F-RESPONSE NOW/UNIVERSAL™ VALIDATION TESTING REPORT

INCLUDES F-RESPONSE DISCOVERYSHARES™, PHYSICAL DEVICES, PARTITIONS, AND MEMORYSHARES™
# DOCUMENT CONTROL

This is a controlled document produced by F-Response (“F-RESPONSE”). The control and release of this document is the responsibility of the F-RESPONSE document owner. This includes any amendment that may be required.

<table>
<thead>
<tr>
<th>Issue Control</th>
</tr>
</thead>
<tbody>
<tr>
<td>Issue</td>
</tr>
<tr>
<td>Classification</td>
</tr>
<tr>
<td>Document Title</td>
</tr>
<tr>
<td>Approved By</td>
</tr>
<tr>
<td>Released By</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Owner Details</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
</tr>
<tr>
<td>Office Region</td>
</tr>
<tr>
<td>Contact Number</td>
</tr>
<tr>
<td>Email Address</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Revision History</th>
</tr>
</thead>
<tbody>
<tr>
<td>Issue</td>
</tr>
<tr>
<td>1.1</td>
</tr>
<tr>
<td>1.2</td>
</tr>
</tbody>
</table>
## TABLE OF CONTENTS

**Document Control** ................................................................................................................................................................................................. 2

**Testing Results Summary** ............................................................................................................................................................................................ 5

**Introduction** ........................................................................................................................................................................................................ 6

  **Scope** ........................................................................................................................................................................................................... 6

**Purpose** ........................................................................................................................................................................................................ 7

**Document Layout** ..................................................................................................................................................................................................... 8

**Test Results** ........................................................................................................................................................................................................ 9

  **Disk Validity** ....................................................................................................................................................................................................... 9

  **Read Accuracy** ................................................................................................................................................................................................... 10

  **Write Prevention** .................................................................................................................................................................................................. 12

**Test Environment** ........................................................................................................................................................................................................ 13

  **Test Environment Software** ........................................................................................................................................................................ 13

**Test Result Details** .................................................................................................................................................................................................. 14

  **Obtain Baseline (Windows)** ............................................................................................................................................................................ 14

  **Obtain Baseline (Linux)** ................................................................................................................................................................................ 17

  **Obtain Baseline (Apple OS X)** ........................................................................................................................................................................ 20

  **Disk Validity Testing – WinHex** ................................................................................................................................................................. 22

  **Read Accuracy Testing – WinHex, X-Ways** .................................................................................................................................................. 24

  **Write Prevention Testing – Windows** ........................................................................................................................................................ 28

  **Write Prevention Testing – Linux, Apple OS X** ......................................................................................................................................... 34

**Appendix A. Contacts** .................................................................................................................................................................................................. 37

  **Agile Risk Management LLC DBA F-RESPONSE** ............................................................................................................................................. 37

**Appendix B. Legal Notices** .................................................................................................................................................................................. 38
The purpose of this testing is to validate the accuracy and reliability of F-Response Now/Universal™ software using the repeatable test method presented herein. The results of the testing are hereby published for independent validation and peer review.

F-Response Now/Universal™ uses a patent-pending process to create a reliable, read-only connection between an examiner’s computer and a computer under inspection. The function of the F-Response Now/Universal™ Response software tested herein is that an established F-Response Now/Universal™ network connection is completely read-only, functioning much like a software write blocker albeit over a network connection. The testing validates that F-Response Now/Universal™ software protects the integrity of the data on the computer under inspection because it does not permit alteration of any data on the computer under inspection during the test.

The results of our testing confirm that the network connection established by F-Response Now/Universal™ software does reliably and accurately create a read-only connection between an examiner’s computer and a computer under inspection. Our testing uses generally accepted forensics techniques and tools to verify and validate the results. The scientific method presented is done so in accordance with the Daubert Principles (Daubert v. Merrell Dow Pharmaceuticals, Inc. (1993) 509 U.S. 579, 589), and as such we submit that F-Response Now/Universal™ is suitable for use in acquiring data that is intended for use in a court of law.

