NAME: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_



Lab 4A:   
Forensic Image Acquisition – Acquiring a RAM Image from a Linux Operating System

ITSC 306: Computer Forensics

Table of Contents

[Lab Outcome 2](#_Toc494886090)

[Readings 2](#_Toc494886091)

[Introduction 2](#_Toc494886092)

[1.0 USB Setup 3](#_Toc494886093)

[2.0 Acquiring Linux RAM using Lime 8](#_Toc494886094)

[References 12](#_Toc494886095)

ITSC 306: Computer Forensics

Lab 4A: Forensic Image Acquisition – Acquiring a RAM Image from a Linux Operating System

Lab Outcome

* Complete the acquisition of RAM from a Linux operating system.

Readings

* The [lmg README information](https://github.com/halpomeranz/lmg) (https://github.com/halpomeranz/lmg)

Introduction

As you’ve already learned, the best place to discover malware is in RAM. Malware has to run, and with RAM size steadily increasing, and with specialized software to parse through the dump, memory is becoming a secondary file system.

The first step in any investigation involving the acquisition of a computer system is to first acquire the memory. It is extremely that you not immediately “pull the plug” on a system because too much valuable data could be lost.

Unlike the straightforward capture of volatile memory from a Windows operating system using tools such as DumpIt or FTK Imager, the Linux kernel can be more difficult. Since the Linux kernel upgrade to 2.6, you can no longer use DD to capture the [ /dev/mem ] data.

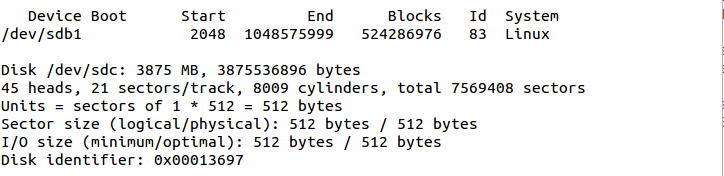
However, third party tools have been created to capture RAM from a Linux OS. The Linux Memory Grabber (lmg) script enables you to run a command from a USB drive that targets the system, captures the RAM and builds a Volatility profile that can be used when analyzing the system.

1. USB Setup

To complete the methodology suggested in this lab, you need to acquire and access specific tools using a USB drive that is formatted ext4 to interact with Linux.

**Note:** Use a separate USB drive so you don’t lose the USB data created in Lab 2 to capture RAM from a Windows OS.

1. Download the following tools:
   * **lmg-master.zip** from <https://github.com/halpomeranz/lmg>
   * **Lime-master.zip** source code from <https://github.com/504ensicsLabs/LiME>
   * **Volatility 2.3.1.zip** source code from [www.volatilityfoundation.org/releases](http://www.volatilityfoundation.org/releases)
2. Prepare the USB drive.
   1. Open a terminal and run the command tail –f /var/log/syslog.
   2. Plug in the USB drive and note the device label. In this case, **sdc**.
   3. In a second terminal, run the command sudo fdisk -l and note the size of the USB disk. This is used when formatting the drive with ext4.



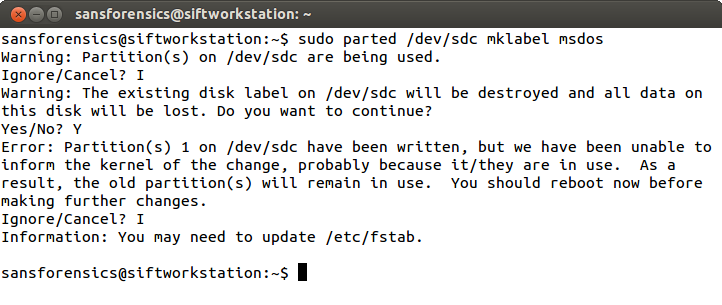
**Figure 1:**

* 1. Format the USB drive (ext4) by running the following commands. Select **Ignore** for any warning messages.

parted /dev/sdc mklabel msdos

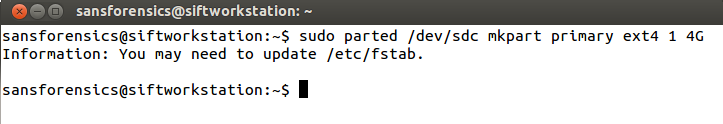
parted /dev/sdc mkpart primary ext4 1 4G

