NAME: \_\_\_\_Coleton Sanheim\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_



Lab 5: Experimenting with Encryption, Cloning and Destroying Images

ITSC 306: Computer Forensics

Table of Contents

[Lab Outcome 2](#_Toc494115352)

[Readings 2](#_Toc494115353)

[Introduction 2](#_Toc494115354)

[1.0 Setting Up 3](#_Toc494115355)

[Install PGP 3](#_Toc494115356)

[Acquire an Image using DCFLDD 3](#_Toc494115357)

[2.0 Encrypting an Unencrypted Image 4](#_Toc494115358)

[3.0 Acquiring an Image with Encryption 6](#_Toc494115359)

[4.0 Disk Cloning and Duplication 7](#_Toc494115360)

[5.0 Wiping Media 11](#_Toc494115361)

[References 14](#_Toc494115362)

ITSC 306: Computer Forensics

Lab 5: Experimenting with Encryption, Cloning and Destroying Images

Lab Outcome

* Using both Windows and Linux tools, acquire a secured image using encryption, clone the acquired image and securely destroy the image using wiping techniques.

Readings

Read the following from the textbook:

* Secure an Image with Encryption (pp. 211–218)
* Disk Cloning and Duplication (pp. 219–224)
* Secure Wiping and Data Disposal (pp. 224–228)

Introduction

Security is always a concern when handling forensic evidence. Whether it be storing images on a shared server, transferring images between investigators and lawyers, or transporting images between offices, the loss of evidence files or evidence files being accessed by an unknown party is of the utmost concern.

Security can be enforced using encryption. Single files or entire hard drives can be encrypted. In this lab, open source tools such as PGP and OpenSSL are used to encrypt acquired images, in addition to enforcing encryption on-the-fly. Simply deleting files is not a secure process to safeguard your data. Because of this, wiping media will be illustrated as a way to securely delete files and media.

1. Setting Up

## Install PGP

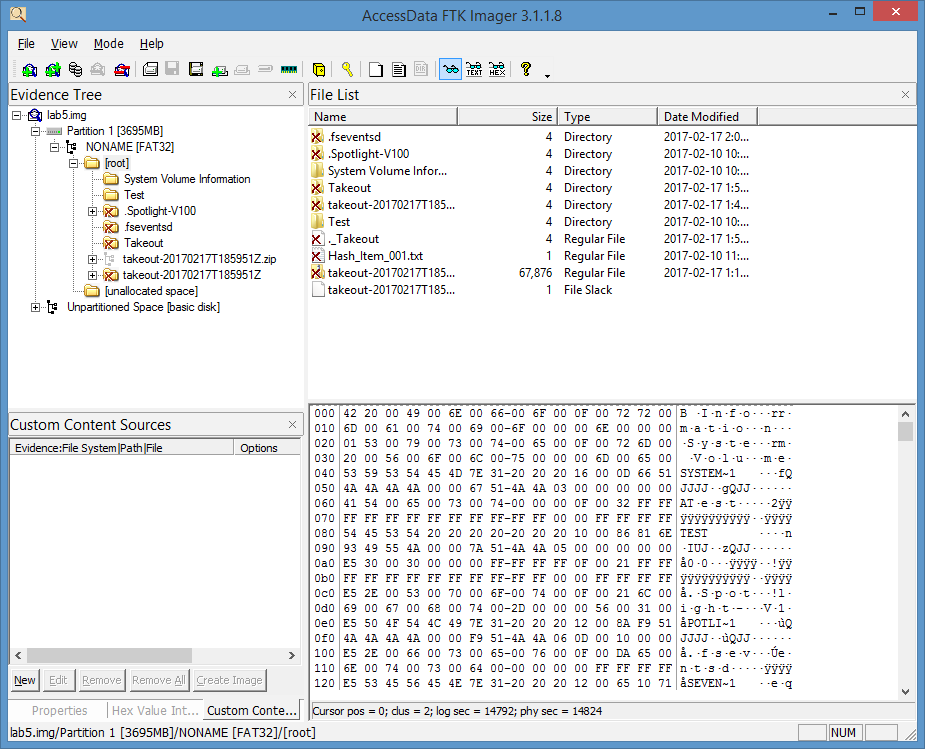
In order to invoke encryption during this lab, you will use both GPG and OpenSSL, which are installed on SIFT by default.

