NLECTC NIJ

Criminal Justice
Electronic Crime Technology
Center of Excellence

SAFE Boot CD

Version 1.2.1.6711

EVALUATION REPORT

January 2012

NIJ Electronic Crime Technology Center of Excellence
550 Marshall St., Suite B
Phillipsburg, NJ 08865
www.ECTCoE.org

NIJ ECTCOE TESTING AND EVALUATION PROJECT STAFF

Robert J. O'Leary, CFCE; DFCP
Russell Yawn, CFCE
Chester Hosmer
Mark Davis, Ph.D.
Donald Stewart, CFCE; ACE
Randy Becker, CFCE
Jacob Fonseca
Michael Terminelli, ACE
Victor Fay-Wolfe, Ph.D.
Kristen McCooey, CCE; ACE
Laurie Ann O'Leary

Table of Contents

Introduction

The National Institute of Justice (NIJ) Electronic Crime Technology Center of Excellence (ECTCoE) has been assigned the responsibility of conducting electronic crime and digital evidence tool, technology and training testing and evaluations in support of the NIJ Research, Development, Testing and Evaluation (RDT&E) process.

The National Institute of Justice RDT&E process helps ensure that NIJ's research portfolios are aligned to best address the technology needs of the criminal justice community. The rigorous process has five phases:

- **Phase I: Determine technology needs principally in partnership with the Law Enforcement and Corrections Technology Advisory Council (LECTAC) and the appropiate Technology Working Group (TWG).** NIJ identifies criminal justice practitioners' functional requirements for new tools and technologies. (For more information on LECTAC and the TWGs, visit http://www,justnet.org.)
- **Phase II: Develop technology program plans to address those needs.** NIJ creates a multiyear research program to address the needs identified in Phase I. One of the first steps is to determine whether products that meet those needs currently exist or whether they must be developed. If a solution is already available, Phases II and III are not necessary, and NIJ moves directly to demonstration, testing and evaluation in Phase IV. If solutions do not currently exist, they are solicited through annual, competitively awarded science and technology solicitations and TWG members help review the applications.
- **Phase III: Develop solutions**. Appropriate solicitations are developed and grantees are selected through an open, competitive, peer-reviewed process. After grants are awarded, the grantee and the NIJ program manager then work collaboratively to develop the solutions.
- **Phase IV: Demonstrate, test, evaluate and adopt potential solutions into practice.** A potential solution is tested to determine how well it addresses the intended functional requirement. NIJ then works with first-adopting agencies to facilitate the introduction of the solution into practice. After adoption, the solution's impact on practice is evaluated. During the testing and evaluation process, performance standards and guides are developed (as appropriate) to ensure safety and effectiveness; not all new solutions will require the publication of new standards or guides.
- **Phase V: Build capacity and conduct outreach to ensure that the new tool or technology benefits practitioners.** NIJ publishes guides and standards and provides technology assistance to second adopters.[1]

The High Priority Criminal Justice Technology Needs are organized into five functional areas:

- Protecting the Public.
- Ensuring Officer Safety.
- Confirming the Guilty and Protecting the Innocent.
- Improving the Efficiency of Justice.
- Enabling Informed Decision-Making.

The NIJ ECTCoE tool, technology and training evaluation and testing reports support the NIJ RDT&E process, which addresses high priority needs for criminal justice technology.

[1] *National Institute of Justice High-Priority Criminal Justice Technology Needs,* March 2009 NCJ 225375.

Overview

Product Information

SAFE Boot CD is a software write-blocking solution that can be used to collect potential evidence from a computer. The following is from the product website (www.forensicsoft.com):

> "The SAFE boot disk allows for write-blocked acquisition, triage and/or analysis of any attached disks, including IDE (PATA and SATA), SCSI, USB, IEEE1394, SAS, Fiber Channel, flash media, etc. This includes any hardware RAID arrays, which can be acquired and/or analyzed in the SAFE environment as a single array rather than having to acquire individual disks and attempt to rebuild the RAID array in order to analyze it. Because Windows® device drivers are readily available for all disk controllers (i.e., SAS, SCSI, SATA, etc.), using the SAFE boot disk, you will never be unable to forensically image a RAID array due to lack of drivers, which is a common issue with forensic examiners using Linux-based boot disks.
>
> Since the SAFE boot disk is built on a Microsoft Windows® environment, you have the ability to utilize your favorite GUI forensic tools such as EnCase®, FTK® Imager, X-Ways® Forensics, etc. with zero learning curve. The SAFE boot disk will have you out performing onsite acquisition, triage and analysis immediately. The user error risks and issues that come along with utilizing Linux-based boot disks, such as typos in command line applications like "dd" or confusing /dev/sda with /dev/sdb (or similar) do not exist within the SAFE boot disk environment."

Product Description

From the product's website:

> "SAFE (System Acquisition Forensic Environment) is the first and only forensically sound Windows boot disk. SAFE is a fully licensed version of Windows PE 3.0 protected by the proven SAFE Block software write-blocking technology. You can now boot and safely acquire and/or analyze any X86-based computer using your favorite Windows computer forensic software, without the need to remove drives. This means that you can now easily and safely image every RAID, SAS, Fiber Channel and/or laptop hard drive without the need for special adapters, controller cards or any other hardware device not already present on the machine. In addition, even those drives protected by BitLocker can be accessed and analyzed."