**Note:** The size of the USB drive is 4G. In this case, the drive is 4GB, as determined in Step 2.



**Figure 2:**

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



**Figure 3:**

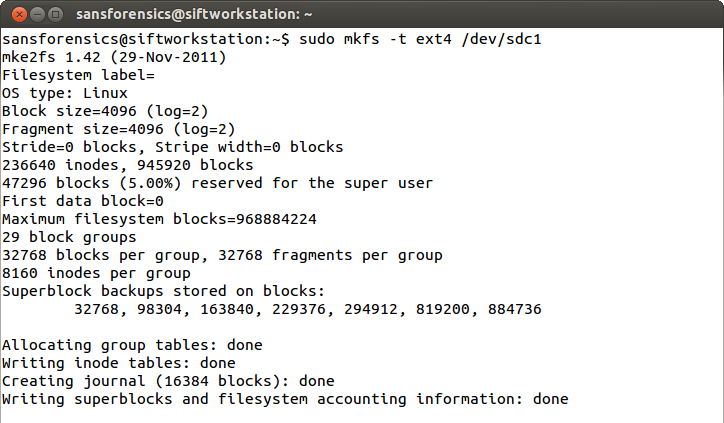
Source: SANS Institute. Reproduced and used in accordance with the fair dealing provisions in section 29 of the Canadian Copyright Act for the purposes of education, research or private study. Further distribution may infringe copyright:

* 1. Unmount the USB to format the drive.

sudo umount /dev/sdc1

* 1. Write the ext4 file system to the drive.

sudo mkfs –t ext4 /dev/sdc1



**Figure 4:**

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:

The drive has now been formatted as ext4. You can now install the Lime software.

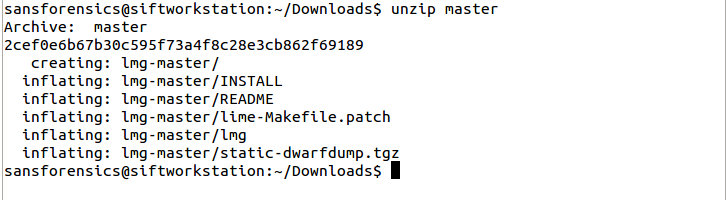
1. Install Lime software.
2. Create a folder named **lime** on the root of the USB drive.



**Figure 5:**

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. Unzip the **master** or **lmg-master** folder in your **Downloads** folder.



**Figure 6:**

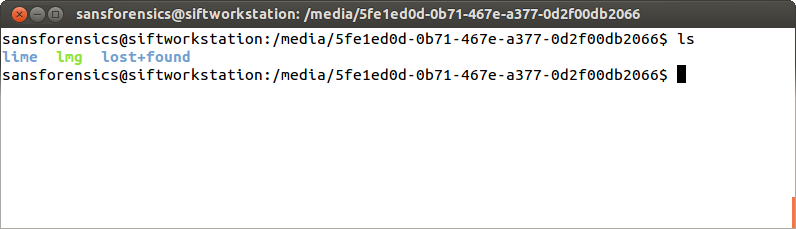
Source: SANS Institute. Reproduced and used in accordance with the fair dealing provisions in section 29 of the Canadian Copyright Act for the purposes of education, research or private study. Further distribution may infringe copyright

1. Copy the **lmg** file in the **lmg-master** folder to the root of your USB drive.

The lmg file and lime folder appear in the root.