## Acquire an Image using DCFLDD

1. Using a USB drive, create an image entitled [ **lab5.img** ] using dcfldd to use in this lab.

[ sudo dcfldd bs=4k conv=noerror if=/dev/sdc of=lab5.img ]

1. Examine the image you created using FTK Imager to confirm that the image is readable.



**Figure 1:**

Source: FTK Imager. Reproduced and used in accordance with the fair dealing provisions in section 29 of the Canadian Copyright Act for the purposes of education, research or private study. Further distribution may infringe copyright.

1. Encrypting an Unencrypted Image

Once you have confirmed that your forensic image is readable by FTK Imager, encrypt the image previously acquired.

**Example 1: Encrypt an image file using PGP**

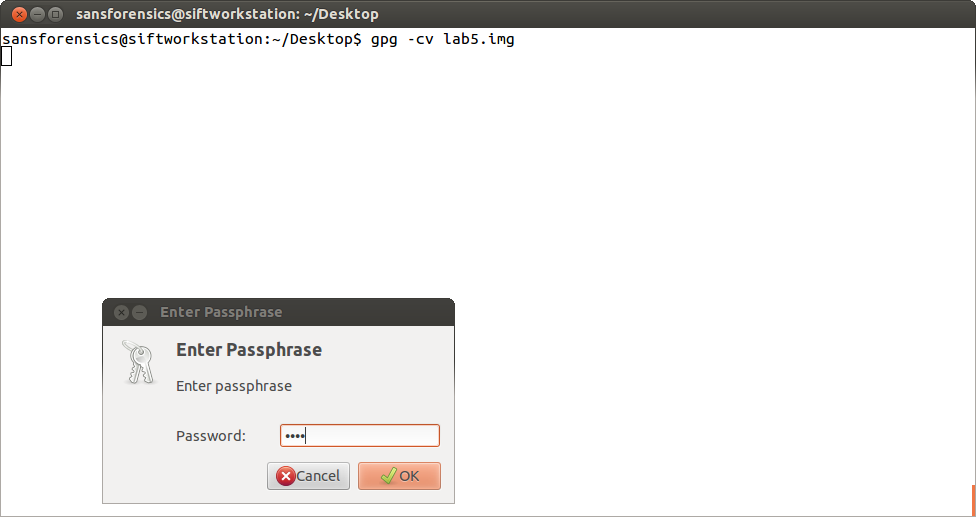
1. To encrypt an image using GPG, run the following command on the [ lab5.img ] file from the Desktop.

**Note:** SIFT also includes PGP.

[ gpg –cv lab5.img ]

An *Enter Passphrase* window appears in GPG.

1. Enter a password and select **OK**. Repeat the password and select **OK** again.

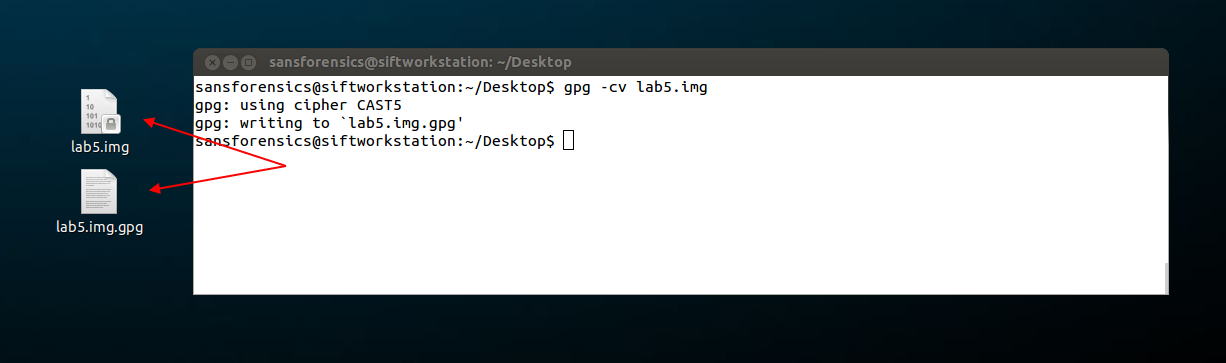


**Figure 2:**

Source: GnuPG. Reproduced and used in accordance with the fair dealing provisions in section 29 of the Canadian Copyright Act for the purposes of education, research or private study. Further distribution may infringe copyright.