The SAFE Boot CD is avaiable in two versions, a consultant version for $399 (USB) and an enterprise version for $1,199 (USD).

Special Features

- Windows Drivers

  The most common problem with Linux-based boot disks is that drivers for RAID and other disk controllers are often not included in and/or not available for common Live Linux boot CDs. Even when drivers are available, most non-Linux users would have difficulty installing any additional driver into their favorite Linux boot CD. The SAFE boot disk is based on the Windows 7 x 86 operating system, and Windows drivers are readily available for all Intel-based RAID and disk controllers. SAFE comes loaded with most Windows drivers and the ability to install any additional Windows drivers with a very simple process that can be done onsite at any time if needed.

■ NTFS File System Support

DOS or Linux OS boot disks do not support writing to the NTFS file system, without the use of a third-party tool or experimental drivers, resulting in most examiners writing their forensic images to the FAT32 file system. Using SAFE, you have the fully functional ability to write to NTFS and NTFS compressed file systems, taking advantage of larger partition sizes, larger file size limits and the advantage of native NTFS compression. By writing directly to NTFS, SAFE saves substantial time and effort by the examiner.

■ SAFE Write Blocking

The proven software write-blocking technology used in SAFE Block XP has been integrated into the SAFE boot disk. This means that upon booting any machine with the SAFE boot disk, every attached disk and flash device are automatically blocked without any required user interaction. Further, this is true write blocking and not simply setting up an OS to logically mount read-only or not auto-mount like some other popular Linux boot disks.

Upon booting, if the examiner wishes to image a disk, with the click of a mouse the user simply unblocks the target disk that the examiner will write to and leaves all other disks blocked. All media is protected throughout the boot process and only become unblocked when/if the examiner chooses to unblock a disk. If the examiner just wishes to preview and/or search the computer, then all media can be left blocked for the entire SAFE session.

■ Use Your Favorite Windows Forensic Tools

Many forensic examiners have had to resort to the use of Linux boot CDs for some forensic tasks, requiring them to use DD, DCFLDD, MD5SUM, SHA-1SUM and many other Linux tools they may not be comfortable with. Now with the SAFE boot CD, forensic examiners can use their favorite Windows forensic tools in the familiar Windows environment.

❑ Tools:

- FTK Imager.
- EnCase6 (EnCase dongle required for full mode; acquisition mode without EnCase dongle).
- X-Ways Forensics (X-Ways dongle required).
- WinRAR.
- WinHex (WinHex dongle or license required).
- Irfanview Image viewer.
- VLC video viewer.
- Open Office 1.5.

To add third-party tools to the SAFE boot environment, also download the free Tools Disk Creator software.

■ Perform BitLocker Operations and Acquisitions

The SAFE boot disk includes the command line tool “manage-bde.exe,” which allows for the detection and unlocking of BitLocker encrypted volumes, along with many other functions.

■ HPA and DCO Unlocking

The SAFE boot disk identifies and provides access to Host Protected Areas (HPAs) and Device Configuration Overlay (DCO) on IDE (PATA and SATA) disks of the booted computer. HPA and/or DCO can be temporarily removed by the investigator to provide access to the full disk for tasks such as acquisition or searching.

■ Case Logging

SAFE has built-in logging that creates a forensic examiner’s log file of all system attributes and various steps performed.

■ Built-In Tools

SAFE’s Windows environment has built-in tools for exploration, viewing and simple forensics functions.

Evaluation and Testing of SAFE Boot CD

Test Bed Configuration

To prepare for testing and evaluation of the SAFE Boot CD, a test bed was designed and configured to simulate realistic conditions. Knowledge of what "evidence" exists on the test bed enables easy evaluation of the SAFE Boot CD. The test bed is located in the computer lab at the Electronic Crime Technology Center of Excellence, 550 Marshall St., Suite B, Phillipsburg, NJ 08865. The following is a list of the systems used for testing and their configuration details:

- Computer
  - Gateway Mid Tower PC (Gateway Test PC):
    - Model Number: MFATXSL KTA 300SE.
    - Serial Number: 0026280320.
    - MFG DATE: 2/15/2002.
    - Intel 400075P motherboard.
    - Intel Celeron 1200 MHz, 1.2 GHz.
    - 512 MB Ram installed.
    - DVD/CD Reader.
    - 3.5-Inch Floppy Drive.
- Hard Drive
  - Western Digital WD200 20GB Hard Drive:
    - Model Number: WD200BB-75CAA0.
    - Serial Number: WMA8J1826063.
    - DCM: HSEHNA2AB.
    - MFG Date: 6 MAR 2002.
    - Wiped with SPADA disk wiping utility.
- Operating system: Microsoft XP Home Edition

  The operating system, Microsoft XP Home Edition Version 2002 (55277-OEM-0011903-00105), was installed from the OEM CD-ROM supplied by Gateway. A standard installation was performed, the time zone set for eastern U.S. and Canada, and service pack 3 and all pending updates were installed.
- User accounts and computer name configuration
  - The Gateway Test PC was named "Test Computer 1" with the owner set to "ECTCoE." The following users were configured on the computer:

