CyberScience Laboratory Functional Analysis of

Shadow™

September 2004

Prepared By:
CyberScience Laboratory
Rome, New York 13441-4114
315.838.7000
www.cybersciencelab.com

DISCLAIMER

This report was prepared for the United States Government by the CyberScience Laboratory (CSL).

With respect to information provided in this document, neither the United States Government, nor any of its employees, nor the CSL, nor any of its employees makes any warranty, expressed or implied, including, but not limited to, the warranties of merchantability and fitness for a particular purpose. Further, neither the United States Government, nor any of its employees, nor the CSL, nor any of its employees, assumes any legal liability for the accuracy, completeness, or usefulness of any information, apparatus, product, or process disclosed.

Reference herein to any specific commercial products, processes, or services by trade name, trademark, manufacturer, or otherwise does not necessarily constitute or imply its endorsement, recommendation, or favoring by the United States Government or the CSL. The information and statements contained in this document shall not be used for the purpose of advertising, or to imply the endorsement or recommendation of the United States Government of the CSL.

Acknowledgment:
This study was sponsored by the National Institute of Justice. The National Institute of Justice is a component of the Office of Justice Programs. Points of view or opinions contained within this document are those of the authors and do not necessarily represent the official position of the U.S. Department of Justice.

TABLE OF CONTENTS

TABLES

FIGURES

1 OVERVIEW

The Shadow is a hardware device designed to aid in the investigation of a computer hard drive. It provides the investigator with read/write access to a suspect computer, while ensuring that the integrity of the suspect drive is preserved. With the help of the Shadow, the investigator has the ability to use the system being examined exactly as the suspect would, without the worry of destroying valuable evidence.

The Shadow allows the investigator to boot to the suspect drive and install software to aid in the investigation. It is compatible with any operating system, and can be used with any ATAPI 4,5 or 6 IDE device.

The device functions by redirecting all write commands from the suspect system to the ShadowDrive at the physical interface level. At any time, the investigator may “zero” the Shadow, thus erasing all of the writes made to the ShadowDrive.

The Shadow was developed by VOOM Technologies, Inc. The manufacturer’s suggested retail price is $1295. More information about the product is available at http://www.voomtech.com/voom_products/smart_storage_solutions/Shadow.html

Figure 1-1 is a front view of the Shadow device.

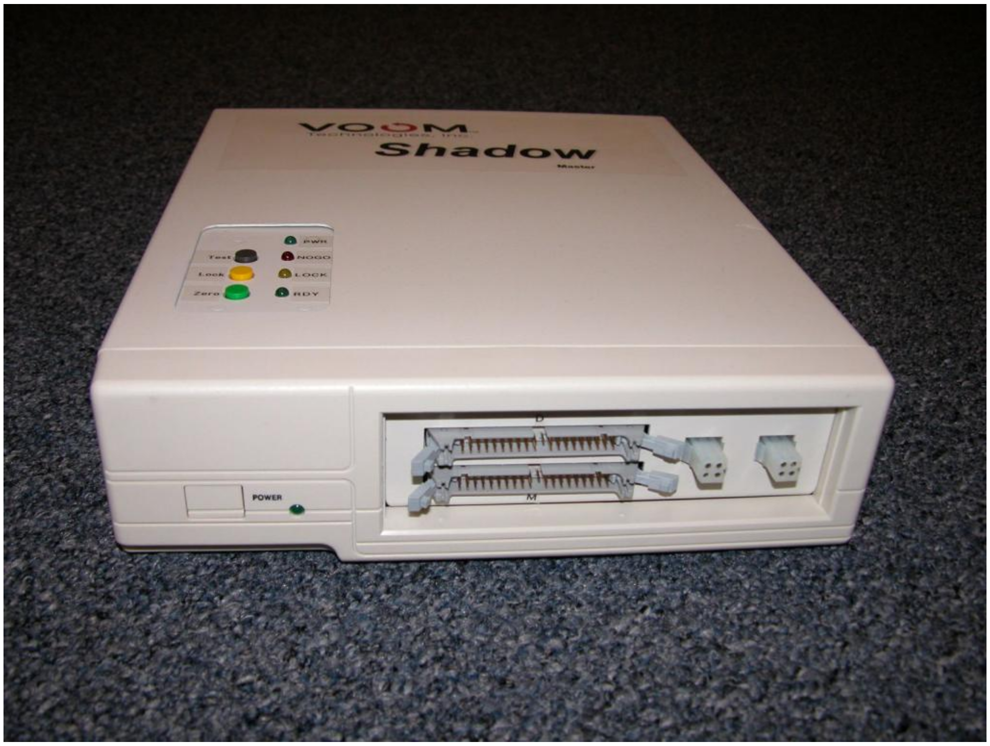

Figure 1-1

2 METHODOLOGY

2.1 Operating Systems Tested

- Microsoft Windows XP Professional Edition (base installation)
- Microsoft Windows XP Home Edition Service Pack One
- Microsoft Windows 98SE (base installation)
- Fedora Core 2.0 (base installation)