**Notes:**

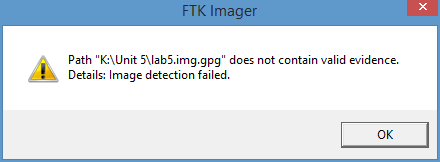
* There is no time indication associate to the encryption process.
* When the process completes, you will have two image files: [ lab5.img ] and   
  [ lab5.img.gpg ].



**Figure 3:**

Source: Sansforensics@SIFT-Workstation. Reproduced and used in accordance with the fair dealing provisions in section 29 of the Canadian Copyright Act for the purposes of education, research or private study. Further distribution may infringe copyright.

* If you use FTK Imager open the image, an error message appears. FTK doesn’t recognize the image file.



**Figure 4:**

Source: FTK Imager. Reproduced and used in accordance with the fair dealing provisions in section 29 of the Canadian Copyright Act for the purposes of education, research or private study. Further distribution may infringe copyright.

**Example 2: Encrypt an image file using openssl**

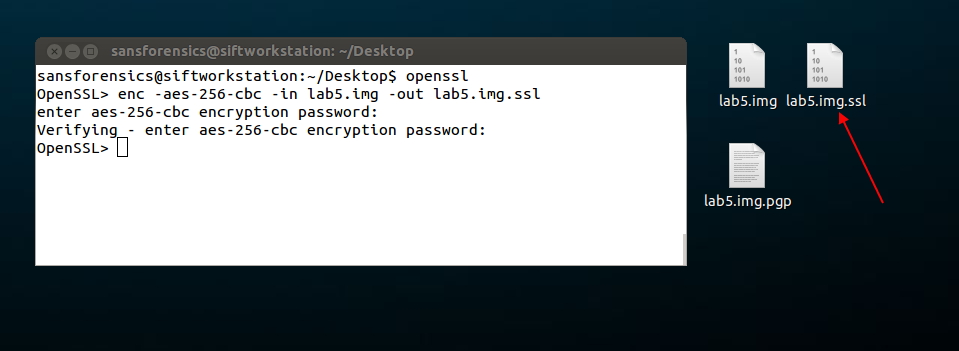
1. Open a terminal and navigate to your lab5.img file.
2. Start OpenSSL by running the command [ openssl ] from a terminal.
3. From the OpenSSL prompt, encrypt the image using the [ aes256 ] algorithm.

[ enc –aes-256-cbc –in (File to be Encrypted) –out (Filename of encrypted file) ]

[ enc –aes-256-cbc –in lab5.img –out lab5.img.ssl ]

1. When prompted by OpenSSL, enter a password for the encrypted file.

The file is encrypted (see Figure 5).



**Figure 5:**

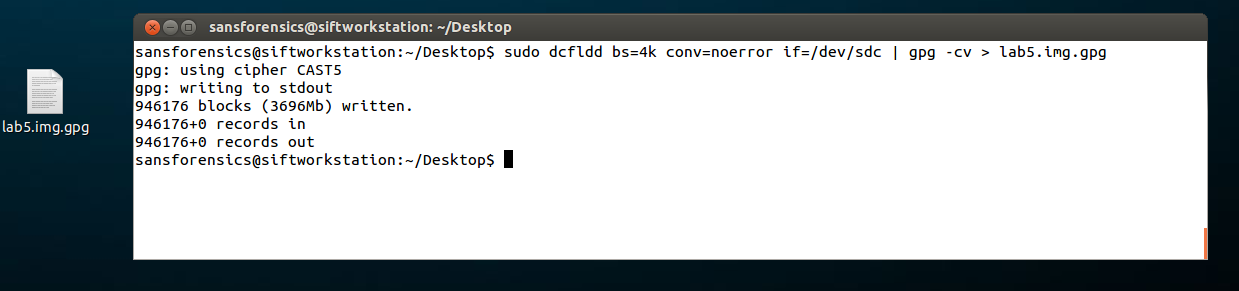
Source: Sansforensics@SIFT-Workstation. Reproduced and used in accordance with the fair dealing provisions in section 29 of the Canadian Copyright Act for the purposes of education, research or private study. Further distribution may infringe copyright.

1. Acquiring an Image with Encryption

Encrypting an image during the acquisition process is as easy as piping the file during acquisition to GPG or OpenSSL.