LABXPGTWY1	Administrator account	password = ectcoe
Alice	Limited User account	password = testpass
Bill	Limited User account	no password
Charlie	Limited User account	no password

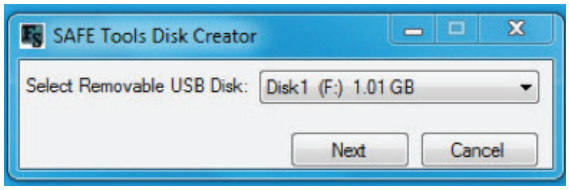
- Configuring SAFE Tools Disk Creator

  Prior to using the SAFE Boot CD, the investigator should perform certain preparations. A program that can be downloaded with the SAFE Boot CD is the "Tools Disk Creator."

  The "Tools Disk Creator" is a tool used to configure a device such as a USB flash drive or an External USB hard drive to be a "Tools Volume."

  Using the "Tools Disk Creator" is straightforward. After being downloaded from Forensic Soft, the tool is installed on a computer. The USB device is inserted into the USB port on the computer (this has to be done prior to running the program or you will

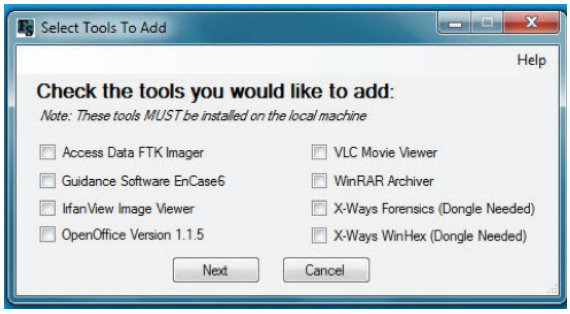
get a screen telling you there are no USB devices to prepare). The “SAFE Tools Creator” program is run. A window is opened up on the desktop providing a choice of which USB device you want to prepare:



After choosing which USB device to prepare, ‘Next’ is clicked on and a new window with the choices for which tools to install is presented. Note the sentence under Check the tools you would like to add:

Note: These tools MUST be installed on the local machine.

The window menu also indicates which forensic tools you may need to use a dongle with.



After checking the boxes for the tools to be installed for use with the SAFE Boot CD, the SAFE Tools Disk Creator software installs the necessary files on your USB device to run the programs you use.

Test: Forensic Soundness

The SAFE Boot Disk v1.2.1.6711 is advertised as a forensically safe way to view the contents of a hard drive without the need for removing it from a suspect’s computer. It should be understood by the user of this boot disk that the suspect computer must be configured to boot from the CD-ROM in order to ensure forensic soundness.

When booting to the SAFE CD, all drives on the computer are locked by default. This test will demonstrate the integrity of the locked drives. Each drive will be navigated to and files will be opened.

The Gateway Test PC will be booted from the SAFE Boot CD. The hard drive installed in the Gateway Test PC is a Western Digital WD200BB-75DEA0, 20 GB hard drive, S/N WMAD21288126. The original hard drive was cloned to this drive to make an ECTCoE test drive. Both drives were hashed to verify they were identical.

The MD5 hash of the original ECTCoE test drive and the Western Digital test drive is 4A5A614AD-2FE6F32D6E8A490BFf6ADBD as calculated by SPADA (System Preview and Data Acquisition).

After navigating though the test hard drive using the SAFE explorer and other tools, the computer will be turned off using the SAFE programs shutdown button. The ECTCoE test hard drive will then be removed and the MD5 hash will be calculated with the Checksum calculator in SPADA. This will be performed to test if the MD5 hash value changes from the known MD5 hash value on the test hard drive.

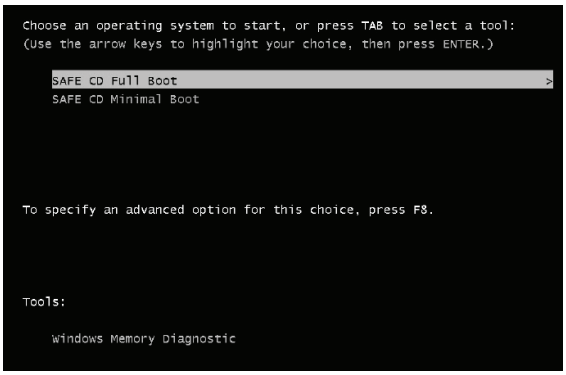
To perform this test, the following actions were performed:

1. Before any system configuration or testing was performed, the BIOS for the Gateway test computer was checked by pressing F1 at power on and verifying the boot sequence. It was verified that the computer would boot from the CD-ROM drive first if a boot CD was in the drive.

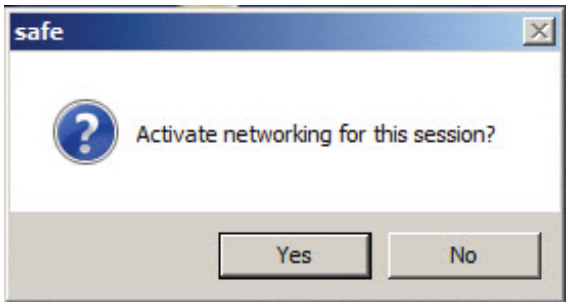
2. The ECTCoE test drive was installed in the Gateway test computer.

