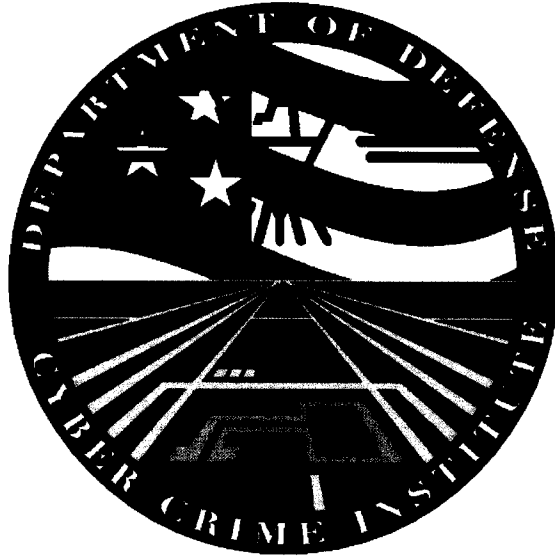



# Validation Report

## ForensicSoft Safe Boot Disk



**DCCI-2010-P000034**

**April 2012**

  
Francis Westerman  
Digital Forensic Engineer  
Date 18 APR 12

  
William Eber  
Director,  
Defense Cyber Crime Institute  
Date 18 APR 12

# Validation Report

## ForensicSoft Safe Boot Disk



**DCCI-2010-P000034**

**April 2012**

---

**Francis Westerman**  
Digital Forensic Engineer

Date

---

**William Eber**  
Director,  
Defense Cyber Crime Institute

Date

## Table of Contents

<b>1.0 Purpose and Scope .....</b>	<b>1</b>
<b>2.0 References .....</b>	<b>1</b>
<b>3.0 Requirements.....</b>	<b>1</b>
<b>4.0 Results.....</b>	<b>2</b>
<b>5.0 Findings.....</b>	<b>2</b>
<b>Appendix A: Test Details .....</b>	<b>3</b>
<b>Appendix B: Test Software and Hardware .....</b>	<b>6</b>
<b>Appendix C: Test Data Sets .....</b>	<b>7</b>

**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 boot Disk, hereinafter referred to as, Safe-Disk.
- 1.2 Safe-Disk was developed by Forensic Soft Incorporated. Safe-Disk is a boot disk (CD or USB) which, with a USB dongle, boots a computer to a forensically sound (write blocked) version of Windows, that serves as a platform for all popular Windows forensics tools.
- 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 the Defense Cyber Crime Center (DC30, 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-Disk for digital forensic imaging and extraction of evidence. The validation process is not intended to test every possible feature of Safe-Disk.

## **2.0 References**

SAFE\_Boot\_Help file down loaded from vendor web site.

## **3.0 Requirements**

- 3.1 Baseline Requirements (Pre-defined)
  - 3.1.1 Create bootable CD of SAFE\_BOOT.
  - 3.1.2 Creates a USB tools disk, and adds dc3dd to it.
  - 3.1.3 Write-blocks all drives, except boot CD drive, after startup.
  - 3.1.4 Write-blocks all externally added drives.
  - 3.1.5 Can unlock drives to use to write on (to image to).
  - 3.1.6 USB dongle can be either Consultant type or Enterprise type.
- 3.2 Customer Requirements (User-defined)

N/A

## 4.0 Results

Result	Requirement(s)
Satisfied	3.1.1, 3.1.2, 3.1.3, 3.1.4, 3.1.5, 3.1.6
Not Satisfied	N/A

## 5.0 Findings

5.1 Details of Requirements not satisfied.

N/A

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).

5.2.1 The boot disk was created using SAFE ISO image. (Satisfies REQ 3.1.1).

5.2.2 Tools USB-thumb drive was built using SAFETools2 installed program. Dc3dd was added to the tools disk and the eSATA drivers for the eSATA cards on the MAC PRO were also added. (Satisfies REQ 3.1.2).

5.2.3 A boot USB-thumb drive can be created using SAFEUSBv121 installed program.

5.2.4 The boot disk and the tools USB-thumb drive were pre-created, and will be used for all testing.

5.2.5 After drives, showing locked on system display, will attempt to store data on them. After the failure message, the drives were rehashed and found to be unaltered.

5.2.6 After drives, showing locked on system display, are unlocked, they will attempt to store data on them. And once completed, the drives were rehashed and found to be altered.

5.2.7 The Consultant dongle, when removed, will cause shutdown after 1minute if not returned to USB port. The Enterprise dongle can be removed after startup and the system will continue to operate without a time limit.