2.2 Functional Analysis

- Shadow's ability to block all writes to the suspect drive.
- Shadow's ability to provide complete read/write access to the suspect drive.

2.3 Hardware Used

- Shadow Master Device
- Gateway E4200
  - 700MHz Pentium III Processor, 128 MB of RAM,
    Quantum Fireball Ict10- 20GB Hard Drive
- Dell Dimension 2350
  - 1.8 GHz Pentium IV Processor, 256 MB of RAM,
    Maxtor 6EO40LO- 40 GB Hard Drive

2.4 Software Used

- WinHex Version 11.0
- Partition Magic Version 8.0
- Microsoft Office XP Professional (base installation)
- DriveSpy Version 1.62
- RndFile Random File Generator Version 1.1
- SHED Hex Editor Version 1.1
- Offline NT Password and Registry Editor Bootdisk Version BD040818
- ERD Commander 2002

2.5 Using the Shadow

The Shadow is available in two different models, Shadow Master and Shadow Slave. The Shadow Master is designed to be used on a suspect drive configured as "Master." If the suspect hard drive is jumpered as "Slave," then a Shadow Slave must be used. For this evaluation, only a Shadow Master was used.

To connect the Shadow to a suspect's machine, the device must bypass the connection between the suspect's motherboard and hard drive. Before a connection is made, the computer under investigation must be disconnected from its power source. The IDE cable connecting the hard drive and motherboard must be removed along with the DC power connector running from the power supply to the hard drive. The Shadow is shipped with two IDE cables. One of these cables has one blue end and one black end (Cable A), while the other has two black ends (Cable B). First, the blue end of Cable A is to be connected to the suspect's motherboard or IDE controller, while the black end connects to the Shadow connector labeled "M." Cable B is then used to connect the suspect hard drive to the Shadow connector labeled "D." Figure 2-1 depicts the supplied cables.

The Shadow must then be connected to provide the suspect drive with DC power. Cable C is used to connect the power connector on the front of the Shadow device to the power connector on the back of the suspect hard drive. Once this connection has been made, the Shadow may be plugged into an AC power outlet with Cable D. The Device is then powered up. If the device is ready, two green lights will be illuminated. If the device has been connected to a new machine, it should "zero," or erase all previous writes. If the Shadow is reconnecting to the same computer, then the user must push the "zero" button three times in order to reset the Shadow device. Once the Shadow is ready, the suspect machine may be powered up just as it was in its original state. Figure 2-2 depicts the proper configuration.

2.6 Summary of Testing Procedures

In order to determine if the Shadow device provides write-block protection to the suspect drive, the DriveSpy program was utilized to generate a series of five MD5 hashes[1]. The first hash was taken prior to the connection of the Shadow. The Shadow was then connected to the system and a second hash was taken. The third hash was taken after various commands were executed in an attempt to write to the drive being protected. The Shadow device was then "zeroed" and a fourth hash was taken of the drive. Finally, the Shadow device was disconnected from the system, and a fifth hash was generated.

In order to determine if the Shadow device provides an investigator with read/write access to the suspect drive, a series of commands were executed. These commands were executed on each system to determine if the presence of the Shadow would alter or inhibit the

[1] A hash is a string of characters generated from a given data set such as a hard drive. If the data set is changed in any way, then it will generate a different hash value.

functionality of the suspect system in any way[2]. The commands used varied for each operating system utilized and are identified in Tables 3-1 through 3-4.