3. The Gateway test computer was powered on and the SAFE boot CD was inserted into the CD-ROM drive.

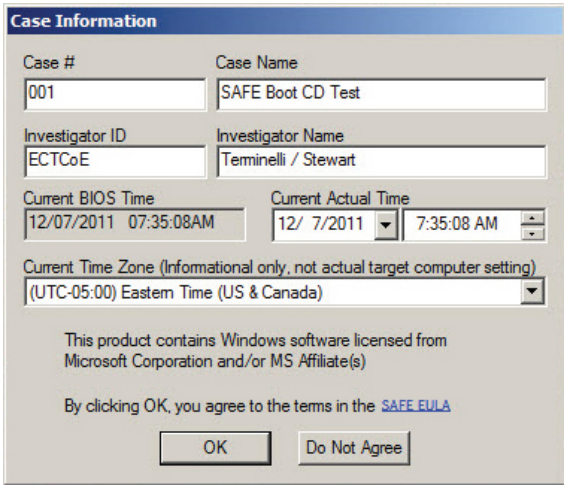
   The first screen that appears is the Windows Boot Manager, which gives you the choice of Safe CD Full Boot or SAFE CD Minimal Boot. For this test Full Boot was chosen.



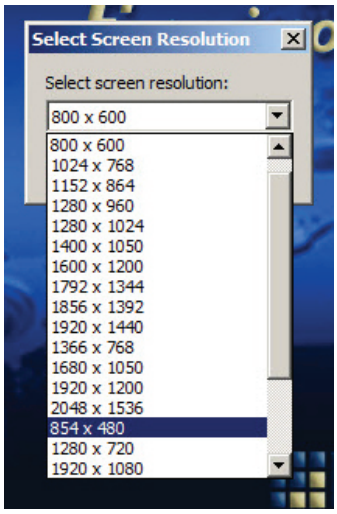
4. The computer then booted the SAFE environment and asked the user if he wanted to activate networking.



5. The next screen asked for case information including Case#, Case Name, Investigator ID and the Investigator Name. Those items were entered as shown in the screenshot. The program inserts the Current BIOS Time and asks for the Current Actual Time. If there is a time difference between the BIOS reported time and current time and date, the investigator can modify the Current Actual Time field.

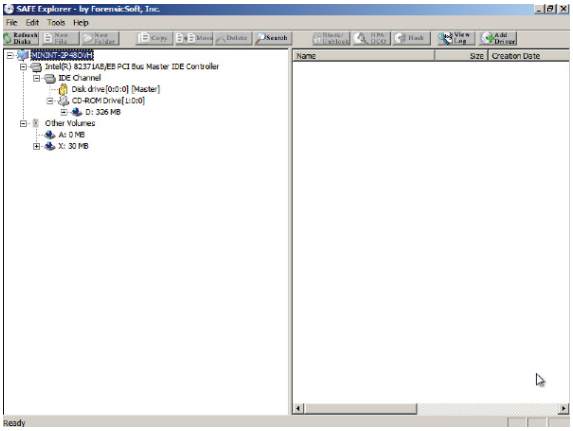


6. The following window allows the user to set or change the screen resolution of the computer that is booted with the SAFE Boot CD. This setting will be dependent on the hardware capabilities, particularly the video card, of the computer that is running the SAFE Boot CD.



7. The SAFE Boot CD then identifies all of the hardware on the computer and the Main Menu options are shown.

8. SAFE explorer was selected and the program below was displayed. This program can be used to explore the hard disk of the computer.



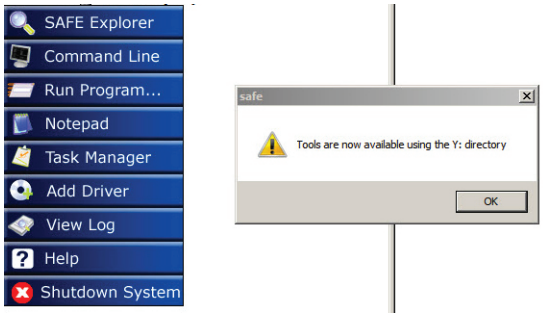
The menu bar has four choices: File, Edit, Tools and Help. Under the Tools menu, the user can select Refresh Disks, Write Block, HPA/DCO, HASH, View Log, Add Driver and Set Resolution. Each menu item has a corresponding CTRL + letter key sequence for a shortcut.

Under the menu bar several buttons appear. These buttons are either highlighted or grayed out depending on the current navigation state of SAFE Explorer. The grayed out buttons (New File, New Folder, Copy, Move and Delete), are only enabled when a disk is highlighted that is not write-protected. Most often this will be a drive that will be used to export data or where other tools will be loaded. The buttons that are not grayed out and enabled (Refresh Disks, Search, Block/Unblock, HPA/DCO, Hash, View Log and Add Driver) are functional on the write-protected disk(s). These enabled buttons correspond to the Tools Menu options.

