

Independent Validation & Verification
Of
**Storage Media Archival Recovery Toolkit
(SMART)**

February 2002

Thomas Rude, CISSP
Security Consultant
Red Hat, Inc.

<u>TABLE OF CONTENTS</u>	<u>Page</u>
I. Overview	3
II. Test Bed	4
III. Set Up	4
IV. Methodology	5
V. Results	6-7
VI. Appendix A (step-by-step)	8-11

I. Overview

The purpose of this project is to perform an Independent Validation and Verification (IV&V) of the *Storage Media Archival Recovery Toolkit (SMART)*, BeOS Platform, by **ASR Data and Acquisition, LLC**.

SMART is a software program that enables the program user to perform the following actions:

- make bit stream copies of data (imaging)
- authenticate data (hashing)
- wipe media (wiping)
- restore data (restoring)

In order to validate the accuracy of *SMART*, the following functionalities will be tested:

- Authenticate
- Image
- Wipe
- Restore

Verification of these validations will be provided by using two other software toolsets:

- 1) BeOS *md5sum* and *dd*
- 2) Linux *md5sum* and *dd*

Both BeOS and Linux are operating systems. *Md5sum* and *dd* are commands that can be issued by a user within these operating system environments. By using not one, but two toolsets, the odds of detecting an error within the *SMART* program are greater. And by using two different operating systems verifying the accuracy of *SMART* becomes more concrete.

Having the results match from all three toolsets on both platforms lends great credibility to both the functionality and accuracy of the *SMART* program.

II. Test Bed

The following resources will be used for this IV&V:

Personal Computer:	Compaq Deskpro EN Series
Processor Type:	Intel Pentium II
Processor Speed:	300/66 MHz
Memory Size:	128 MB
Primary Drive 0:	Maxtor Hard Drive, Model DiamondMax Plus
Primary Drive 1:	Not Installed
Secondary Drive 0:	ATAPI Device (CD-ROM)
Secondary Drive 1:	Seagate Hard Drive, Model ST33221A
Operating System 1:	BeOS Professional 5.03
Operating System 2:	Red Hat Linux 7.2
Validation Tool:	<i>SMART for BeOS</i>
Verification Tools:	md5sum (textutils package) v2.0 on BeOS dd (fileutils package) v4.0 on BeOS md5sum (textutils package) v2.0.14 on Linux dd (fileutils package) v4.1 on Linux

III. Set Up

The system will be configured as follows:

- Primary Drive 0:
 - 20GB capacity
 - Test Drive
 - Operating Systems: BeOS 5.03 and Red Hat Linux 7.2
 - Validation Tool: *SMART*
 - Verification Tools: md5sum, dd
- Secondary Drive 1:
 - 3.2GB capacity
 - Evidentiary Drive
 - Operating Systems: Red Hat Linux 7.2

IV. Methodology

- 1) Hash Secondary Drive 1 (Evidentiary)
 - *SMART* authentication function
 - *md5sum* in BeOS
 - *md5sum* in Red Hat Linux
- 2) Image Secondary Drive 1 (Evidentiary)
 - *SMART* image function
 - *dd* in BeOS
 - *dd* in Red Hat Linux
- 3) Hash Images of Secondary Drive 1 (Evidentiary)
 - *SMART* authentication function
 - *md5sum* in BeOS
 - *md5sum* in Red Hat Linux
- 4) Wipe Secondary Drive 1 (Evidentiary)
 - *SMART* wipe function
- 5) Hash *SMART*-wiped Secondary Drive 1 (Evidentiary)
 - *SMART* authentication function
 - *md5sum* in BeOS
 - *md5sum* in Red Hat Linux
- 6) Restore *SMART* image of Secondary Drive 1 (Evidentiary)
 - *SMART* restore function
- 7) Hash *SMART*-restored Secondary Drive 1 (Evidentiary)
 - *SMART* authentication function
 - *md5sum* in BeOS
 - *md5sum* in Red Hat Linux

V. Results

The results of the Independent Validation and Verification Authentication process are summarized in *Table 1* below:

	Secondary Drive 1 (Evidentiary)	SMART Secondary Drive 1 Imaged (Evidentiary)	SMART Secondary Drive 1 Wiped (Evidentiary)	SMART Secondary Drive 1 Restored (Evidentiary)
SMART Authentication	b5030dfce8a5ea008c1cdf8356513c63	b5030dfce8a5ea008c1cdf8356513c63	2a284aa5b643cf2d8bc02f585bcd4c10	b5030dfce8a5ea008c1cdf8356513c63
BeOS md5sum	b5030dfce8a5ea008c1cdf8356513c63	b5030dfce8a5ea008c1cdf8356513c63	2a284aa5b643cf2d8bc02f585bcd4c10	b5030dfce8a5ea008c1cdf8356513c63
Red Hat Linux md5sum	b5030dfce8a5ea008c1cdf8356513c63	b5030dfce8a5ea008c1cdf8356513c63	2a284aa5b643cf2d8bc02f585bcd4c10	b5030dfce8a5ea008c1cdf8356513c63

Table 1: Summary of Authentication Values

Based upon the set up and methodology the following would be expectations:

- 1) All three hash values for the original Evidentiary (Secondary Drive 1 (Slave)) hard drive would be equivalent
- 2) All three hash values for the *SMART*-imaged Evidentiary (*SMART* Secondary Drive 1 Image) hard drive would be equivalent
- 3) All three hash values for the BeOS *dd* imaged Evidentiary hard drive would be equivalent
- 4) All three hash values for the Red Hat Linux *dd* imaged Evidentiary hard drive would be equivalent
- 5) All three hash values for the *SMART*-wiped Evidentiary (*SMART* Secondary Drive 1 Wiped) hard drive would be equivalent, but not equal to any other values calculated during the process
- 6) All three hash values for the *SMART*-restored Evidentiary (*SMART* Secondary Drive 1 Restored) hard drive would be equivalent

As shown in *Table 1* all hash (authentication) values are equivalent where we would expect them to be equivalent (the original Evidentiary drive, the *SMART*-created image of the Evidentiary drive, and the *SMART*-restored image of the Evidentiary drive).

The hash values are also equivalent to one another for the *SMART*-wiped Evidentiary drive, yet this value is different from all three other values (as we would expect it to be).

Note that the two images created by both BeOS and Red Hat Linux *dd* do not appear in *Table 1*. We were not testing the validity of either BeOS *dd* or Red Hat Linux *dd*. These were used to verify that *SMART* did indeed create a bit image copy of the Evidentiary drive. These hash values do appear in *Table 2* below for reference.

	<i>BeOS dd</i> Secondary Drive 1 Imaged (Evidentiary)	<i>Red Hat Linux dd</i> Secondary Drive 1 Imaged (Evidentiary)
SMART Authentication	b5030dfce8a5ea008c1cdf835651 3c63	b5030dfce8a5ea008c1cdf835651 3c63
BeOS md5sum	b5030dfce8a5ea008c1cdf835651 3c63	b5030dfce8a5ea008c1cdf835651 3c63
Red Hat Linux md5sum	b5030dfce8a5ea008c1cdf835651 3c63	b5030dfce8a5ea008c1cdf835651 3c63

Table 2: Summary of Authentication Values for BeOS and Red Hat Linux *dd* Images

Interpreting the findings we see that each of the four functionalities of *SMART* has been validated:

- The hash value of the original Evidentiary hard drive calculated by *SMART* is verified by the equal values calculated by *md5sum* on both the BeOS and Red Hat Linux platforms (Authentication)
- The *SMART* image of the Evidentiary hard drive is equal in value to both images created by both BeOS and Red Hat Linux *dd*. All three hash values for all three Evidentiary images are identical, using all three programs (Image)
- The *SMART* wipe of the Evidentiary hard drive is verified by the equal hash values calculated by *md5sum* on both the BeOS and Red Hat Linux platforms for the *SMART* wiped Evidentiary hard drive. This wiped value is not equal to either the original Evidentiary hard drive nor the images of the Evidentiary hard drive (Wipe)
- The *SMART* restored Evidentiary image to the wiped Evidentiary hard drive is verified by the equal hash values calculated by *md5sum* on both BeOS and Red Hat Linux for this restored image on the Evidentiary hard drive (Restore)