Figure 2-1 is a view of the cables utilized by the Shadow

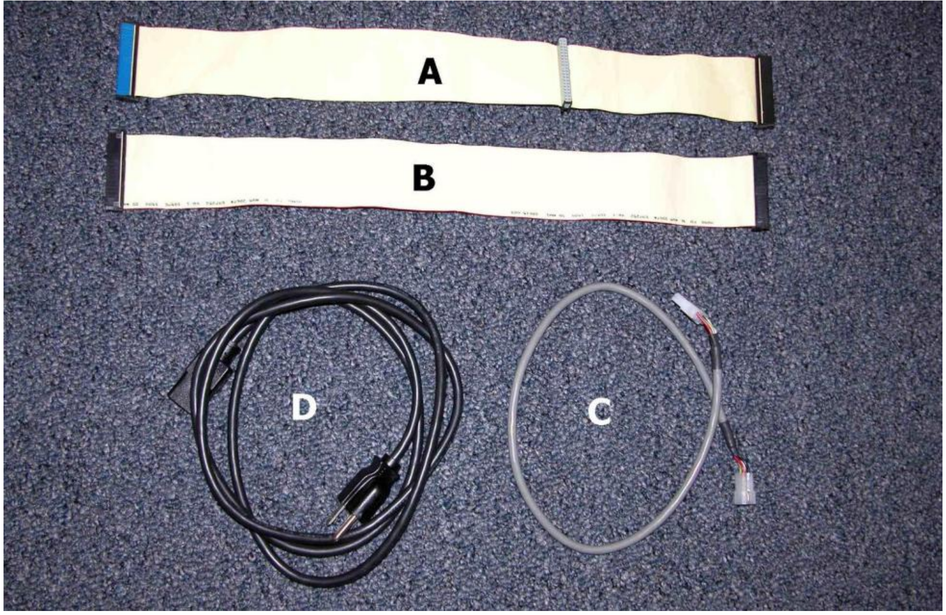

Figure 2-1

Figure 2-2 depicts the proper connection method for the Shadow

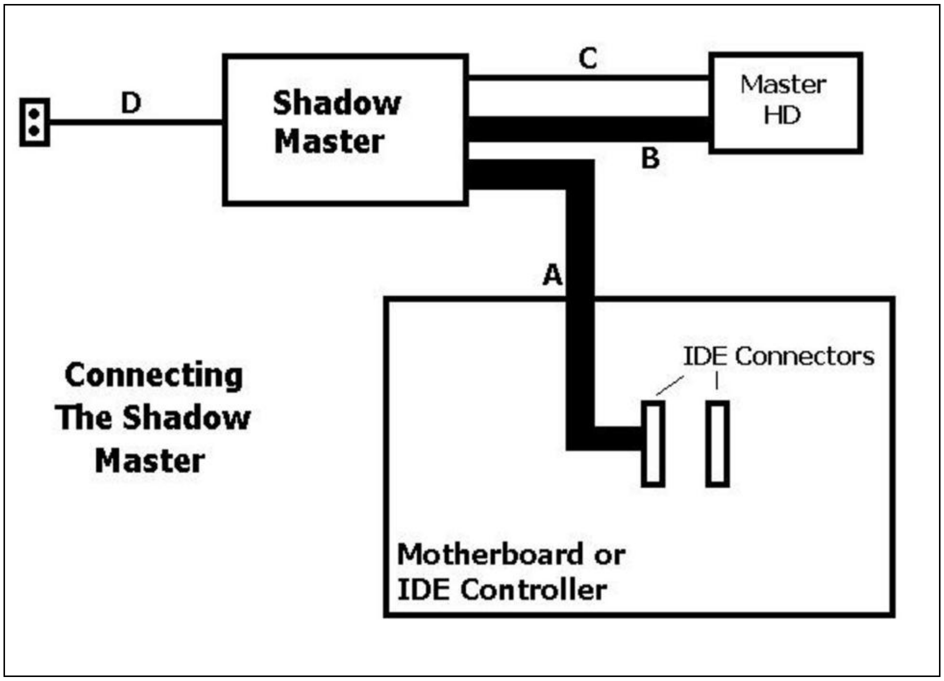

Figure 2-2

[2] For a detailed description of the executed commands, see Appendices I and II.

3 TESTING RESULTS

3.1 Examining a System Running Windows XP Professional

This test was conducted to determine if the Shadow would prevent write requests to a hard drive with the Windows XP Professional operating system, while allowing the investigator to examine the drive with full read/write access.