1. Pipe the acquisition to PGP during acquisition.
2. Enter your password when requested, and then click **OK**.

[ sudo dcfldd bs=4k conv=noerror if=/dev/sdc | gpg -cv > lab5.img.pgp ]



**Figure 6:**

Source: Sansforensics@SIFT-Workstation. Reproduced and used in accordance with the fair dealing provisions in section 29 of the Canadian Copyright Act for the purposes of education, research or private study. Further distribution may infringe copyright.

1. Disk Cloning and Duplication

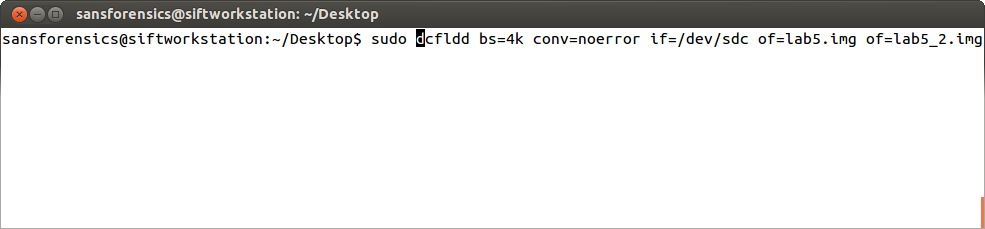
You can use DCFLDD at the time of acquisition to create two output files. By hashing the output files, you can confirm that they are clones of each other.

**Example 1:** **Cloning at time of acquisition**

1. Image a USB drive and create two output files.

[ dcfldd bs=4k conv=noerror if=/dev/(USB Drive) of=lab5.img of=lab5\_2.img ]

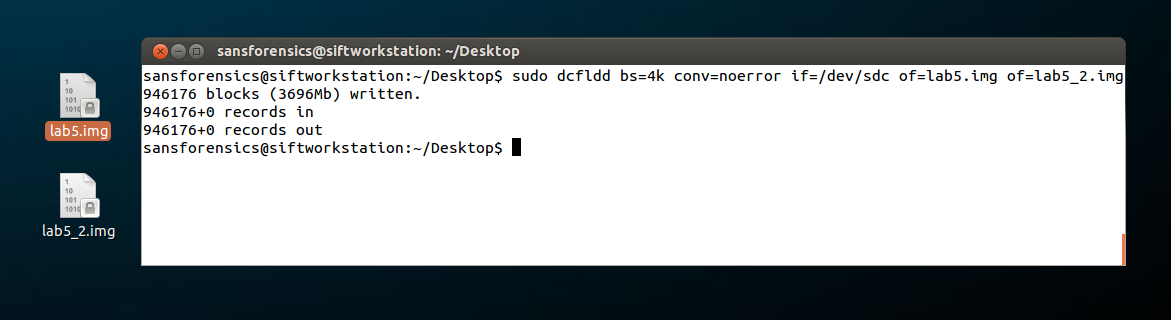
[ dcfldd bs=4k conv=noerror if=/dev/sdc of=lab5.img of=lab5\_2.img ]



**Figure 7:**

Source: Sansforensics@SIFT-Workstation. Reproduced and used in accordance with the fair dealing provisions in section 29 of the Canadian Copyright Act for the purposes of education, research or private study. Further distribution may infringe copyright.

Two image files are created: [ lab5.img ] and [ lab5\_2.img ].



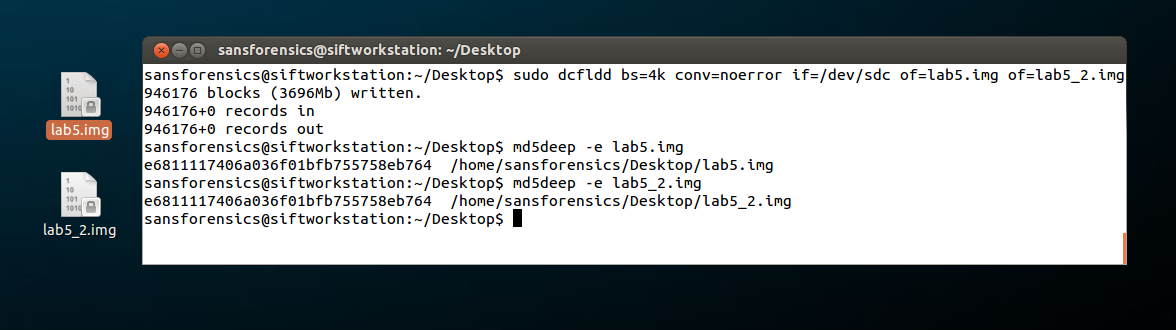
**Figure 8:**

Source: Sansforensics@SIFT-Workstation. Reproduced and used in accordance with the fair dealing provisions in section 29 of the Canadian Copyright Act for the purposes of education, research or private study. Further distribution may infringe copyright.

