## CIT 430/530

## Forensic Lab #4 – Mirror Imaging Suspect HDs

In this lab, you will remotely mirror a suspect’s hard drive, store the file as an image on a destination device, then perform a brief analysis.

## Introduction

In real-world settings, the main requirement for mirroring hard disks, is that the destination device has **at least as** much space as the suspect’s hard drive. A destination could be another Hard Disk, USB or CD/DVD. Since we use VMs and have limited disks space, full mirroring may not be possible.

|  |  |  |
| --- | --- | --- |
| Suspect’s disk on another computer |  | Destination disk on another computer |
|  | Cloned data |  |
| **IP = 10.2.56.26**  *Source Device* |  | **Forensic Workstation**  *Destinatin Device* |

## Tools

* dd
* R-Linux

## Part 1: Background

Due to the limited space on the target system, a copy of the hard drive (HD) on the target has been created for you. The steps used to make the image file are explained below. In this example, SIFT acts as the ‘forensic workstation’ and device at 10.2.56.15 is the ‘target’ machine.

|  |  |
| --- | --- |
| **1** | SSH connection created from SIFT to target being hosted on a remote network. |
|  |  |
| **2** | Once the ssh connection completes, the SIFT terminal prompt changes to the target prompt.  The account used to access the target does not have the necessary priviledges. The ‘sudu su’ command raises ‘student’ to ‘root’. The ‘dd’ command is issued to create a bit-for-bit copy of the target device’s HD structure and saved as a raw (.dd) image file. |
|  |  |
| **3** | When ‘dd’ completes, the connection is closed and the sansforensic prompt returns. |

## Tasks Part 1: Mirroring Suspect HD

In this section you will securely connect to the target and copy the .dd image file to your SIFT workstation. As shown above, the target machine was initially mirrored using a ssh connection and the dd program.

Since this is a lab environment, the tools we use are free and often have limitations. For examinations completed by professional forensics investigators, tools such as Encase Enterprise, ProDiscover can be used to acquire images remotely and securely. Although these tools are popular and useful, their expense often results in investigations being carried out with tools such as the ones we use in this course.

1. On your forensic workstation issue the following command:

**sftp** [**student@10.2.56.1**](mailto:student@10.2.56.26)**5**

* + Note: when prompted for a password(s) enter **cit247**

**get SuspectHD.dd**

* + Note: the copy process may take several minutes

## Tasks Part 2: Image Analysis

In this section of the lab you will use the program RLinux to perform brief analysis of the SuspectHD.dd file. RLinux is a tool primarily used for data recovery, but it is also useful in forensic investigations.

1. RLinux has been installed on your system already. Issue the following commands from the to run the program.

**cd Downloads/usr/local/R-Linux/bin**

**sudo ./R-Linux**

1. Accept any messages when the R-Linux GUI starts
2. In R-Linux, select the “Open Image” button to load the SuspectHD.dd image file created in Part 1.
3. Allow R-Linux to scan the image, by hitting the “Scan” button and selecting ‘Detailed’ scan.
   1. Note: All other settings can be kept as is.
4. Examine the outputs returned by R-Linux
5. In a new terminal, use the **sudo fdisk -l** command against the SuspectHD.dd file and compare its results to the report from R-Linux.

## Submission

Although R-Linux is a data recovery application, it can also be used as a forensic tool. Once you’ve completed the steps above provide a one to two-page, double-spaced write-up addressing the following:

* Instances/examples a data recovery tool can be used during a digital forensic investigation.
  + *It may be helpful to review the* [*R-Linux user manual*](https://www.r-tt.com/downloads/Free_Linux_Recovery_Manual.pdf) *and test out some of its features.*
* Explain how an investigator can verify the mirror image they created from a suspects HD is an exact bit-for-bit copy.
  + *Your answer should not refer to opening suspect files/directories etc.*
* Benefits and disadvantages of acquiring data remotely
* A comparison of outputs returned by fdisk and RLinux
* In your opinion, which tool provides more forensic value, if any? What is your reasoning behind your choice?

Kaleb Alstott

When looking at R-Linux there is a lot of cool and unique features that make this tool so useful. Looking over the [*R-Linux user manual*](https://www.r-tt.com/downloads/Free_Linux_Recovery_Manual.pdf) there is multiple ways that the R-Linux tool could be used for data recovery methods. Overall, this tool is used when and for recovering files on damaged or deleted partitions, files removed by virus attack or power failure, after the partition with the files was reformatted even for a different file system, and much more. This would be useful in a digital forensics’ investigation due to how helpful this tool is at recovering data. In an investigator can verify that a mirror image he/she created is an exact same from the suspects HD is an exact bit for bit copy is by identifying the hash values and comparing if they are the same. If they are the same, then the mirror copy is an exact bit for bit image from the suspects. When looking at requiring data remotely there can be quite a few advantages and disadvantages to how you extract your data. The advantages of requiring data remotely can be mostly summed in cost efficient, speed of how data is retrieved, and most of all it is contactless. The disadvantages of acquiring data remotely are few and far but some may be network reliability, ability to troubleshoot, remote acquisition capabilities of mobile devices, etc. When we ran our tests of fdisks and R-Linux they were very similar and showed a lot, of the same data, the only clear differences I was able to see is that R-Linux showed a lot more in-depth information about partitions and their values. When looking at the R-Linux we can see it is very clear cut and formatted in a graph type view that is easy to identify what you are looking for. This is a very simple and effective way at looking at this data recovery. When we look at fdisk we see a lot of basic information that is printed out as normal such as sectors, size, start and end, type, but what is different here is that the fdisk failed to read the extended partition table. Finally, in my opinion I would say that the R-Linux tool provided the most forensic value in this investigation. I think this is because it is clearer cut and straight forward mostly, but also the R-Linux was able to read and display more information about the partitions is what stood out to me most.