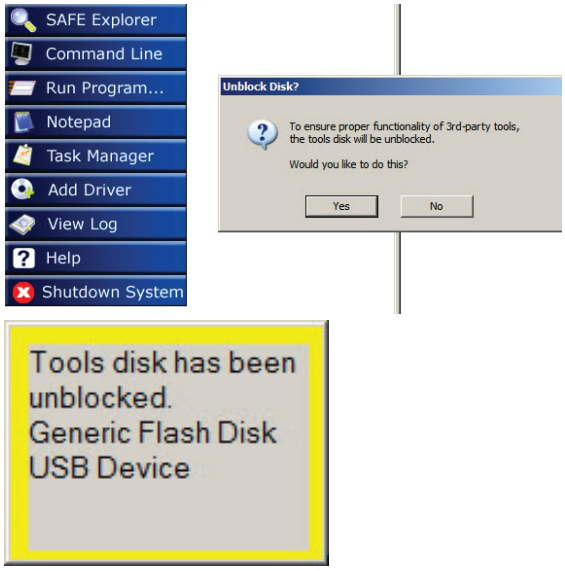
The SAFE Boot CD identifies and provides access to Host Protected Areas (HPAs) and Device Configuration Overlay (DCO) on IDE (PATA and SATA) disks of the booted computer. HPA and/or DCO can be temporarily removed by the investigator to provide access to the full disk for tasks such as acquisition or searching.

9. After the initial boot and running SAFE Explorer, the investigator can choose to use other tools that were configured previously with the SAFE Tools Disk Creator. For this test a USB flash drive was used that was preconfigured with FTK Imager, InfranView, EnaCase6, OpenOffice.org1.1.5 and VLC video player from Video Lan.

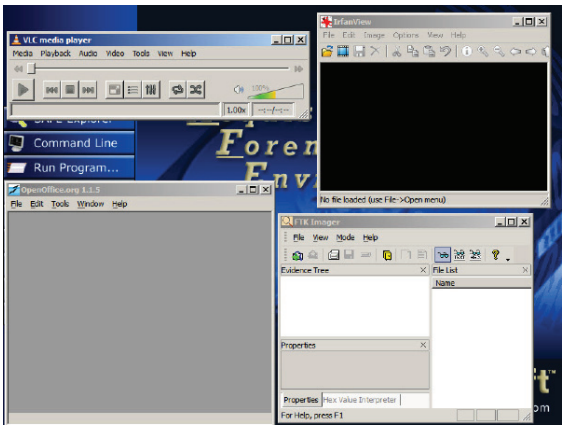
When the Tools Volume is plugged into the USB port a series of windows appears advising the investigator that the tools are available and the Tool Volume assigned drive letter.



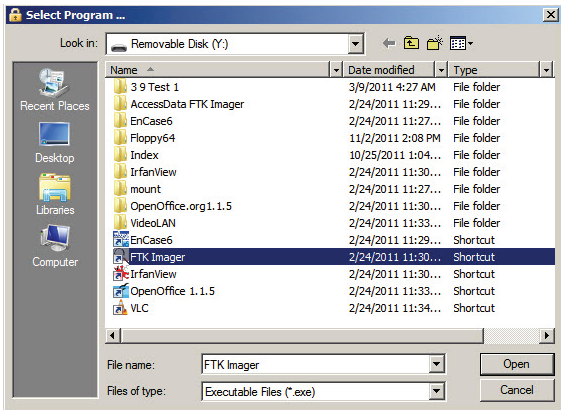
When OK is clicked another window appears advising to unblock the Tools Volume to allow for the third-party tools to run properly. After clicking Yes, a window opens up in the lower right-hand part of the screen advising that the “Tools Disk has been unblocked.” It then lists the USB Drive in the test case as a “Generic Flash Disk USB Device.”



Using the "Run Program" selection on the Main Menu screen displays the Tools Volume with shortcuts for the programs that were previously installed. In the image below, InfranView, FTK Imager, VLC Media Player and Open Office are running and can be used to view files. FTK imager can be used to image the hard drive if needed.



In addition, from within SAFE Explorer, a file can be opened with the third-party tools by right-clicking a file and selecting the tool from the menu. SAFE has a built-in viewer for graphic files; however, files such as .doc and video files will need to be opened with the third-party tools.



Several files were opened and closed from the user folders "C:\Documents and Settings\Alice\" and "C:\Documents and Settings\Bill\" in an attempt to change the last accessed date and times on the files. Attempts were also made to move, delete, edit and copy files to the write-protected drive. All attempts failed. Messages advised that the files could not be saved to the attempted locations.

The following is a list of files that were accessed on the ECTCoE test hard drive from SAFE explorer, including what programs were used to open and to try to change the files.

- C:\Documents and Settings\Alice\My Documents\:
  - Personal.doc (Open Office.org 1.1).
  - Trojan Downloader.doc (Open Office.org 1.1).
- C:\Documents and Settings\Alice\My Documents\My Pictures\:
  - DSC00674.jpg (InfranView v4.28).
  - DSC00676.jpg (Built in viewer - Berksoft HMview 4.04).
- C:\Documents and Settings\Bill\My Documents\:
  - Credit Card and SS numbers.txt (Open Office. org 1.1, Notepad).
  - DECTLIMA1[1].pdf (Open Office.org 1.1 - failed to open).
  - Bone.doc (Open Office.org 1.1).