1. Ensure the lmg file is executable by entering the following command:

sudo chmod +x /media/(USB Drive)/lmg ]

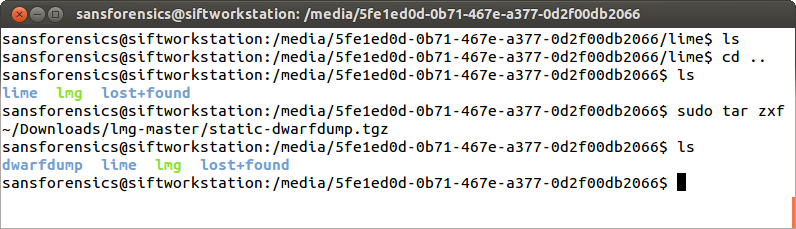


**Figure 7:**

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. Extract the **static-dwarfdump.tgz** file to the root of the USB drive from /media/(USB).

sudo tar zxf ~/Downloads/lmg-master/static-dwarfdump.tgz

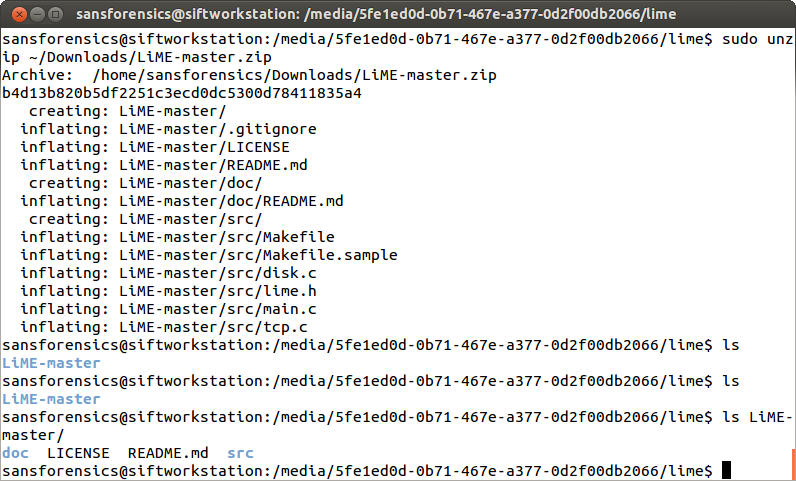


**Figure 8:**

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. Navigate to the **lime** folder on the USB and unzip the contents of the   
   **Lime-master.zip** folder to it:

sudo unzip ~/Downloads/Lime-master.zip

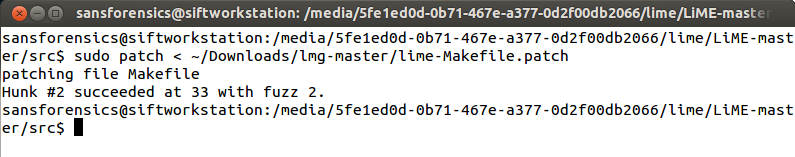


**Figure 9:**

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. Run the available patch file to work with both 32- and 64-bit operating systems by navigating to the **lime/Lime-master/src** folder and running the following command:

sudo patch < ~/Downloads/lmg-master/lime-Makefile.patch



**Figure 10:**

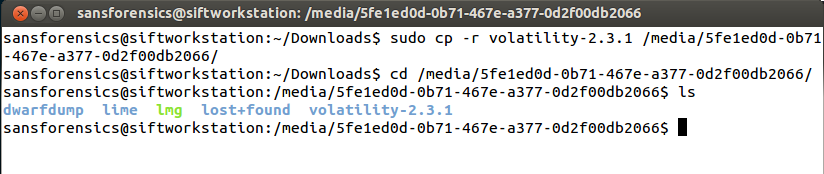
Source: SANS Institute. Reproduced and used in accordance with the fair dealing provisions in section 29 of the Canadian Copyright Act for the purposes of education, research or private study. Further distribution may infringe copyright

1. Install Volatility
2. Extract the contents of the **volatility-2.3.1.zip** file to the **Downloads** folder.

sudo unzip ~/Downloads/volatility-2.3.1.zip

1. Copy the volatility folder to the root of the USB drive.

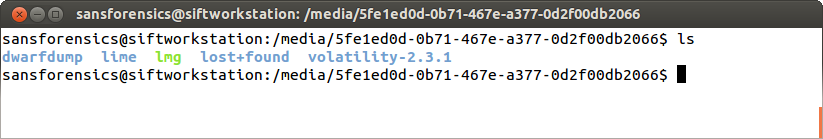
sudo cp –r volatility-2.3.1 /media/(USB Drive)



**Figure 11:**

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. Ensure that the USB drive is ready and contains the following files:



**Figure 12:**

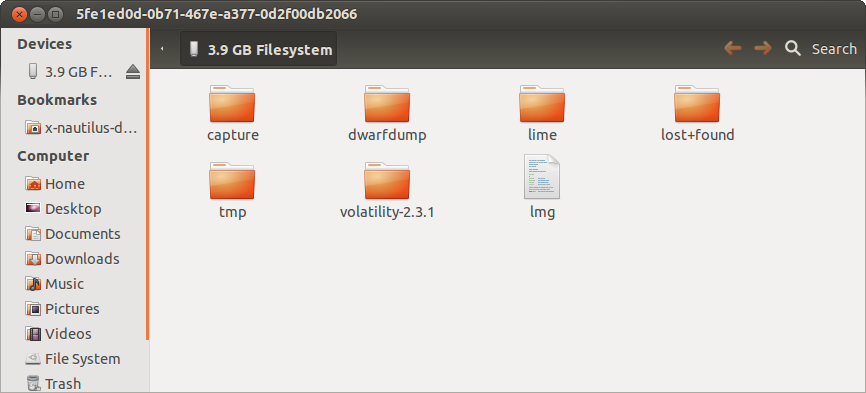
Source: SANS Institute. Reproduced and used in accordance with the fair dealing provisions in section 29 of the Canadian Copyright Act for the purposes of education, research or private study. Further distribution may infringe copyright

2.0 Acquiring Linux RAM using Lime

When preparing a USB drive with Lime installed, ensure that the USB drive is larger than the amount of RAM you are obtaining.

1. Plug in the prepared USB drive to the Linux SIFT system.

SIFT auto-mounts the drive.



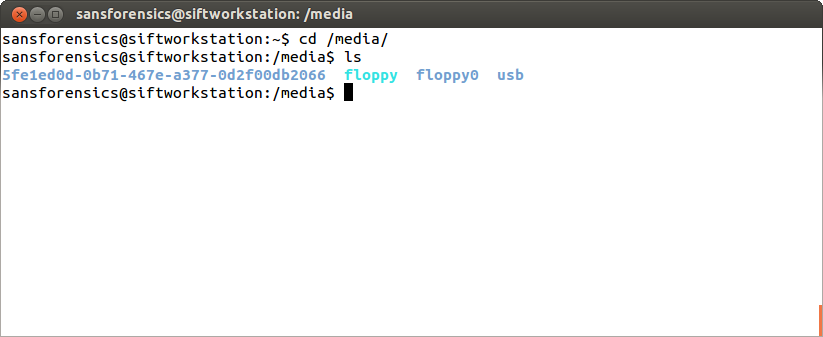
**Figure 13:**

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. Open a Command Prompt and navigate to **/media**. Run the ls command and check that the USB has been mounted.

cd /media

ls

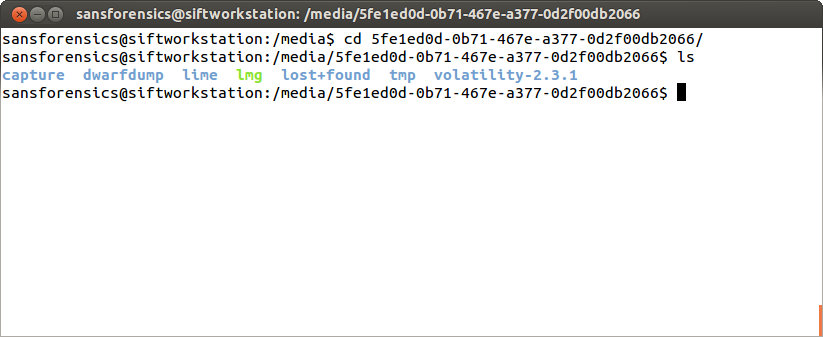


**Figure 14:**

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. Navigate to the root of your USB drive and then run the lmg script.