Unless otherwise noted, all testing activities were performed against the F-Response Now/Universal™ application code base (F-Response Now/Universal™ Discovery, Digital Forensics, and Incident Response Class Appliances), release 1.0.72-5 (Windows, Linux, and Apple OS X).
INTRODUCTION

SCOPE

The scope of this project was limited to the validation and testing of F-Response Now/Universal™ DiscoveryShares™, Physical Devices, and Partitions on the following platforms.

- Microsoft Windows
  - Windows 7 32bit
  - Windows 8.1 64bit
  - Windows Server 2012 64bit
- Linux
  - 3.1x Linux Kernel 32bit
  - 3.1x Linux Kernel 64bit
- Apple OSX
  - Apple OSX 10.8
PURPOSE

This document outlines the F-Response Now/Universal™ Software validation process, results, and methodology developed and executed by F-Response. F-Response Now/Universal™ Software validation answers the following questions:

- Disk Validity
  - Does F-Response Now/Universal™ accurately present the remote Physical Disk(s)?
- Read Accuracy
  - Does F-Response Now/Universal™ correctly and accurately read data from the remote Physical Disk(s)?
- Write Prevention
  - Does F-Response Now/Universal™ effectively prevent write operations from occurring on the remote Physical Disk(s)?
This document will adhere to the following layout:

- **Test Results**
  - Presents a table representing the test results by operating system.

- **Test Environment and Procedure**
  - Presents the environment and procedure used in the testing process.

- **Test Results Details**
  - Presents the detailed results of the testing procedures, including screen captures.
**TEST RESULTS**

**DISK VALIDITY**

*Does F-Response Now/Universal™ accurately present the remote PhysicalDisk(s)?*

In order to test the validity of the locally attached remote F-Response Now/Universal™ physical disk, we collected the total disk size in sectors and the sector size using multiple local data collection sources. This provided a baseline to test against when the F-Response Now/Universal™ disk is attached to our local workstation for analysis. The detailed process used to obtain these results is included in section 4 of this document.

<table>
<thead>
<tr>
<th>DISK VALIDITY TESTING RESULTS</th>
<th>NATIVE (LOCAL MACHINE)</th>
<th>REMOTE (F-RESPONSE NOW/UNIVERSAL™PRESENTED)</th>
<th>RESULT</th>
</tr>
</thead>
<tbody>
<tr>
<td>Platform</td>
<td>Total Sectors</td>
<td>Sector Size</td>
<td>Total Sectors</td>
</tr>
<tr>
<td>WINDOWS 7 X86</td>
<td>83886080</td>
<td>512</td>
<td>83886080</td>
</tr>
<tr>
<td>WINDOWS 8.1 X64</td>
<td>67108864</td>
<td>512</td>
<td>67108864</td>
</tr>
<tr>
<td>WINDOWS SERVER 2012 X64</td>
<td>83886080</td>
<td>512</td>
<td>83886080</td>
</tr>
<tr>
<td>LINUX 3.1 KERNEL X86</td>
<td>83886080</td>
<td>512</td>
<td>83886080</td>
</tr>
<tr>
<td>LINUX 3.1 KERNEL X64</td>
<td>83886080</td>
<td>512</td>
<td>83886080</td>
</tr>
<tr>
<td>APPLE OSX 10.8</td>
<td>83886080</td>
<td>512</td>
<td>83886080</td>
</tr>
</tbody>
</table>
READ ACCURACY

Does F-Response Now/Universal™ correctly and accurately read data from the remote PhysicalDisk(s), Partitions, and DiscoveryShares™?

In order to test the read accuracy of the locally attached remote F-Response Now/Universal™ physical disks, DiscoveryShares™, and partitions, we obtained hash values for the individual files listed below, as well as a portion of the raw disk (Physical Sector 0) from the local F-Response Now/Universal™ device (physical disks and partitions only). Both these hash values were then computed using select Computer Forensics software packages on their native operating system.