Action Taken	Functioned Correctly
Create Files & Directories	Yes
Copy Files & Directories	Yes
Rename Files & Directories	Yes
Move Files & Directories	Yes
Delete Files & Directories	Yes
Change Attributes of Files and Directories	Yes
Create Partition Using Disk Manager	Yes
Delete Partition Using Disk Manager	Yes
Install Software	Yes
Remove Software	Yes
Add Users	Yes
Remove Users	Yes
Change Administrator Password	Yes
Change Admin Password Using ERD Commander	Yes
Change Admin Password Using Offline NT Password Editor	Yes
Update Windows Operating System	Yes
Clear Internet Cache (History, Cookies, Temp Files)	Yes
Empty Windows Recycle Bin	Yes
Reboot Operating System	Yes
Run Disk Defragmenter	Yes
Edit a Document Using Microsoft Word	Yes
Edit a Document Using Microsoft Notepad	Yes
Edit a Document Using a Hex Editor (WinHex)	Yes
Create a Partition Using Partition Magic	Yes
Delete a Partition Using Partition Magic	Yes
Converting a Partition Using Partition Magic	Yes
Resizing a Partition Using Partition Magic	Yes

Table 3-1

Results

The initial hash of the suspect drive was **116706422353ebc5845c9627354bac16**. An identical hash was generated after the Shadow was connected, after it was zeroed, and again after it had been disconnected. This indicates that the integrity of the drive was preserved throughout.

All commands executed generated the expected results. The Shadow did not inhibit the operation of the suspect system in any way.

3.2 Examining a System Running Windows XP Home

This test was conducted to determine if the Shadow would prevent write requests to a hard drive with the Windows XP Home operating system, while allowing the investigator to examine the drive with full read/write access.

Action Taken	Functioned Correctly
Create Files & Directories	Yes
Copy Files & Directories	Yes
Rename Files & Directories	Yes
Move Files & Directories	Yes
Delete Files & Directories	Yes
Change Attributes of Files and Directories	Yes
Create Partition Using Disk Manager	Yes
Delete Partition Using Disk Manager	Yes
Install Software	Yes
Remove Software	Yes
Add Users	Yes
Remove Users	Yes
Change Administrator Password	Yes
Change Admin Password Using ERD Commander	Yes
Change Admin Password Using NT Password Editor	Yes
Update Windows Operating System	Yes
Clear Internet Cache (History, Cookies, Temp Files)	Yes
Empty Windows Recycle Bin	Yes
Reboot Operating System	Yes
Run Disk Defragmenter	Yes
Edit a Document Using Microsoft Word	Yes
Edit a Document Using Microsoft Notepad	Yes
Edit a Document Using a Hex Editor (WinHex)	Yes
Create a Partition Using Partition Magic	Yes
Delete a Partition Using Partition Magic	Yes
Converting a Partition Using Partition Magic	Yes
Resizing a Partition Using Partition Magic	Yes

Table 3-2

Results

The initial hash of the suspect drive was **8a2e0c9220eb57887a9f79762d63603e**. An identical hash was generated after the Shadow was connected, after it was zeroed, and again after it had been disconnected. This indicates that the integrity of the drive was preserved throughout.

All commands executed generated the expected results. The Shadow did not inhibit the operation of the suspect system in any way.

3.3 Examining a System Running Windows 98SE

This test was conducted to determine if the Shadow would prevent write requests to a hard drive with the Windows 98SE operating system, while allowing the investigator to examine the drive with full read/write access.

Action Taken	Functioned Correctly
Create Files & Directories	Yes
Copy Files & Directories	Yes
Rename Files & Directories	Yes
Move Files & Directories	Yes
Delete Files & Directories	Yes
Change Attributes of Files and Directories	Yes
Install Software	Yes
Remove Software	Yes
Add Users	Yes
Remove Users	Yes
Change Windows Password	Yes
Update Windows Operating System	Yes
Clear Internet Cache (History, Cookies, Temp Files)	Yes
Empty Windows Recycle Bin	Yes
Reboot Operating System	Yes
Run Disk Defragmenter	Yes
Edit a Document Using Microsoft Word	Yes
Edit a Document Using Microsoft Notepad	Yes
Edit a Document Using a Hex Editor (WinHex)	Yes
Create a Partition Using Partition Magic	Yes
Delete a Partition Using Partition Magic	Yes
Resizing a Partition Using Partition Magic	Yes

Table 3-3

<u>Results</u>

The initial hash of the suspect drive was **19493c7b6f92bac057ca801e142767c1**. An identical hash was generated after the Shadow was connected, after it was zeroed, and again after it had been disconnected. This indicates that the integrity of the drive was preserved throughout.

All commands executed generated the expected results. The Shadow did not inhibit the operation of the suspect system in any way.

3.4 Examining a System Running Fedora Core 2

This test was conducted to determine if the Shadow would prevent write requests to a hard drive with the Fedora Core 2 operating system, while allowing the investigator to examine the drive with full read/write access.