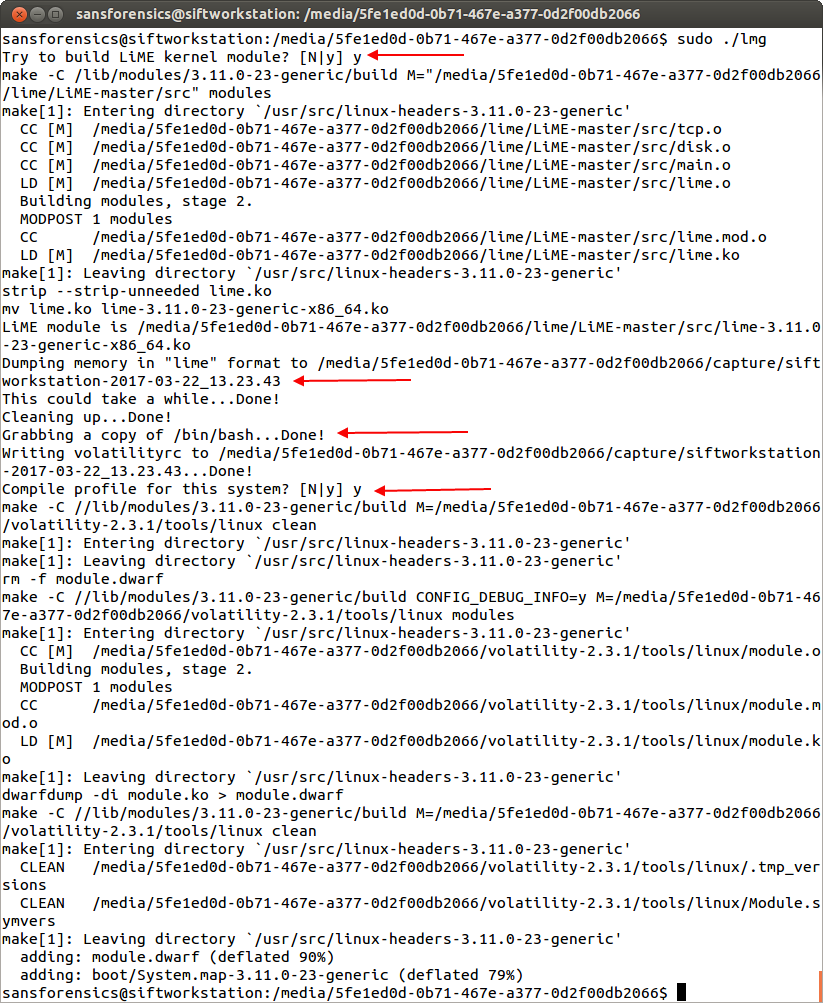
sudo ./lmg



**Figure 15:**

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. When the program requests to build a LiME kernel module, select **y**.
2. When the program asks: Compile profile for this system, select **y**.

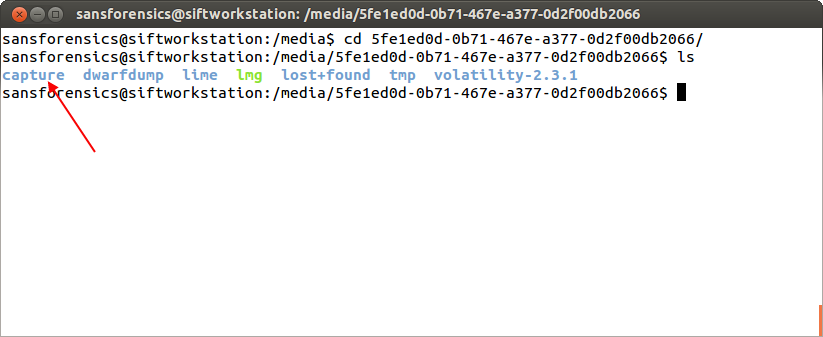


**Figure 16:**

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

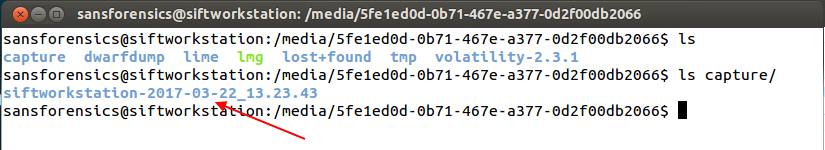
1. Confirm the capture.

When finished, a **capture** folder is created containing the RAM dump.



**Figure 17:**

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



**Figure 18:**

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

References

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