- C:\Documents and Settings\Bill\My Documents\My Pictures\:
  - Ace_Club.jpg (InfranView v4.28).
  - Frankfurt 114.jpg (Berksoft HMview 4.04).
  - Frankfurt 115.jpg (Berksoft HMview 4.04).

10. The drive was hashed to determine if any files had changed. With SAFE Explorer the write-protected drive (Disk Drive (0:0:0) [master]) was highlighted and the HASH button was selected.

11. A window opens up for the user to choose MD5 or SHA-1 Hash. MD5 was selected.

12. After the hash process was completed for the entire drive, a window opened on the screen with the resulting MD5 hash value and the message, "A copy of the following hash value has been saved in the log." The value returned was not visible.

13. Shutting down the SAFE Boot CD program resulted in the following windows opening. The first window asks for a drive to save the log to that must be unblocked. Another window pops up asking where to save the log to. The log was saved to the Y:\ drive, which was earlier identified as the Tools volume. Another window opens and the user is instructed to remove the SAFE Boot CD and any other removable media. When the user clicks on OK, the computer shuts down.

14. After the shutdown was complete, the ECTCoE test drive was removed and attached to a Tableau TD1 Forensic Duplicator that has the capability of performing a hash on a write-protected drive. The result was the following hash, 4A5A614AD-2FE6F32D6E8A490B4F6ADBD, which matched the hash calculations performed before testing. The logs from the Tableau TD1 Forensic Duplicator were saved.

15. The SAFE Log that was saved to the Tools volume in a folder named Safe Log consisted of six files: Report.cass, report.js, report.xslt, SafeLog.html, SafeLog.xml and SafeLogMD5.txt. It should be noted that the file SafeLogMD5.txt is the MD5 hash value of the log xml file.

    When SafeLog.xml is opened the entire log is displayed. The Case ID, Investigator Name, BIOS, Actual Time, Time Zone, and the drive's make and model number are contained in the report. Actions performed are then displayed in chronological order.

Test Results

Within the event log the value under "HASH" on \\.\PhysicalDrive0\ showed the type of hash as MD5 but the value was blank. Using the Tableau TD1 Forensic Duplicator to perform a hash on the ECTCoE test drive before and after accessing files using the SAFE Boot CD verified that no file or drive contents were changed during the course of this testing. In this test, the SAFE Boot CD performed as expected.

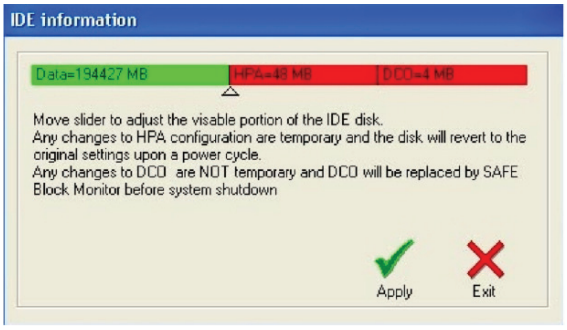
Test: HPA/DCO Function

In order to test the HPA/DCO read function of the SAFE Boot CD, the following steps were taken:

1. A drive had to be prepared with an HPA, or Host Protected Area. Using the freeware tool MHDD, which allows a user to work with hard drives at the lowest possible level, an HPA was created on a 20 GB hard drive. A hash of this hard drive was taken with the Tableau TD1 Forensic Duplicator with the result of: 676CFD10D800880ED96B8D57F828026C.

2. This test hard drive was connected to the Gateway test computer. The Gateway test computer was then booted with the SAFE Boot CD. Once the SAFE Boot CD loaded, the SAFE Explorer was started. SAFE explorer opened and identified the disks connected to the computer and indicated that an HPA was found on the test hard drive.

3. The menu bar button was also highlighted indicating the HPA was found. When the button is clicked, a window opens up and shows the data area of the hard drive in bright green. The HPA is in red, as in the screenshot below.



4. The slider was moved so the HPA area of the hard drive no longer was hidden. This allowed the entire hard drive to be viewed. After the test was finished, the HPA was returned back to its original size and the apply button was clicked.

Test Results

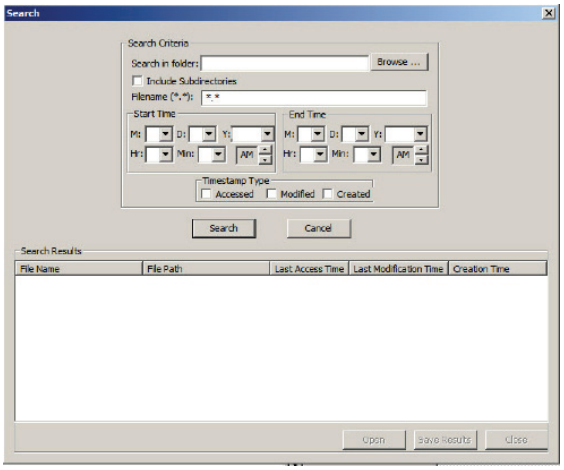
After this test a hash was calculated using the Tableau TD1 Forensic Duplicator resulting in 676CFD-10D800880ED96B8D57F828026C, which matches the result before the SAFE Boot CD was used to view the HPA on the drive. In this test, the SAFE Boot CD performed as expected.