<table>
<thead>
<tr>
<th>READ ACCURACY TESTING RESULTS</th>
<th>NATIVE (LOCAL MACHINE)</th>
<th>REMOTE (F-RESPONSE NOW/UNIVERSAL™ PRESENTED)</th>
<th>RESULT</th>
</tr>
</thead>
<tbody>
<tr>
<td>PLATFORM</td>
<td>File Hash</td>
<td>Data Hash</td>
<td>File Hash</td>
</tr>
<tr>
<td>WINDOWS 7 X86 (DISCOVERYSHARE™)</td>
<td>8B88EBBB05A0E56B7 DCC708498C02B3E</td>
<td>N/A</td>
<td>8B88EBBB05A0E56B7 DCC708498C02B3E</td>
</tr>
<tr>
<td>WINDOWS 8.1 X64 (DISCOVERYSHARE™)</td>
<td>ACDBE1ED38167C8B0 1B8F63161BB2CEA</td>
<td>N/A</td>
<td>ACDBE1ED38167C8B0 1B8F63161BB2CEA</td>
</tr>
<tr>
<td>WINDOWS SERVER 2012 X64 (DISCOVERYSHARE™)</td>
<td>928791755FDDEA721 B053535EF84FA17</td>
<td>N/A</td>
<td>928791755FDDEA721 B053535EF84FA17</td>
</tr>
<tr>
<td>LINUX 3.1 KERNEL X86 (DISCOVERYSHARE™)</td>
<td>835F8651D266F285C9 6F5AD2E4066243</td>
<td>N/A</td>
<td>835F8651D266F285C9 6F5AD2E4066243</td>
</tr>
<tr>
<td>LINUX 3.1 KERNEL X64 (DISCOVERYSHARE™)</td>
<td>A66ED71FF10AECA7C 7DA78751F49D2AC</td>
<td>N/A</td>
<td>A66ED71FF10AECA7C 7DA78751F49D2AC</td>
</tr>
<tr>
<td>APPLE OSX 10.8 (DISCOVERYSHARE™)</td>
<td>565140D56B9893751 A53B12A190CE6E6C</td>
<td>N/A</td>
<td>565140D56B9893751 A53B12A190CE6E6C</td>
</tr>
<tr>
<td>WINDOWS 7 X86</td>
<td>8B88EBBB05A0E56B7 DCC708498C02B3E</td>
<td>C9A5A6878D97B48C C965C1E41859F034</td>
<td>8B88EBBB05A0E56B7 DCC708498C02B3E</td>
</tr>
<tr>
<td>WINDOWS 8.1 X64</td>
<td>ACDBE1ED38167C8B0 1B8F63161BB2CEA</td>
<td>C9A5A6878D97B48C C965C1E41859F034</td>
<td>ACDBE1ED38167C8B0 1B8F63161BB2CEA</td>
</tr>
<tr>
<td>WINDOWS SERVER 2012 X64</td>
<td>928791755FDDEA721 B053535EF84FA17</td>
<td>C9A5A6878D97B48C C965C1E41859F034</td>
<td>928791755FDDEA721 B053535EF84FA17</td>
</tr>
<tr>
<td>LINUX 3.1 KERNEL X86</td>
<td>835F8651D266F285C9 6F5AD2E4066243</td>
<td>C9A5A6878D97B48C C965C1E41859F034</td>
<td>835F8651D266F285C9 6F5AD2E4066243</td>
</tr>
<tr>
<td>Operating System</td>
<td>Kernel</td>
<td>Hash 1</td>
<td>Hash 2</td>
</tr>
<tr>
<td>------------------</td>
<td>--------</td>
<td>--------</td>
<td>--------</td>
</tr>
<tr>
<td>LINUX 3.1 KERNEL X64</td>
<td>A66ED71FF10AECA7C 7DA78751F49D2AC</td>
<td>C9A5A6878D97B48C</td>
<td>A66ED71FF10AECA7C 7DA78751F49D2AC</td>
</tr>
</tbody>
</table>
WRITE PREVENTION

Does F-Response Now/Universal™ accurately prevent write operations from occurring on the remote PhysicalDisk(s), partitions, and DiscoveryShares™?