The findings for the IV&V are summarized in *Table 3*:

SMART function	Passed	Failed
Authenticate	X	
Image	X	
Wipe	X	
Restore	X	

Table 3: Validation Findings Summary

VI. Appendix A (step-by-step)

- Power on the PC
- Boot into BeOS
- Start up *SMART* program
- Create a new job titled 'Validation'
- Navigate to 'Disks & Partitions' tab
- From the 'All Physical Disks' area right-click '/dev/disk/ide/ata/1/slave/0/raw' and select 'Authenticate.' This calculates the hash value for the Evidentiary (Secondary Drive 1 Slave) hard drive as:

SHA1: 8d2b8688 653982cf dce761b6 dfac5473 ec6387e2
MD5: b5030dfce8a5ea008c1cdf8356513c63
CRC32: 3998191527

- Close the *SMART* program
- Shutdown the PC
- Power on the PC
- Boot into Red Hat Linux
- Issue the command 'md5sum /dev/hdd' to calculate the hash value of the Evidentiary (Secondary Drive 1 Slave) hard drive. The result:
b5030dfce8a5ea008c1cdf8356513c63

- Shutdown the PC
- Power on the PC
- Boot into BeOS
- Issue the command 'md5sum /dev/disk/ide/ata/1/slave/0/raw' to calculate the hash value of the Evidentiary (Secondary Drive 1 Slave) hard drive. The result:
b5030dfce8a5ea008c1cdf8356513c63

NOTE: All three hash values for the original Evidentiary drive have been calculated in the steps above.

- Start up *SMART* program
- Open the 'Validation' job
- Navigate to 'Disks & Partitions' tab
- Under 'All Physical Disks' right-click on '/dev/disk/ide/ata/1/slave/0/raw' and select 'Acquire' 'To a Single Image File.' This will acquire the physical device Evidentiary hard drive into a single image file.
- (Wait for imaging process to complete)
- Navigate to 'Disk Images' tab in *SMART*. Right-click on image file created in step above, select 'Authenticate' 'Against a Disk/Partition', view the 'All Physical Disks' area and select '/dev/disk/ide/ata/1/slave/0/raw', finish by clicking 'Authenticate' button. This will authenticate the image created by *SMART* against the hash value for the Evidentiary hard drive. The result:

'Authenticate Against Disk/Partition: Authenticity Verified!'

- Close the *SMART* program

NOTE: The *SMART* image of the Evidentiary hard drive has now been created.

- Issue the command `'md5sum /dev/disk/ide/ata/1/slave/0/raw'` to calculate the hash value of the Evidentiary (Secondary Drive 1 Slave) hard drive. The result:

b5030dfce8a5ea008c1cdf8356513c63

- Shutdown the PC
- Power on the PC
- Boot into Red Hat Linux
- Issue the command `'md5sum /dev/hdd'` to calculate the hash value of the Evidentiary (Secondary Drive 1 Slave) hard drive. The result:

b5030dfce8a5ea008c1cdf8356513c63

NOTE: Calculating these two *md5sum* values verifies that the *SMART* program did not change any bits on the Evidentiary hard drive during the imaging process.

- Issue the command `'dd if=/dev/hdd of=LinuxValidationImage bs=512 conv=noerror'`

- (Wait for the process to complete)

- Issue the command `'md5sum -b LinuxValidationImage'`

b5030dfce8a5ea008c1cdf8356513c63

- Shutdown the PC
- Power on the PC
- Boot into BeOS
- Issue the command `'dd if=/dev/disk/ide/ata/1/slave/0/raw of=BeValidationImage bs=512 conv=noerror'`

- (Wait for process to complete)

- Issue the command `'md5sum -b BeValidationImage'`

b5030dfce8a5ea008c1cdf8356513c63

- Navigate to Red Hat Linux partition
- Issue the command `'md5sum -b LinuxValidationImage'` the result:

b5030dfce8a5ea008c1cdf8356513c63

- Shutdown the PC
- Power on the PC
- Boot into Red Hat Linux
- Issue the command `'mount -t befs -o ro,noexec /dev/hda4 /mnt/mymount'`

- Issue the command `'md5sum -b BeValidationImage'` and the result is:
b5030dfce8a5ea008c1cdf8356513c63
- Compare *md5sum* values for these two images against the value for the image created by *SMART*

NOTE: By using *dd* in BeOS and Red Hat Linux to create images of the Evidentiary drive these images can be hashed and their values compared against the value for the image created by *SMART*. If all values are equivalent then all images are identical.