1. Use md5deep to hash the two image files. If they are clones, the hash values will match.

[ md5deep –e lab5.img ]

[ md5deep –e lab5\_2.img ]

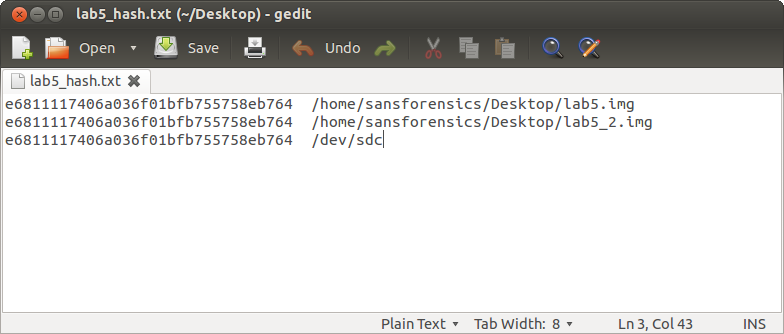


**Figure 9:**

Source: Sansforensics@SIFT-Workstation. Reproduced and used in accordance with the fair dealing provisions in section 29 of the Canadian Copyright Act for the purposes of education, research or private study. Further distribution may infringe copyright.

Observe that the two hash values match.

1. Hash the original UDB drive. All three hashes should match.



**Figure 10:**

Source: Sansforensics@SIFT-Workstation. Reproduced and used in accordance with the fair dealing provisions in section 29 of the Canadian Copyright Act for the purposes of education, research or private study. Further distribution may infringe copyright.

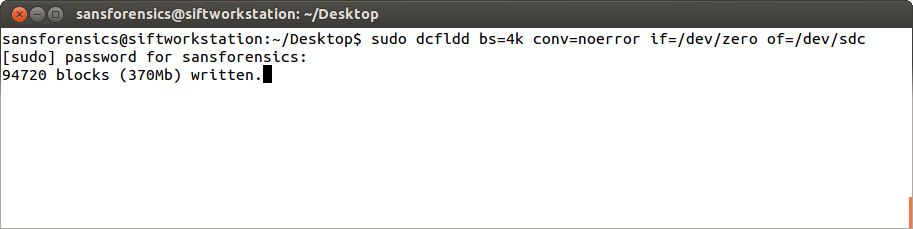
**Example 2: Cloning an image file to a drive**

In this example, take the lab5.img file and clone it to your USB drive. Because you are using your original USB drive, the only preparation on the disk is to wipe it of data.

1. Plug in your USB drive and ensure that it is recognized by the system.
2. From a terminal, run the following command to wipe the disk of data.

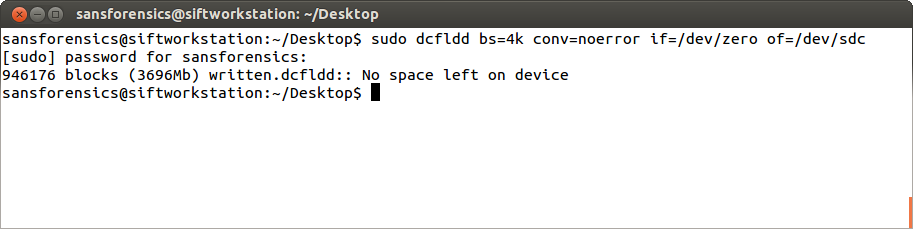
[ sudo dcfldd bs=4k conv=noerror if=/dev/zero of=/dev/sdc ]

1. Check that the device is all zeros.



**Figure 11:**

Source: Sansforensics@SIFT-Workstation. Reproduced and used in accordance with the fair dealing provisions in section 29 of the Canadian Copyright Act for the purposes of education, research or private study. Further distribution may infringe copyright.



