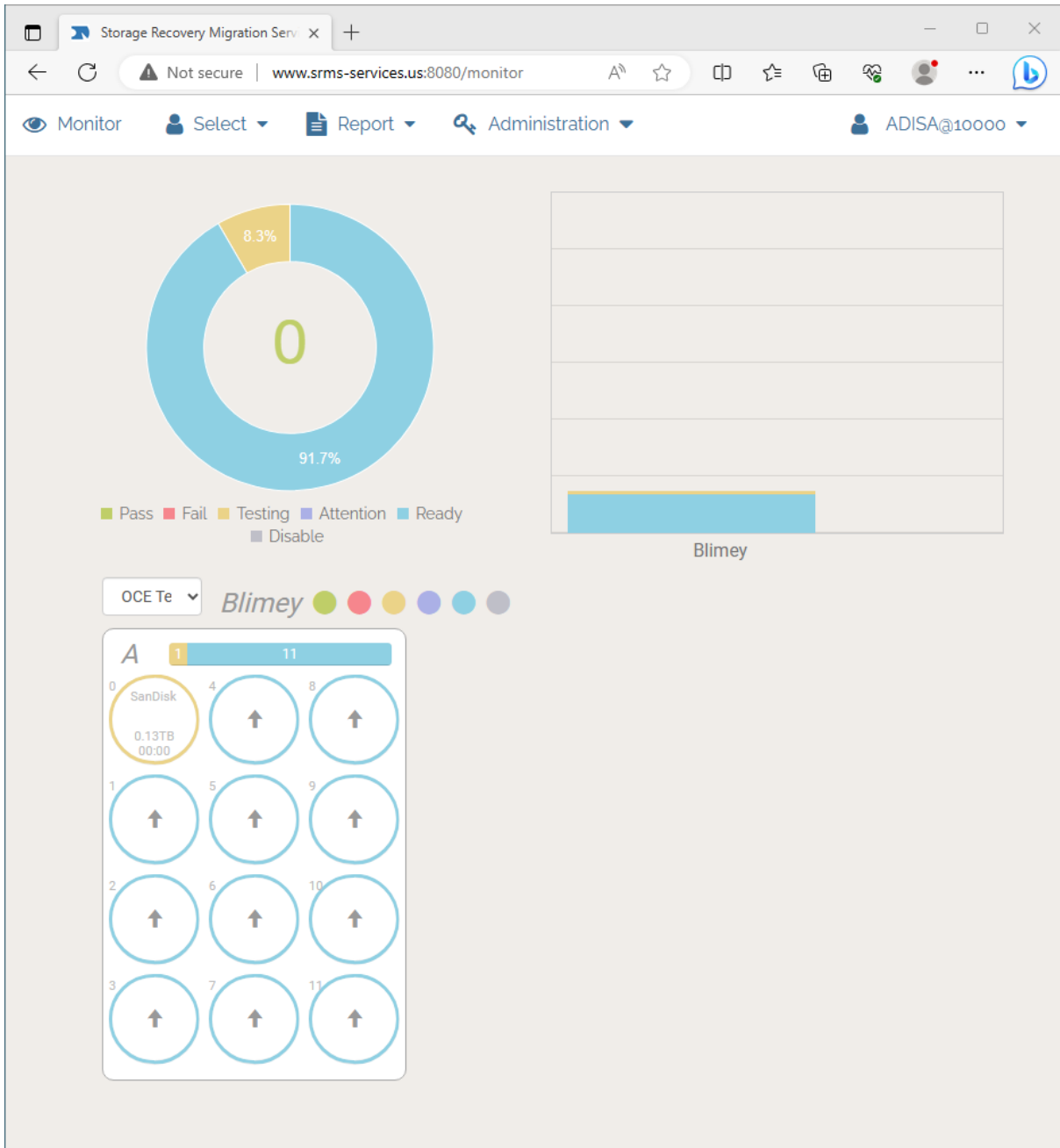
Contents of Reference LBA 0:

Client Confidential

	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F		
0x0000	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
0x0010	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
0x0020	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
0x0030	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
0x0040	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
0x0050	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
0x0060	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
0x0070	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
0x0080	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
0x0090	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
0x00A0	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
0x00B0	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
0x00C0	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
0x00D0	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
0x00E0	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
0x00F0	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
0x0100	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
0x0110	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
0x0120	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
0x0130	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
0x0140	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
0x0150	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
0x0160	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
0x0170	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
0x0180	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
0x0190	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
0x01A0	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
0x01B0	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
0x01C0	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
0x01D0	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
0x01E0	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
0x01F0	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00

*** Checking the Whole Disk ***
Verification Complete - Wed Jun 21 13:01:25 2023

SSD-ATA1



Storage Recovery Migration Serv x +

Not secure | www.srms-services.us:8080/monitor

Monitor Select Report Administration ADISA@10000

8.3%

1

Pass Fail Testi

OCE Te Bl

A 1

SanDisk
RL9
0.13TB
00:08

4

1 2 3

5 6 7

10 11

Blimey A - 0

Repair Level: 9

Test Time: 00:08

Manufacturer: SanDisk 0.13TB


Model: SD7SB6S128G1001

Serial Number: 163093400853

WWN: 5001B444A4DCB5A2

SSD-SATA

CERTIFICATE OF SSD SANITIZATION

SSD INFORMATION		
Vendor: SanDisk	Model: SD7SB6S128G1001	Capacity: 128 GB
Serial Number: 163093400853		
World Wide Name: 5001B444A4DCB5A2		
Reference Number:		
SANITIZATION INFORMATION		
Method Type: NIST Clear	Date(UTC): 21-Jun-23 08:41	
Method Used: Security Erase Unit	Key: JBNXPLYM7GJ3MQ3A	
Method Details:		
Equipment Used: SRMS ORS Version 9.1.W01.6474		
Verification Method: Full Verify		
Post Sanitization Classification:		
Notes:		
OPERATOR INFORMATION		
Name:	Title:	
Group:	Location:	
Signature:		
Website:	Phone:	
VALIDATION INFORMATION		
Name:	Date:	
Organization:	Location:	
		

```

/dev/sg0 - SanDisk SD7SB6S128G1001 - 163093400853 - X3551001 - ATA
*** Full Verification ***
Reference Sector : 0
Device LBA size : 512
Device MaxLBA : 250069679

```

Client Confidential

Contents of Reference LBA 0:

	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F		
0x0000	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
0x0010	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
0x0020	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
0x0030	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
0x0040	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
0x0050	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
0x0060	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
0x0070	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
0x0080	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
0x0090	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
0x00A0	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
0x00B0	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
0x00C0	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
0x00D0	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
0x00E0	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
0x00F0	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
0x0100	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
0x0110	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
0x0120	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
0x0130	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
0x0140	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
0x0150	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
0x0160	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
0x0170	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
0x0180	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
0x0190	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
0x01A0	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
0x01B0	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
0x01C0	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
0x01D0	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
0x01E0	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
0x01F0	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00

*** Checking the Whole Disk ***
Verification Complete - Wed Jun 21 10:25:20 2023

Appendix D – ARC Testing Equipment

Include a table here of the systems and configuration used to conduct the testing

Include a table here of the software and versions used to conduct the testing

Hardware used:

<i>Make</i>	<i>What was it used for?</i>
ARCPC-02	Analysis
ARCPC-05	Disk Verification
ARCPC-08	Disk Verification

Table 10 – Hardware Used

Software used:

<i>Software</i>	<i>Version</i>	<i>What was it used for?</i>
ARC Disk Utility	v1.0.2	Devices overwrite/verification

Table 11 – Software Used