


Validation Report

ForensicSoft Safe Block




DCCI-2010-P000035

July 2011


Francis Westerman
Digital Forensic Engineer

7 July 2011
Date

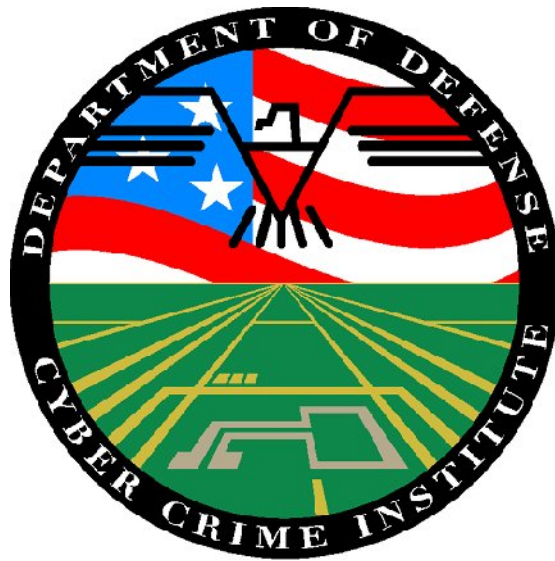

William Eber
Director,
Defense Cyber Crime Institute

7 July 2011
Date

FOR OFFICIAL USE ONLY
Defense Cyber Crime Institute

Validation Report

ForensicSoft Safe Block



DCCI-2010-P000035

July 2011

Francis Westerman
Digital Forensic Engineer

Date

William Eber
Director,
Defense Cyber Crime Institute

Date

FOR OFFICIAL USE ONLY
Defense Cyber Crime Institute

Table of Contents

1.0 Purpose and Scope	1
2.0 References	1
3.0 Requirements.....	1
4.0 Results.....	2
5.0 Findings.....	2
Appendix A: Test Details	3
Appendix B: Test Software and Hardware	7
Appendix C: Test Data Sets	8

FOR OFFICIAL USE ONLY
Defense Cyber Crime Institute

1.0 Purpose and Scope

- 1.1 The purpose of this project is to validate Forensic Soft Incorporated's Safe Block, hereinafter referred to as, Safe Block.
- 1.2 Safe Block was developed by Forensic Soft Incorporated. SAFE Block is a software-based write blocker which facilitates the quick and safe acquisition and/or analysis of any disk or flash storage media attached directly to a Windows workstation. It is proven to be safe.
- 1.3 The testing detailed in this Validation Report is intended to determine whether the specific requirements, as outlined in Section 3.0, are satisfied. The testing is limited to validating features and capabilities as identified by the requesting party. This report does not imply or constitute an endorsement by DC3, the Defense Cyber Crime Institute (DCCI), or the United States Government.
- 1.4 The DCCI developed this validation to determine the extent and circumstances under which computer crime investigating agents assigned to Defense Criminal Investigative Organizations (DCIOs) may employ Safe Block for digital forensic imaging and extraction of evidence. The validation process is not intended to test every possible feature of Safe Block.

2.0 References

N/A

3.0 Requirements

- 3.1 Baseline Requirements (Pre-defined)
 - 3.1.1 Installs on Windows XP and Windows 2003.
 - 3.1.2 Configurable as to which if any mass storage devices are to be locked.
 - 3.1.3 When locked, mass storage devices are in write protect mode.
 - 3.1.4 Detects and can remove hpa's and dco's.
- 3.2 Customer Requirements (User-defined)

N/A

4.0 Results

Result	Requirement(s)
Satisfied	3.1.1, 3.1.2, 3.1.3
Not Satisfied	3.1.4

5.0 Findings

5.1 Details of Requirements not satisfied.

5.1.1 Unable to perform HPA/DCO testing due to not having any native IDE ports on MAC pro and SATA native is not supported in current version. It was already known that this requirement would fail. For this reason the tests for this requirement were not conducted.

5.2 Observations and/or Anomalies of interest that do not affect the ability of the tool to meet Baseline and Customer Requirements (e.g. unexpected behavior, workarounds).

N/A

FOR OFFICIAL USE ONLY
Defense Cyber Crime Institute

Appendix A: Test Details

This appendix details each test that was performed by the Engineer in order to identify whether the tool satisfies, or does not satisfy, the Requirements as outlined in Section 3.

Note: Column 6, Reference(s), corresponds to Findings, Anomalies and/or Observations, as identified in Section 5.

The following tests and results were obtained from a 64-bit Windows Server 2003 operating system on a MACPRO platform:

Test ID:	Req(s):	Test Description:	Expected Result:	Actual Result:	Ref:
1.1	3.1.1	Install Forensic Soft Incorporated's Safe Block software.	Software will install and be ready to execute and configure.	Expected Result Obtained	N/A
1.2	3.1.2	Start GUI and go to setup and set all devices fixed and removable to be locked, and also set to remember status of fixed disks. Two drives are already in the SATA bays. Reboot system and check status of the fixed drives in SATA bays.	GUI will allow, after password logon, for the setup of the fixed devices and removable devices. Remember status is set and the exit is pressed. After reboot, restarted GUI, and after logon the SATA drives are locked.	Expected Result Obtained	N/A
1.3	3.1.2	Start GUI and go to setup and set all devices fixed and removable to be unlocked, and also set to not remember status of fixed disks. Two drives are already in the SATA bays. Reboot system and check status of the fixed drives in SATA bays.	GUI will allow, after password logon, for the setup of the fixed devices and removable devices. Remember status is turned off and the exit is pressed. After reboot restarted GUI and after logon the SATA drives are unlocked.	Expected Result Obtained	N/A

