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



Lab 4B:   
Forensic Image Acquisition – Capturing and Validating

ITSC 306: Computer Forensics

Table of Contents

[Lab Outcomes 2](#_Toc494887955)

[Readings 2](#_Toc494887956)

[Introduction 2](#_Toc494887957)

[1.0 Setting Up the SIFT Workstation 3](#_Toc494887958)

[2.0 USB Set-up 3](#_Toc494887959)

[3.0 Acquiring RAM Using DumpIt 3](#_Toc494887960)

[4.0 Hashing the USB Drive 3](#_Toc494887961)

[5.0 Image the USB Drive 4](#_Toc494887962)

[6.0 Lab Extras: Mount the Image.raw Capture 4](#_Toc494887963)

[References 6](#_Toc494887964)

ITSC 306: Computer Forensics

Lab 4B: Forensic Image Acquisition – Capturing and Validating

Lab Outcomes

* Capture RAM from a running Windows system.
* Hash the drive used to capture the RAM.
* Image the drive used to capture the RAM.
* Mount the image file to confirm its contents.

Readings

* Your instructor will provide any additional reading suggestions.

Introduction

The goal of this lab is to complete several core forensic functions. The first is to acquire RAM from a Windows operating system. Once you’ve acquired the RAM, the next step is to hash and image the USB drive used to capture the RAM. Finally, a new concept of mounting the image file will be demonstrated.

1. Setting Up the SIFT Workstation
2. Start your SIFT workstation.
3. On your desktop, create a folder named **Lab5**.
4. Open the program **gedit** and create a text file entitled **lab5\_Notes.txt**. Use this file to keep notes of the lab process.
5. USB Set-up

DumpIt is used to acquire the RAM from a Windows OS.

**Note:** The USB must be larger than the RAM in the Windows system.

1. Note how much RAM is on the Windows system.
2. Plug in your USB drive and ensure it is recognized by Windows in Windows Explorer.
3. Format the drive FAT32 or NTFS and label the drive **LAB5**.

Note: The USB can use FAT32 format. However, remember that up to 4 GB of RAM can be acquired using FAT32, so if the suspect machine has more than 4 GB of RAM, use NTFS format.

1. Copy the **DumpIt.exe** file you used in Lab 2 onto the USB drive. You can also download it from <https://comae.typeform.com/to/XlvMa7>.
2. Acquiring RAM Using DumpIt
3. Open a Command Prompt with Administrator privileges and change the drive letter to that of your USB drive.
4. Run DumpIt and acquire the RAM.
5. Complete your notes documenting the process you followed.
6. Once completed, eject the USB drive.
7. Hashing the USB Drive
8. Open a Terminal in SIFT and run tail –f /var/log/syslog.
9. Attach the USB drive and note the device name.
10. Remount the drive to read only.
11. Hash the device using md5sum and direct the output to a text file named **preHash.txt** in the **Lab5** folder on your Desktop.
12. Confirm the text file was created.
13. Recursively hash the files on the USB drive and output the results to a text file named **fileHash.txt**.
14. Image the USB Drive
15. Using the command dcfldd, image the drive to the **Lab5** folder on your Desktop. Name the image **image.raw** and md5 hash the image while it’s being acquired.
16. Confirm that the preHash and the acquisition hashes match.
17. Update your notes.
18. Lab Extras: Mount the Image.raw Capture
19. Run the command ls /mnt to confirm that there is a /mnt/usb entry. If not, create a USB mount point:

mkdir /mnt/usb.

1. Mount the image file. The standard command is:

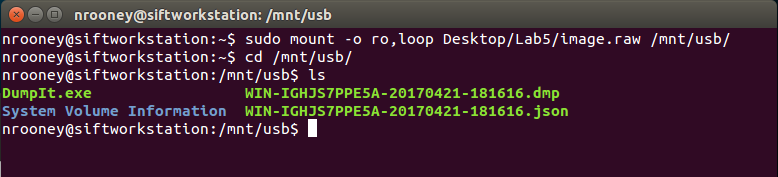
sudo mount options Path to Image File Mount Point

sudo mount –o ro,loop Desktop/Lab5/image.raw /mnt/usb

This command says to mount the image, -o using the options ro,loop (Read Only and Loop) and the mount point /mnt/usb.

The loop device allows you to mount regular files as if they were block devices..

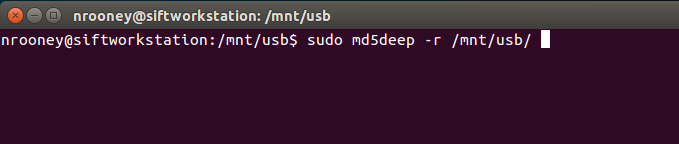
1. Change into the /mnt/usb directory and run ls to view the contents of the **image.raw** file.



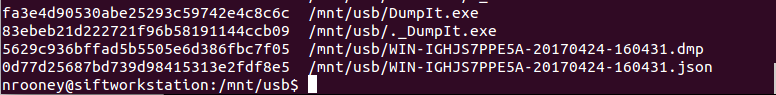
**Figure 1: Image File**

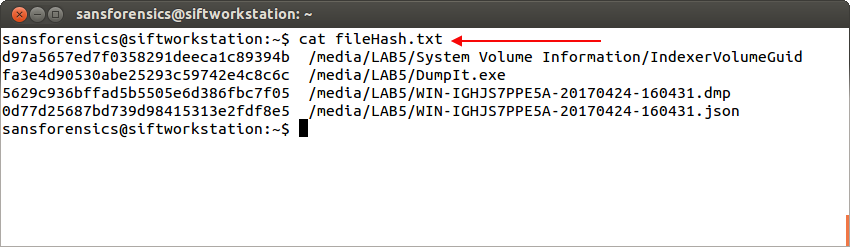
Source: SANS Institute. Reproduced and used in accordance with the fair dealing provisions in section 29 of the Canadian Copyright Act for the purposes of education, research or private study. Further distribution may infringe copyright

1. Hash the files in the mounted image to confirm that the hash values match those created in Part 4.0.



:



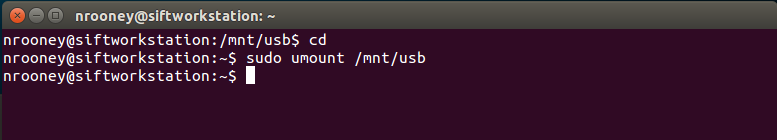


Source: SANS Institute. Reproduced and used in accordance with the fair dealing provisions in section 29 of the Canadian Copyright Act for the purposes of education, research or private study. Further distribution may infringe copyright

1. Unmount the image file.

cd

sudo umount /mnt/usb



**Figure 2: Unmount Image**

Source: SANS Institute. 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. Update your notes and forward them to your instructor.

References

SANS Institute (2017). SIFT Workstation [VMware Appliance]. Retrieved from https://digital-forensics.sans.org/community/downloads