Action Taken	Functioned Correctly
Create Files & Directories	Yes
Copy Files & Directories	Yes
Rename Files & Directories	Yes
Move Files & Directories	Yes
Delete Files & Directories	Yes
Change Attributes of Files and Directories	Yes
Mount File System	Yes
Unmount File System	Yes
Install Software Package	Yes
Remove Software Package	Yes
Add Users	Yes
Remove Users	Yes
Change Root Password	Yes
Clear Internet Cache (History, Cookies, Temp Files)	Yes
Empty Trash	Yes
Reboot Operating System	Yes
Edit a Document Using Open Office	Yes
Edit a Document Using Emacs	Yes
Edit a Document Using a Hex Editor (SHED)	Yes
Create a Partition Using FDisk	Yes
Delete a Partition Using FDisk	Yes

Table 3-4

Results

The initial hash of the suspect drive was **42d48a8ee6c1b647a244e884606b106b**. An identical hash was generated after the Shadow was connected, after it was zeroed, and again after it had been disconnected. This indicates that the integrity of the drive was preserved throughout.

All commands executed generated the expected results. The Shadow did not inhibit the operation of the suspect system in any way.

4 CONCLUSION

The Shadow preserved the integrity of the drive being protected. This was true for all four test scenarios. Additionally, the device provided full read/write access so that the drive being examined could be used just as it was before the Shadow was connected.

As long as the Shadow remained connected, changes to the suspect drive were preserved even after the system under examination was rebooted. After using the “zero” function, these changes were discarded, and the drive reverted to its original state[3].

When the suspect system was hashed for the third time in each scenario, the hash generated was different from the other four. This indicates that the temporary changes made to the ShadowDrive are detected by DOS and the system BIOS. This discrepancy is merely temporary and is resolved when the ShadowDrive is zeroed.

The Shadow can also be used in a “locked” state. When in this mode, the device will function as a traditional write-blocking utility. Once the Shadow has been locked, it cannot revert to an unlocked state without being shutdown and restarted.

The “zero” and “lock” functions should only be enabled when the system being examined is powered off. Although implementing the “zero” or “lock” function while the system is running will not compromise the integrity of the drive being examined, it may cause the system to crash or become unstable during the next boot process.

The Shadow contains an 80 GB hard drive that serves as the ShadowDrive. This drive provided sufficient disk space for all of the commands executed during the evaluation. However, if a considerably high quantity of writes are made to the Shadow drive, it is possible to overload it with data. By utilizing a file generation program called RndFile, the user was able to create several extremely large files (10 GB) in an attempt to exceed the Shadow drive’s capacity. The creation of these files resulted in a system crash, but did not compromise the integrity of the drive being examined.

[3] In certain models of the Shadow, the “zero” button must be pressed three times before the drive is zeroed out. This issue has been corrected in later versions, but the product’s documentation fails to identify this anomaly.

Appendix I - Description of Executed Commands for Microsoft Windows

Create Files and Directories: Ten files were created by using the “New” command, and selecting a corresponding program. These files consisted of the following types: .txt, .doc, .xls, .zip and .bmp. These files ranged in size from 1 kilobyte to 1 megabyte. Five directories were then created using the “New Folder” command. Each directory accommodated two of the files. The files and directories were saved in the “c:” directory.

Copy Files and Directories: The aforementioned files and directories were copied to the system desktop via the “Copy” and “Paste” functions.

Rename Files and Directories: The ten created files and directories were renamed using the “Rename” function.

Move Files and Directories: The created files and directories were moved from the desktop to the “My Documents” folder via the “Cut” and “Paste” functions.

Delete Files and Directories: The files and directories were sent to the Windows Recycle Bin via the “Delete” operation.

Change File Attributes: The “Read Only” and “Hidden” attributes were changed for each of the files and directories by using the “Properties” menu.

Create Partition – Disk Manager: Using the “Manage” function of “My Computer,” a 2GB FAT32 partition was created out of space that was previously unallocated.

Delete Partition - Disk Manager: Using the “Manage” function of “My Computer,” a 2GB FAT32 partition was deleted.

Install Software: The Microsoft Office XP Professional Software Suite was installed from a CD-ROM.

Remove Software: The Microsoft Office XP Professional Software Suite was uninstalled from the “Add/Remove Programs” menu of the “Control Panel.”

Add Users: Using the “Users” menu of the “Control Panel,” two user accounts with administrative priveledges were created.

Remove Users: The aforementioned user accounts were deleted via the “Users” menu of the “Control Panel.”