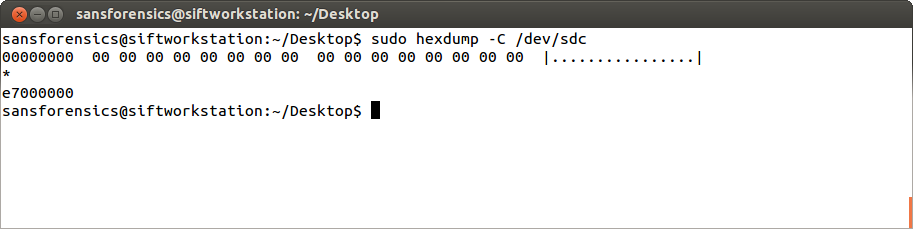
**Figure 12:**

Source: Sansforensics@SIFT-Workstation. Reproduced and used in accordance with the fair dealing provisions in section 29 of the Canadian Copyright Act for the purposes of education, research or private study. Further distribution may infringe copyright.

1. Verify the disk has been wiped by running the following command:

[ sudo hexdump –C /dev/(device) ]

[ sudo hexdump –C /dev/sdc ]

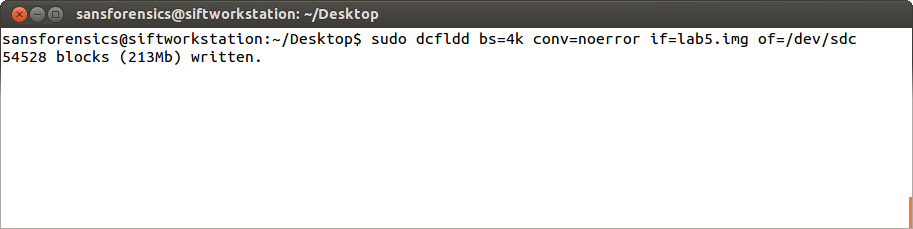


**Figure 13:**

Source: Sansforensics@SIFT-Workstation. Reproduced and used in accordance with the fair dealing provisions in section 29 of the Canadian Copyright Act for the purposes of education, research or private study. Further distribution may infringe copyright.

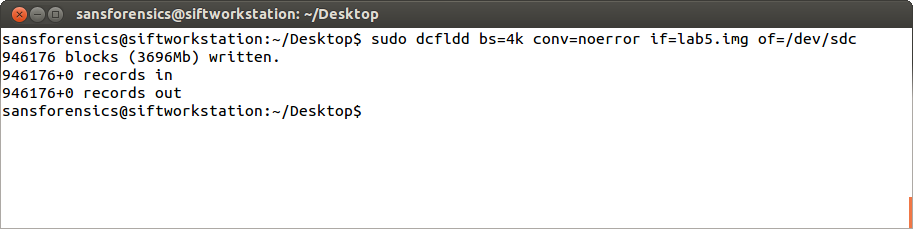
1. Clone the USB disk with your lab5 image by running the following command using dcfldd. The input file is your lab5.img.

[ sudo dcfldd bs=4k conv=noerror if=lab5.img of=/dev/sdc ]



**Figure 14:**

Source: Sansforensics@SIFT-Workstation. Reproduced and used in accordance with the fair dealing provisions in section 29 of the Canadian Copyright Act for the purposes of education, research or private study. Further distribution may infringe copyright.

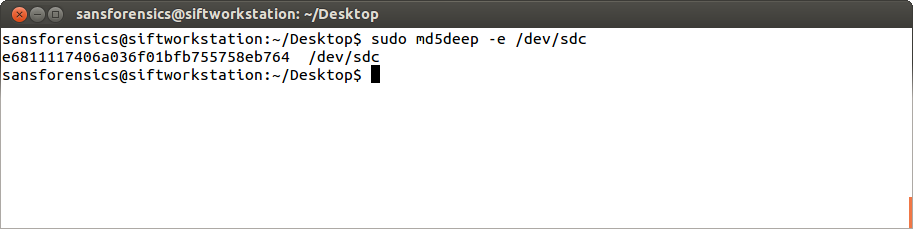


**Figure 15:**

Source: Sansforensics@SIFT-Workstation.. Reproduced and used in accordance with the fair dealing provisions in section 29 of the Canadian Copyright Act for the purposes of education, research or private study. Further distribution may infringe copyright.

1. Confirm the process, hash the USB drive to verify the clone. The hash should match the original lab5.img hash previously executed:

(e6811117406a036f01bfb755758eb764 /dev/sdc)



**Figure 16:**

Source: Sansforensics@SIFT-Workstation. Reproduced and used in accordance with the fair dealing provisions in section 29 of the Canadian Copyright Act for the purposes of education, research or private study. Further distribution may infringe copyright.