- Shutdown the PC
- Power on the PC
- Boot into BeOS
- Start up *SMART* program
- Open 'Validation' job
- Navigate to 'Disks & Partitions' tab
- From the 'All Physical Disks' area right-click on `'/dev/disk/ide/ata/1/slave/0/raw'` and select 'Wipe' This will wipe the original Evidentiary hard drive.
- (Wait for wiping process to complete)
- From the 'All Physical Disks' area right-click on `'/dev/disk/ide/ata/1/slave/0/raw'` and select 'Authenticate' to produce a hash value for the wiped Evidentiary hard drive. The result is:
SHA1: e02c5ad9 6884794d c29ceb08 fef5e0fc cb12d031
MD5: 2a284aa5b643cf2d8bc02f585bcd4c10
CRC32: 2885298984

- Create a new job 'Image Validation'
- Right-click in 'Image Validation' Job tab and select 'Import Image'
- Import both BeOS and Red Hat Linux *dd* images
- Right-click on each image and select 'Authenticate' to produce hash value for each

- Close the *SMART* program
- Issue the command `'md5sum -b /dev/disk/ide/ata/1/slave/0/raw'` to calculate the hash value for the *SMART* wiped Evidentiary hard drive. The result of this command is:
2a284aa5b643cf2d8bc02f585bcd4c10

- Shutdown the PC
- Power on the PC
- Boot into Red Hat Linux
- Issue the command `'md5sum /dev/hdd'` to calculate the hash value for the *SMART* wiped Evidentiary hard drive. The result is:
2a284aa5b643cf2d8bc02f585bcd4c10

- Shutdown the PC

NOTE: In the steps above *SMART* was used to wipe the Evidentiary hard

drive, and then produce a hash value for this wiped Evidentiary hard drive. Using *md5sum* in BeOS and Red Hat Linux a second set of hash values were calculated for the *SMART* wiped Evidentiary hard drive. These values match the value calculated by *SMART*.

- Power on PC
- Boot into BeOS
- Start the *SMART* program
- Navigate to 'Disk Images' tab
- Right-click on the Evidentiary image created by *SMART* and select 'Restore Image to Physical Device' This will restore the image back to the wiped Evidentiary hard drive.
- (Wait for the restore process to complete)
- Navigate to 'Disks & Partitions' tab
- Under 'All Physical Disks' area right-click on '/dev/disk/ide/ata/1/slave/0/raw' and select 'Authenticate' The result of this is:
 - SHA1: 8d2b8688 653982cf dce761b6 dfac5473 ec6387e2
 - MD5: b5030dfce8a5ea008c1cdf8356513c63
 - CRC32: 3998191527
- Close the *SMART* program
- Issue the command 'md5sum -b /dev/disk/ide/ata/1/slave/0/raw' to calculate the value of the Evidentiary hard drive. The result:
 - b5030dfce8a5ea008c1cdf8356513c63
- Shutdown the PC
- Power on the PC
- Boot into Red Hat Linux
- Issue the command 'md5sum -b /dev/hdd' to calculate the value of the Evidentiary hard drive. The result:
 - b5030dfce8a5ea008c1cdf8356513c63
- Shutdown the PC

NOTE: In these last steps *SMART* was used to restore the *SMART*-created image back to the Evidentiary hard drive. After the restoration was complete a hash value was calculated. Then, using *md5sum* in both BeOS and Red Hat Linux the value of the restored Evidentiary hard drive was calculated. All values are identical. And, these restored values equal the original values of the Evidentiary hard drive, indicating that the *SMART* program made a complete bit-image copy of the Evidentiary hard drive and was successful in restoring that image back to the Evidentiary hard drive.

Thomas Rude, CISSP
Red Hat, Inc.
farmerdude@crazytrain.com