FOR OFFICIAL USE ONLY
Defense Cyber Crime Institute

Test ID:	Req(s):	Test Description:	Expected Result:	Actual Result:	Ref:
1.4	3.1.3	Attach hashed non-formatted drive to system and in drive manager. Try to initialize drive.	Windows will return error due to drive being protected and will not modify drive. Hash drive and receive matching hash.	Expected Result Obtained	N/A
1.5	3.1.3	Attach hashed formatted USB stick drive to system and in drive manager. Try to format drive.	Windows will return error due to drive being protected and will not modify drive. Hash drive and receive matching hash.	Expected Result Obtained	N/A
1.6	3.1.3	Attach hashed formatted firewire drive to system and in drive manager. Try to format drive.	Windows will return error due to drive being protected. And will not modify drive. Hash drive and receive matching hash..	Expected Result Obtained	N/A

FOR OFFICIAL USE ONLY
Defense Cyber Crime Institute

The following tests and results were obtained from a 32-bit Windows XP operating system on a MACPRO platform:

Test ID:	Req(s):	Test Description:	Expected Result:	Actual Result:	Ref:
2.1	3.1.1	Install Forensic Soft Incorporated's Safe Block software.	Software will install and be ready to execute and configure.	Expected Result Obtained	N/A
2.2	3.1.2	Start GUI and go to setup and set all devices fixed and removable to be locked. Set remember status of fixed disks. Two drives are already in the SATA bays. Reboot system and check status of the fixed drives in SATA bays.	GUI will allow, after password logon, for the setup of the fixed devices and removable devices. Remember status is set and the exit is pressed. After reboot, restarted GUI, and after logon the SATA drives are locked.	Expected Result Obtained	N/A
2.3	3.1.2	Start GUI and go to setup and set all devices fixed and removable to be unlocked and also set to not remember status of fixed disks. Two drives are already in the SATA bays. Reboot system and check status of the fixed drives in SATA bays.	GUI will allow, after password logon, for the setup of the fixed devices and removable devices. Remember status is turned off and the exit is pressed. After reboot, restarted GUI, and after logon the SATA drives are unlocked.	Expected Result Obtained	N/A
2.4	3.1.3	Attach hashed non-formatted drive to system and in drive manager, try to initialize drive.	Windows will return error due to drive being protected. And will not modify drive. Hash drive and receive matching hash.	Expected Result Obtained	N/A

FOR OFFICIAL USE ONLY
Defense Cyber Crime Institute

Test ID:	Req(s):	Test Description:	Expected Result:	Actual Result:	Ref:
2.5	3.1.3	Attach hashed formatted USB stick drive to system and in drive manager, try to format drive.	Windows will return error due to drive being protected. And will not modify drive. Hash drive and receive matching hash.	Expected Result Obtained	N/A
2.6	3.1.3	Attach hashed formatted firewire drive to system and in drive manager, try to format drive.	Windows will return error due to drive being protected. And will not modify drive. Hash drive and receive matching hash.	Expected Result Obtained	N/A

FOR OFFICIAL USE ONLY
Defense Cyber Crime Institute

Appendix B: Test Software and Hardware

This appendix details any and all software titles used in conjunction with this Validation. When applicable, additional hardware is identified that was used during the course of testing (e.g. write-blockers). Specific details are also present regarding the workstation that was used to conduct the testing.

Software:

Tool	Version	Developer
Microsoft Windows	XP 32-Bit	Microsoft Inc
Microsoft Windows	Windows 2003 Server 64-Bit	Microsoft Inc
Safe Block	Ver 1.3	Forensic Soft Incorporated

Additional Hardware:

Device	Manufacturer	Model Number	Serial Number
N/A	N/A	N/A	N/A

Workstation:

Workstation 1

Feature/Model	Mac Pro (Early 2008)(64-bit)
Form factor	Tower
Motherboard	Apple Inc. Mac-F42C88C8 Proto 1
Processor	8 Core: Two 2.8 GHz, Quad-core Intel Xeon 5400 series processors
Memory	(8) 4GB of 800MHz DDR2 ECC fully buffered DIMM
Graphics	nVidia GeForce 8800 GT (512MB) Dual-DVI (PCIe)
External Devices	N/A
Examination Drive	N/A
Data Storage Drive	N/A

FOR OFFICIAL USE ONLY
Defense Cyber Crime Institute

Appendix C: Test Data Sets

Device	Manufacturer	Model Number	HASH
80 gig SATA hd	Western Digital	WD800AAJS	Md5- a096a6401cf7ff4e9584c4b2fe105b2f
80 gig SATA hd	Western Digital	WD800AAJS	Md5- 731a4e18bbe996875326210fe3f6203f
4 gig USB stick	Kingston	DataTraveler secure	Md5- 9066bce071e849d373585a327ad10308
320 gig firewire external drive	Western Digital	Passport Studio 320	Md5- e8df8cb109a019c27004bb78a6a160d1