1. Wiping Media

Wiping media can be used to wipe single files or complete storage devices.

**Example 1: Wiping a single file**

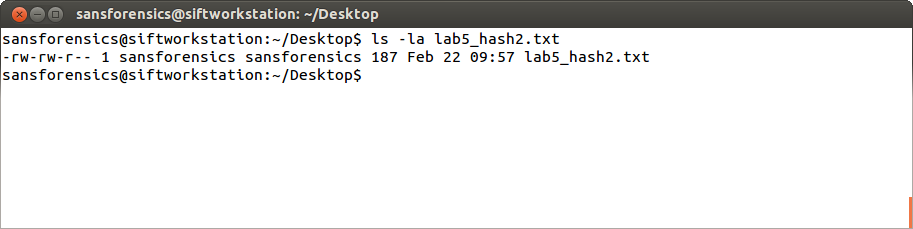
1. Copy the [ lab5\_hash.txt ] file as [ lab5\_hash2.txt ].

To use dd to wipe this file, you need to know the block size.

1. Run the following command and note the size of the file in bytes. This value will be used as our block size.

[ ls –la (file to wipe) ]

[ ls –la lab5\_hash2.txt ]



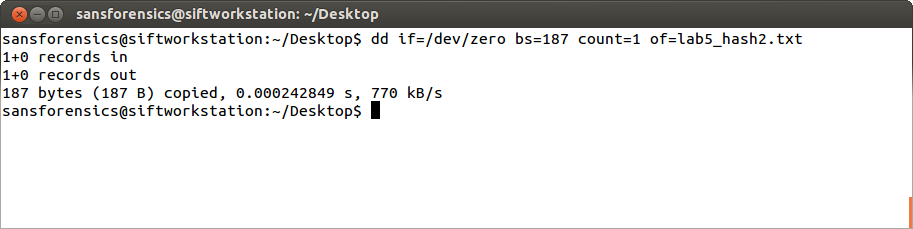
**Figure 17:**

Source: Sansforensics@SIFT-Workstation .Reproduced and used in accordance with the fair dealing provisions in section 29 of the Canadian Copyright Act for the purposes of education, research or private study. Further distribution may infringe copyright.

In this example, the file size is 187 bytes.

1. Use the file size in the dd command to wipe the file. Our count equals 1, meaning the file will only be read and written to once.

[ dd if=/dev/zero bs=187 count=1 of=lab5\_hash2.txt ]

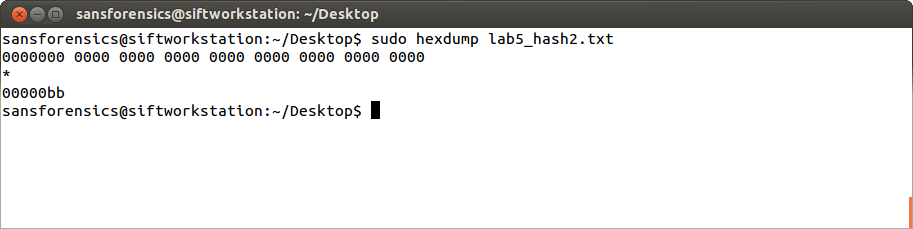


**Figure 18:**

Source: Sansforensics@SIFT-Workstation. Reproduced and used in accordance with the fair dealing provisions in section 29 of the Canadian Copyright Act for the purposes of education, research or private study. Further distribution may infringe copyright.

1. Verify the file has been zero-ed out.

[ sudo hexdump lab5\_hash2.txt ]



**Figure 19:**

Source: Sansforensics@SIFT-Workstation. Reproduced and used in accordance with the fair dealing provisions in section 29 of the Canadian Copyright Act for the purposes of education, research or private study. Further distribution may infringe copyright.

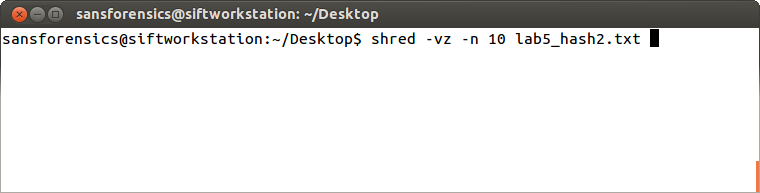
**Example 2: Using the shred command to wipe files**

The shred command has additional options, such as writing random characters or zeros, and writing a number of times.