Test: Search Functionality

In order to test the search functionally of the SAFE Boot CD the following steps were performed:

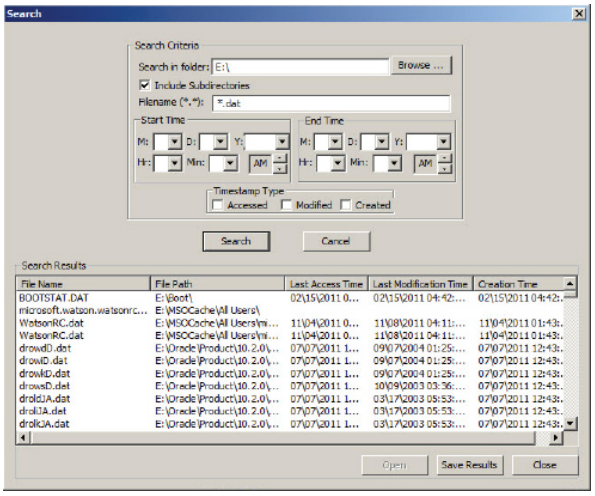
1. SAFE Explorer has a “Search” button. When clicked a window is opened presenting the user with a robust search tool as seen in the screenshot below.

   Choices include what folder to search, subdirectories or folders, filename, start date and time, ending date and time and timestamp type (Last accessed, modified and date created).



2. The entire drive was selected, including subdirectories or folders with the filename of “.dat” or “*.dat” files.

3. When the search completed, SAFE Explorer displayed all the found .dat files in alphabetical order. There is also an option to save the results into a text file.



Test Results

In this test the search functionality performed as expected, returning all of the “.dat” files expected on the hard drive.

Test: Bitlocker Encrypted Hard Drive

Incorporated in the SAFE Boot CD are the Microsoft windows commands to open a BitLocker encrypted hard drive. Under normal circumstances the contents of a BitLocker encrypted hard drive will not be visible to the SAFE Explorer program. FTK Imager used from the Tools volume created in previous tests can be used to examine the header of the hard drive. In this test it was determined that the header of the hard drive was FVE-FS (ASCII) or 2d 46 56 45 2d 46 53 2d (Hexidecimal). In order for SAFE Boot CD to view the contents of the encrypted volume, either the password will need to be known or the USB drive containing the unlock key will need to be available.

A Lenovo ThinkPad Edge laptop computer was used to perform this test. The laptop is configured with a 500 GB hard drive, 8 GB of RAM and an Intel i5 2.66 GHz CPU. Additional configuration was performed on this laptop using the following steps:

1. The laptop was upgraded to Windows 7 Ultimate 64 Bit from Windows 7 Professional 64 bit to enable the BitLocker functionality. The hard drive is divided into several partitions: a system partition (which is made by Win7 when it is installed), OS partition, recovery partition and a partition slightly larger than the OS partition used to store files.

2. The hard drive in the Lenovo laptop was backed up with Lsoft Technologies Active Disk Image v5.1.3 64 bit to an external USB hard drive. An Active Disk Image boot CD-ROM was made so the laptop could be booted without the operating system in case of hard drive failure or corruption. The 500 GB hard drive was removed from the laptop and a 320 GB Seagate Momentus 7200.4, serial number 5VH1GTWY, was installed in its place.

3. The Active Disk Image boot CD-ROM was used to boot the laptop. The Active Disk Image program starts automatically and Restore Image to Disk was selected. The MBR, System partition and the OS partition were restored to the 320 GB hard drive installed in the laptop. When it was complete, the CD-ROM and USB hard drive were removed and the laptop was started.

Since this particular laptop was not equipped with a TPM (Trusted Platform Module) chip, BitLocker was configured to work with a USB drive using the following steps:

1. Click on the Windows Start button and use the search window to search for gpedit.msc. Once found, gpedit.msc was selected.

2. In the left pane, “Computer Configuation,” “Administrative Templates,” “Windows Components,” “BitLocker Drive Encryption” and “Operating System Drives” were expanded.

3. In the right pane, require additional authentication at startup and click on edit were right-clicked.

4. The “Enable” radio button was selected, and under the options section, “Allow BitLocker without a compatible TPM box” was checked. OK was then selected. To apply the change, the computer could either be restarted or the command “gpedit /force” from a command line could be utulized.

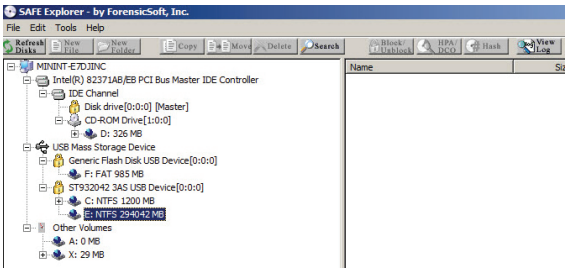
5. The control panel was opened and BitLocker enabled. BitLocker can also be enabled by going into Computer and right clicking on the drive.