**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 ForensicSoft boot disk and a tools USB-thumb drive on a MACPRO platform using a Consultant dongle:***

<b>Test ID:</b>	<b>Req(s):</b>	<b>Test Description:</b>	<b>Expected Result:</b>	<b>Actual Result:</b>	<b>References:</b>
1.0	3.1.1	Burn SAFE.ISO file to CD for the boot disk.	Bootable CD will be created.	Expected Result Obtained	5.2.1, 5.2.3
1.1	3.1.2	Using 8Gig USB thumb drive run Safetools program to create tools disk then copy dc3dd(windows version )to the root directory.	Tools disk with dc3dd will be created.	Expected Result Obtained	5.2.2
1.2	3.1.3	Boot Mac Pro using Safe boot disk and a safe consultant dongle, inspect all drives on system to check status.	All drives except the boot CD drive will be write protected, including the tools drive.	Expected Result Obtained	5.2.4, 5.2.5
1.3	3.1.4	Plugin eSata drive and USB drive, they should mount in the locked mode.	Plugged in USB drive and eSata drives, will mount on system in a locked mode.	Expected Result Obtained	5.2.4, 5.2.5
1.4	3.1.5	All locked drives can be unlocked and written to as needed and then can be relocked.	All drives will unlock can have a file written to them then relocked.	Expected Result Obtained	5.2.4, 5.2.6

**FOR OFFICIAL USE ONLY**  
**Defense Cyber Crime Institute**

1.5	3.1.6	Remove consultant USB dongle.	There will be a dialogue box that says the dongle is missing and you have one minute to replace. If replaced, click on retry and the message goes away and the session continues. If it is not replaced, you are given 2 minutes to save log file before the system is shut-down.	Expected Result Obtained	5.2.7
-----	-------	-------------------------------	---	--------------------------	-------

**FOR OFFICIAL USE ONLY**  
**Defense Cyber Crime Institute**

*The following tests and results were obtained from a ForensicSoft boot disk and a tools USB-thumb drive on a MACPRO platform using an Enterprise dongle:*

<b>Test ID:</b>	<b>Req(s):</b>	<b>Test Description:</b>	<b>Expected Result:</b>	<b>Actual Result:</b>	<b>References:</b>
2.0	3.1.1	Burn SAFE.ISO file to CD for the boot disk.	Bootable CD will be created.	Expected Result Obtained	5.2.1, 5.2.3
2.1	3.1.2	Using 8Gig USB thumb drive run Safetools program to create tools disk. Copy dc3dd (windows version) to the root directory.	Tools disk with dc3dd will be created.	Expected Result Obtained	5.2.2
2.2	3.1.3	Boot Mac Pro using Safe boot disk and a safe consultant dongle, inspect all drives on system to check status.	All drives except the boot CD drive will be write protected, including the tools drive.	Expected Result Obtained	5.2.4, 5.2.5
2.3	3.1.4	Plugin eSata drive and USB drive, they should mount in the locked mode	Plugged in USB drive and eSata drives will mount on system in a locked mode	Expected Result Obtained	5.2.4, 5.2.5
2.4	3.1.5	All locked drives can be unlocked and written to as needed and then can be relocked.	All drives will unlock, can have a file written to them, then relocked	Expected Result Obtained	5.2.4, 5.2.6
2.5	3.1.6	Remove Enterprise USB dongle.	Nothing will happen and the session will continue as if the dongle was still there.	Expected Result Obtained	5.2.7



**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:**

<b>Tool</b>	<b>Version</b>	<b>Developer</b>
Safe Boot Disk	Version 1.2.1	ForensicSoft Inc.
SafeTools 2	Version 2	ForensicSoft Inc.

**Additional Hardware:**

<b>Device</b>	<b>Manufacturer</b>	<b>Model Number</b>	<b>Serial Number</b>
8Gig USB Thumb drive	PNY	Attache	DC3 MB03168
USB dongle	ForensicSoft	N/A	Safe Consultant
USB dongle	ForensicSoft	N/A	Safe Enterprise

**Workstation:**

Workstation 1

<b>Feature/Model</b>	<b>Mac Pro (Early 2008)(64-bit)</b>
<b>Form factor</b>	Tower
<b>Motherboard</b>	Apple Inc. Mac-F42C88C8 Proto 1
<b>Processor</b>	8 Core: Two 2.8 GHz, Quad-core Intel Xeon 5400 series processors
<b>Memory</b>	(4) 2GB (two 1GB) of 800MHz DDR2 ECC fully buffered DIMM
<b>Graphics</b>	nVidia GeForce 8800 GT (512MB) Dual-DVI (PCIe)
<b>External Devices</b>	N/A
<b>Examination Drive</b>	Mac Pro Fedora/Windows build 2 md5 hash:160bbdbcf00970d0de9ba076a05fa62d
<b>Data Storage Drive</b>	N/A

**FOR OFFICIAL USE ONLY**  
**Defense Cyber Crime Institute**

**Appendix C: Test Data Sets**

<b>Test Set ID</b>	<b>Type</b>	<b>Test Set HASH (md5, sha1)</b>
<b>D1</b> 320 GIG sata	Western digital s/n wmav2dk23245	Md5 f021af6ca20442303b497a61fe5b1a79
<b>D2</b> 320 GIG sata	Western digital s/n wmav2dm40715	Md5 54eada99a2af96495d4004660649b356
<b>D3</b> 320GIG USB pocket drive	Western digital sn wx50e69jv095	Md5 23aa4955ff7da8db5dff455636559b49