In order to test the write prevention capabilities of F-Response Now/Universal™, we attempted to perform write operations using both the file system create file and delete file commands, as well as through direct writing to arbitrary locations on the F-Response Now/Universal™ connected disk. In all cases F-Response Now/Universal™ prevented the write operations. In some cases, the local system would return a “success” message, however no actual changes occurred on the remote F-Response Now/Universal™ disk. The detailed process used to obtain these results is included in section 4 of this document.

<table>
<thead>
<tr>
<th>SUBJECT PLATFORM</th>
<th>F-RESPONSE NOW/UNIVERSAL PRESENTED DISCOVERY SHARE</th>
<th>F-RESPONSE NOW/UNIVERSAL PRESENTED DISK</th>
<th>RESULT</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>File Deletion</td>
<td>Data Modification</td>
<td></td>
</tr>
<tr>
<td></td>
<td>System Response Actual Result</td>
<td>System Response Actual Result</td>
<td></td>
</tr>
<tr>
<td>WINDOWS 7 X86</td>
<td>Blocked</td>
<td>Blocked</td>
<td>Pass</td>
</tr>
<tr>
<td>WINDOWS 8.1 X64</td>
<td>Blocked</td>
<td>Success</td>
<td>Pass</td>
</tr>
<tr>
<td>WINDOWS SERVER 2012 X64</td>
<td>Blocked</td>
<td>Success</td>
<td>Pass</td>
</tr>
<tr>
<td>LINUX 3.1 KERNEL X86</td>
<td>Blocked</td>
<td>Success</td>
<td>Pass</td>
</tr>
<tr>
<td>LINUX 3.1 KERNEL X64</td>
<td>Blocked</td>
<td>Success</td>
<td>Pass</td>
</tr>
<tr>
<td>APPLE OSX 10.8</td>
<td>Blocked</td>
<td>Success</td>
<td>Pass</td>
</tr>
</tbody>
</table>

1 All write operations are prevented, however select write operations are held in memory where necessary to improve operations. No write operations reach the physical disk. Full details of the write tests performed are available in section 4 of this document.
The following represents a complete listing of the software used to validate F-Response Now/Universal.

| Application                  | Version | Company               | Used for                                                        | Platform                          |
|------------------------------|---------|-----------------------|                                                               |                                  |
| **F-Response Now/Universal™**| 1.0.74-5| F-Response            | Providing remote forensically sound disk access.               | Multiple (See Scope Section)      |
| GNU Tools (md5, dd, dmesg)   | 2.3.5+ (glibc) | Linux  | Baseline data collection on the Linux/OS X target platform.   | Linux (See Scope Section)         |
| Vmware VSphere               | 5.0     | VMWare Inc.           | Hosting F-Response Now/Universal™ Virtual Test Machines        | VMWare Hypervisor                 |
| X-Ways Forensics/Winhex²     | 17      | X-Ways Technology AG  | Verifying capacity, read accuracy.                             | Windows 7 x86                     |

² X-Ways permission granted for use of demonstration licensed version.
Step 1, Open X-Ways WinHex go to Tools->Open Disk and select the first physical disk, record the provided total number of bytes and sector size. Divide the total number of bytes by the sector size to obtain the sector count. Record the provided values.