6. BitLocker was enabled on the “C:\” (OS drive), the USB device was chosen to save the file and BitLocker encrypted the drive. To verify that the drive was encrypted, the computer was restarted without the USB flash drive and after the BIOS loaded, a message was received that the drive was encrypted with BitLocker and the USB device where the key was located would have to be inserted. Once this was done, the laptop started normally. The laptop was powered off.

To test the functionality of the SAFE Boot CD on a BitLocker encrypted drive, the following steps were performed:

1. The SAFE Boot CD was placed in the CD-ROM drive and the laptop was powered on. Since the laptop was configured to start from the CD-ROM, first it booted into the SAFE Boot CD. Once the boot was complete, the SAFE Explorer was opened. Under Disk drive 0 two partitions were identified. One was a “C:\NTFS” partition of 1200 MB in size and the other was an E:\NTFS partition of 294042 MB in size.

2. The “C:\NTFS” was highlighted and the files contained on that partition could be viewed in the right panel. The “E:\NTFS” partition was highlighted and nothing appeared in the right panel, as shown in the screenshot below.

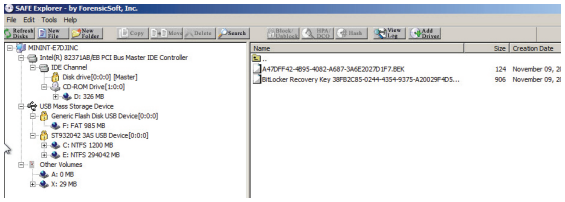


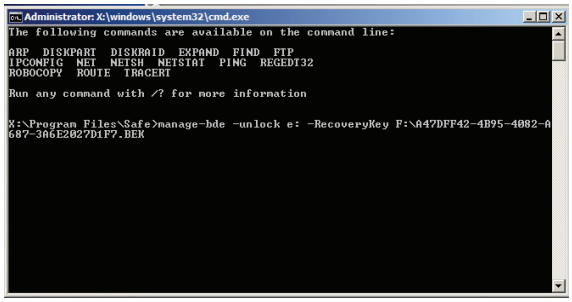
3. Opened the command prompt.

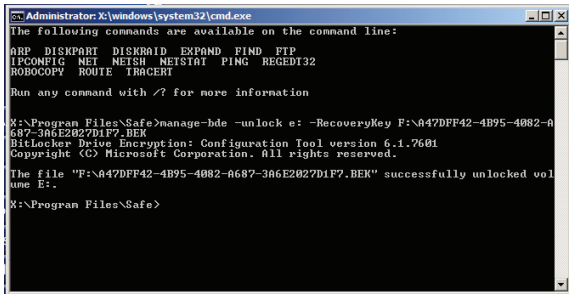
4. Typed “manage-bde –unlock e: -password” without the quotes. A password prompt appeared. With the proper password the drive can be unlocked.

5. Since the test was performed using a recovery key the –RecoveryKey switch was used. It should be noted that when the recovery key was copied to the USB flash drive with the BitLocker configuration tool, the USB flash drive contained no other files. There was one file visible on the USB flash drive. It was “BitLocker Recovery Key 38FB2C85-0244-4354-9375-A20029F4D523.TXT.” Upon opening the organize tab of the SAFE explorer tool and unchecking “Hide Protected Operating System Files,” there was another file found, “A47DFF42-4B95-4082-A687-3A6E2027D1F7.BEK.” This file is then visible when using the SAFE Explorer when the USB flash drive is inserted.

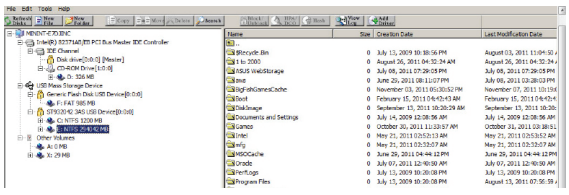
6. From the command prompt, the command “manage-bde –unlock e: -RecoveryKey F:\ A47DFF42-4B95-4082-A687-3A6E2027D1F7.BEK” was entered. Once executed, the drive was unlocked. As a note, when using the -RecoveryKey switch, the drive letter where the key is located has to be included in the path to the BEK file, in this case “F:\.”







7. The contents of Drive E:\NTFS, which is the BitLocker encrypted OS drive, can now be viewed.



Test Results

In this test, the BitLocker functionally of the SAFE Boot CD performed as expected. It should be noted that without the password or the USB device containing the encryption key, this will not work.

Conclusion

In all tests the SAFE Boot CD performed as expected. The SAFE Boot CD can serve as a valuable tool to gather information from computers in a forensically sound manner. No data was altered during any of the testing. HPA/DCO and Bitlocker drives could be viewed with the SAFE Boot CD. The only problem encountered during the testing was that the internal hashing function did not display the hash value of the drive. Also, the BitLocker functionally will only work if the password is known or the USB key containing the key is available.