Change Admin Password: The administrator account password was changed using the “Set Password” option of the “Users” menu.

Change Admin Password: With ERD Commander Utilizing the “Locksmith” function of the ERD Commander 2002 bootable CD-ROM, the administrator password was changed, the machine was rebooted, and the user logged in with the new password.

Change Admin Password: With NT Password Editor Utilizing the Offline NT Password and Registry Editor Bootdisk, the administrator password was changed, the machine was rebooted, and the user logged in with the new password.

Update Operating System: The latest critical updates were downloaded from the Windows Update website (windowsupdate.microsoft.com.)

Clear Internet Cache: Utilizing the “Internet options” tab of the “Tools” drop down menu of Internet Explorer, the user deleted Internet history, cookies, and temporary Internet files.

Empty Recycle Bin: The user navigated to the Windows Recycle Bin and selected the “Empty Recycle Bin” option under the “File” menu.

Reboot Operating System: The operating system was rebooted by selecting “Restart” from within the “Shutdown” menu.

Disk Defragmenter: The user ran the “Disk Defragmenter” utility from the “System Tools” menu.

Edit a MS Word Document: The user opened two Microsoft Word documents and deleted all of the text present in the documents. The documents were then saved.

Edit a File in Notepad: The user opened two text files in Notepad and deleted all of the text present in the file. The files were then saved.

Edit a File With a Hex Editor: The user opened two text files with WinHex and made random changes to the data. The files were then saved.

Create Partition - Partition Magic: Using Partition Magic, the user created a 2GB FAT32 partition from space that was previously unallocated.

Convert Partition - Partition Magic: Using Partition Magic, the FAT32 partition was converted into an NTFS partition.

Resize Partition - Partition Magic: Using Partition Magic, the NTFS partition was changed from a size of 2GB to a size of 3 GB, adding space that was previously unallocated.

Delete Partition - Partition Magic: Using Partition Magic, the NTFS partition was deleted from the system.

Appendix II - Description of Executed Commands for Fedora Core

Create Files and Directories: Ten files were created using various programs. These files consisted of the following file types: .txt, .sxw, .sxc, .tar and .bmp. The files ranged in size from 1 kilobyte to 1 megabyte. Five directories were then created using the "New Folder" command. Each directory accommodated two of the files. The files and directories were saved in the root directory.

Copy Files and Directories: The aforementioned files and directories were copied to the system desktop via the "Copy" and "Paste" functions.

Rename Files and Directories: The ten created files and directories were renamed using the "Rename" function.

Move Files and Directories: The created files and directories were moved from the desktop to the "Home" folder via the "Cut" and "Paste" function.

Delete Files and Directories: The files and directories were sent to the Trash Bin via the "Move to Trash" operation.

Change File Attributes: The file permissions (Read/Write/Execute) were changed for each of the files and directories by using the "Properties" menu.

Mount File System: From the "Disk Management" menu, floppy disk and CD-ROM devices were mounted using the "Mount" operation.

Unmount File System: From the "Disk Management" menu, floppy disk and CD-ROM devices were unmounted using the "Unmount" operation.

Install Software Package: Using the "Add/Remove Packages" menu, various Linux packages were added from the Fedora Core 2 CD-ROM.

Remove Software Package: Using the "Add/Remove Packages" menu, the aforementioned packages were removed from the system.

Add Users: Two user accounts were created via the "Add User" function of the "Users and Groups" menu.

Remove Users: The two user accounts were removed via the "Delete" operation of the "Users and Groups" menu.

Change Root Password: The root password was changed via the “Root Password” menu.

Clear Internet Cache: Using the “Preferences” menu of the Mozilla web browser, the user implemented the “Clear History,” “Clear Cache,” and “Delete all Cookies” options.

Empty Trash: While in the “Trash” folder, all files were deleted from the system via the “Empty Trash” option.

Reboot Operating System: The system was rebooted by selecting the “Restart the Computer” option of the “Logout” menu.

Edit a File With Office Writer: The user opened two .sxw files in Open Office Writer and deleted all of the text present in the files. The files were then saved.

Edit a File With Emacs: The user opened two text files in the Emacs editing program and deleted all of the text present in the files. The files were then saved.

Edit a File With a Hex Editor: The user opened two text files with SHED (Simple Hex Editor), and made random changes to the data. The files were then saved.

Create Partition - Fdisk: Using the Fdisk program, a 2GB ext3 partition was created out of space that had previously been unallocated.

Delete Partition - Fdisk: Using Fdisk, the 2GB ext3 partition was deleted from the system.