3 All testing details assume the F-Response Now/Universal Resource has been properly connected using one of the many editions of F-Response Now/Universal software products, as this process is detailed in numerous training manuals and quick start guides available on the F-Response Now/Universal website (www.F-Response Now/Universal.com) it will not be duplicated herein. In addition while only one baseline collection effort is contained herein, this process was repeated for all platforms identified under the Scope section of this document.
Step 2, Obtain file hash value and data hash value, select a system file, double click on it, and select Tools->Compute Hash, select md5 hash and record this value.
Step 3, Select a single sector on the disk, select Tools->Compute Hash (MD5 128 bit), record the resulting hash value.
Step 1, Use "fdisk –l | more" to return the total capacity and bytes per sector on the attached disk(s).

```
Disk /dev/sda: 42.9 GB, 42949672960 bytes
255 heads, 63 sectors/track, 5221 cylinders, total 838860800 sectors
Units = sectors of 1 * 512 = 512 bytes
Sector size (logical/physical): 512 bytes / 512 bytes
I/O size (minimum/optimal): 512 bytes / 512 bytes
Disk identifier: 0x000dfb79

Device Boot Start   End     Blocks  Id  System
/dev/sda1   * 2048 499711  2488322  83 Linux
/dev/sda2  501750 83884031 41691137  5 Extended
/dev/sda5  501760 83884031 41691136  8e Linux LVM

Disk /dev/mapper/lin64-ubuntu14srv-vg-root: 41.6 GB, 41615084288 bytes
255 heads, 63 sectors/track, 5059 cylinders, total 81281024 sectors
Units = sectors of 1 * 512 = 512 bytes
Sector size (logical/physical): 512 bytes / 512 bytes
I/O size (minimum/optimal): 512 bytes / 512 bytes
Disk identifier: 0x00000000

Disk /dev/mapper/lin64-ubuntu14srv-vg-root doesn't contain a valid partition table

Disk /dev/mapper/lin64-ubuntu14srv-vg-swap_1: 1073 MB, 1073741824 bytes
255 heads, 63 sectors/track, 130 cylinders, total 2097152 sectors
Units = sectors of 1 * 512 = 512 bytes
Sector size (logical/physical): 512 bytes / 512 bytes
I/O size (minimum/optimal): 512 bytes / 512 bytes
Disk identifier: 0x00000000
```
Step 2, Use “md5sum </path/to/file>” to return generate the hash of a relevant system file.
Step 3, Use “dd if=/dev/<disk> bs=1b count=1 | md5sum” to generate the hash of a single sector on the disk.
OBTAIN BASELINE (APPLE OS X)

Step 1. Open a terminal window in Apple OS X and type “diskutil info rdisk0” to obtain total disk size in bytes and sector size in bytes.

![Terminal window displaying diskutil info command output]

- Device Identifier: disk0
- Device Node: /dev/disk0
- Part of Whole: disk0
- Device / Media Name: APPLE MOD HT5547558A9E384 Media
- Volume Name: Not applicable (no file system)
- Mounted: Not applicable (no file system)
- File System: None
- Content (IOCContent): GUID_partition_scheme
- OS Can Be Installed: No
- Media Type: Generic
- Protocols: GDATA
- SMART Status: Verified
- Total Size: 580.1 GB (5691876462072 bytes) (exactly 576773168 512-byte-Blocks)
- Volume Free Spaces: Not applicable (no file system)
- Device Block Size: 512 Bytes
- Read-Only Media: No
- Read-Only Volume: Not applicable (no file system)
- Ejectable: No
- Whole: Yes
- Internal: Yes
- Solid State: No
- OS 9 Drivers: No
- Low Level Format: Not supported
- Device Location: "Lower"
Step 2, Open a Terminal window in Apple OS X and use the following commands to obtain file and data hashes "md5 <path/to/file>" and "dd if=/dev/rdisk0 bs=1b count=1 | md5".

```
sh-3.2# md5 /mach_kernel >> osx-hash.txt
sh-3.2# dd if=/dev/rdisk0 bs=1b count=1 | md5 >> osxhash.txt
dd: unknown operand bs=1b
sh-3.2# dd if=/dev/rdisk0 bs=1b count=1 | md5 >> osxhash.txt
1+0 records in
1+0 records out
512 bytes transferred in 0.038748 secs (16652 bytes/sec)
sh-3.2#
```
DISK VALIDITY TESTING – WINHEX