1. Copy the [ lab5\_hash.txt file ] and rename it as [ lab5\_hash2.txt ].
2. In a terminal, run the shred command with the [ v ] [ z ] and [ n ] options.

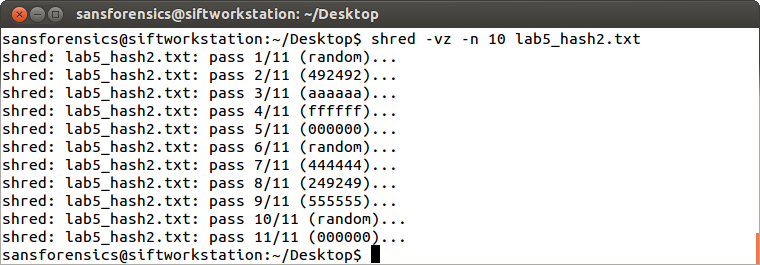
**Note:** [ v ] is verbose, [ z ] is use zeros in the final wipe and [ n ] is the number of times.

[ shred –vz –n 10 lab5\_hash2.txt ]



**Figure 20:**

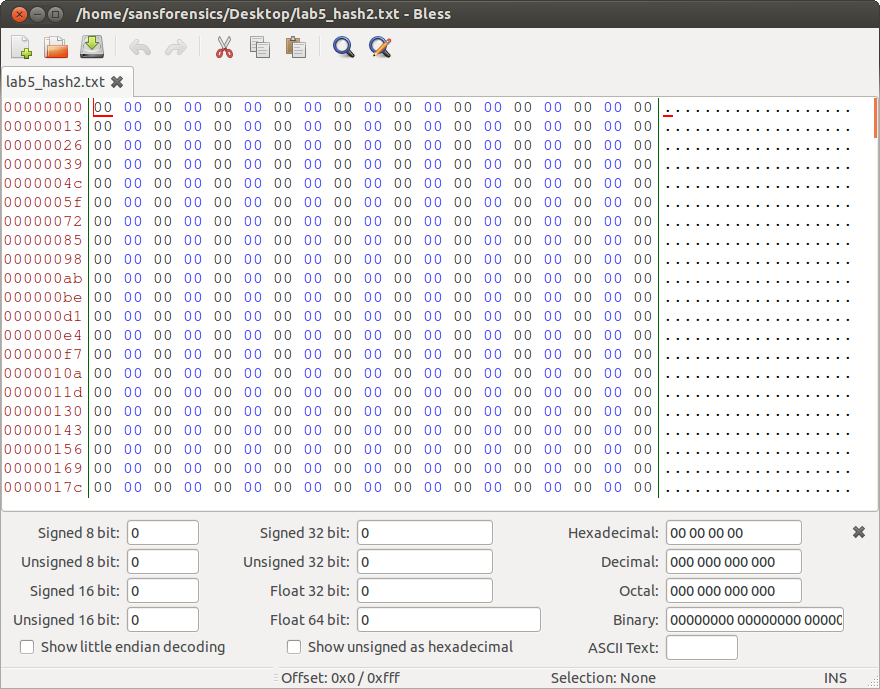
Source: Sansforensics@SIFT-Workstation .Reproduced and used in accordance with the fair dealing provisions in section 29 of the Canadian Copyright Act for the purposes of education, research or private study. Further distribution may infringe copyright.



**Figure 21:**

Source: Sansforensics@SIFT-Workstation. Reproduced and used in accordance with the fair dealing provisions in section 29 of the Canadian Copyright Act for the purposes of education, research or private study. Further distribution may infringe copyright.

1. Use the Bless Hex Editor in SIFT to verify that the file has been wiped.



**Figure 22:**

Source: Sansforensics@SIFT-Workstation. Reproduced and used in accordance with the fair dealing provisions in section 29 of the Canadian Copyright Act for the purposes of education, research or private study. Further distribution may infringe copyright.

References

AccessData. 2010. FTK Imager Lite version 3.1.1 [Computer software]. Retrieved from <http://accessdata.com/product-download/ftk-imager-lite-version-3.1.1>

Sansforensics@SIFT-Workstation 2014. {Computer Software]. Retrieved from <https://digital-forensics.sans.org/community/downloads>