Step 1: Open X-Ways Forensics go to Tools -> Open Disk and select the F-Response Now/Universal presented physical resource.
Step 2, Note Total capacity. Divide total number of bytes by number of bytes per sector to obtain total sector count.
READ ACCURACY TESTING – WINHEX, X-WAYS

Step 1, Open F-Response Now/Universal presented disk/share in X-Ways. Note total number of bytes and bytes per sector and compare to baseline.
Step 2, Select the sector of disk hashed previously during the baseline gathering phase. Press Ctrl-F2 to bring up the hashing dialog. Select MD5 as the hashing type and press Ok, record and compare resulting hash with hash obtained during baseline operation.
Step 3, Browse and select file. Choose Specialist -> Refine Volume Snapshot -> Compute hash MD5(128 bit) -> Option button for 'Apply to tagged files only' -> OK button to calculate Hash value.
Step 4, Record and review the resulting hash value.
WRITE PREVENTION TESTING – WINDOWS

Step 1, Open newly mounted F-Response Now/Universal Discovery Share, select a file, type Delete or Shift+Delete to attempt to delete the file--Option does not exist.
Step 2, Select a file from the local disk and attempt to copy and paste it to the F-Response Now/Universal Discovery Share.
Step 3, Open Disk Manager to review the F-Response Now/Universal presented physical disk. Note the system sees the disk as Read Only.
Step 4, Open WinHex and navigate to Tools -> File Tools -> Wipe Securely -> Choose a file from the F-Response Now/Universal presented source(s)
Step 5, ->Click Delete->OK->OK
Step 6, Return to F-Response Now/Universal testing computer, confirm no data changes have occurred.
WRITE PREVENTION TESTING – LINUX, APPLE OS X

Step 1, Open the attached disk using X-Ways Forensics, record the value of sector zero.
Step 2, Use Winhex to Wipe Start Sectors securely.
Step 3, On the original disk, dump the sector in question using dd and hexdump, compare the resulting values to confirm no writes have taken place.
APPENDIX A. CONTACTS

Agile Risk Management LLC DBA F-RESPONSE

3333 W Kennedy Blvd Suite 201
Tampa, FL 33609

Table 1: Agile Risk Management LLC Contacts

<table>
<thead>
<tr>
<th>Contact</th>
<th>Title</th>
<th>Contact Information</th>
</tr>
</thead>
<tbody>
<tr>
<td>Matthew Shannon</td>
<td>Principal</td>
<td><a href="mailto:mshannon@f-response.com">mshannon@f-response.com</a></td>
</tr>
<tr>
<td>Matthew Decker</td>
<td>Principal</td>
<td><a href="mailto:mjdecker@f-response.com">mjdecker@f-response.com</a></td>
</tr>
</tbody>
</table>
Appendix B. Legal Notices

Copyright © 2014 Agile Risk Management, LLC. All rights reserved.

This document is protected by copyright with all rights reserved.

Trademarks

F-Response® is a registered trademark of Agile Risk Management, LLC. All other product names or logos mentioned herein are used for identification purposes only, and are the trademarks of their respective owners.

Statement of Rights

Agile Risk Management, LLC products incorporate technology that is protected by U.S. patent and other intellectual property (IP) rights owned by Agile Risk Management LLC, and other rights owners. Use of these products constitutes your legal agreement to honor Agile Risk Management, LLC’s IP rights as protected by applicable laws. Reverse engineering, de-compiling, or disassembly of Agile Risk Management, LLC products is strictly prohibited.

Disclaimer

While Agile Risk Management LLC has committed its best efforts to providing accurate information in this document, we assume no responsibility for any inaccuracies that may be contained herein, and we reserve the right to make changes to this document without notice.