## CIT 430/530: Forensic Lab #3 – Forensic Disk and File Analysis

Throughout this lab you will explore forensic image files using various tools. In the first part, you’ll work with an Expert Witness Format (EWF), also known as the ‘Encase’ format image. EWF images are commonly used to standardize and organize the data copied from a suspect’s system.

The second part of the lab introduces you to the open source forensic tool Autopsy. While there are several commercial and non-commercial forensic tools available, Autopsy is commonly used as a reliable and effective application for completing multiple forensic tasks during a computer forensic investigation. During this part of the lab you’ll use Autopsy to view the content of a forensic image file.

Lastly, you will use several command-line tools to view an image files structure and compare the outputs from each command.

## Part 1: Examining ewf images

cd to Downloads and use wget to download the compressed practice files.

**wget http://linuxleo.com/Files/NTFS\_Pract\_2017\_E01.tar.gz**

Verify the files have not been corrupted while copying by calculating a sha1 hash and comparing the returned output to the hash value below:

**sha1sum NTFS\_Pract\_2017\_E01.tar.gz**



Next, untar the file and change to the new directory containing the ewf image files.

**tar xzvf NTFS\_Pract\_2017\_E01.tar.gz**

**cd NTFS\_Pract\_2017**

SIFT has many programs useful for examining ewf files which are a part of the libewf library. In the following steps, use the **ewfinfo** and **ewfverify** commands to complete the table for all four (4) image files downloaded previously.

* ewfinfo – displays metadata stored within an ewf file
* ewfverify – verifies media data stored in ewf files

**ewfinfo NTFS\_Pract\_2017.E0#**

*Note:* the command requires each ewf file to be opened separately. The ‘#’ represents the second digit of the file name.

|  |  |  |
| --- | --- | --- |
|  | **.E01** | **.E02** |
| Case Number | **11-1111-2017** | **11-1111-2017** |
| Examiner Name | **Barry J. Grundy** | **Barry J. Grundy** |
| Evidence Number | **11-1111-2017-001** | **11-1111-2017-001** |
| Evidence Notes | **This image is for artifact recovery.** | **This image is for artifact recovery.** |
| Acquisition Date | **Mon May 1 22:19:14 2017** | **Mon May 1 22:19:14 2017** |
| System Date | **Mon May 1 22:19:14 2017** | **Mon May 1 22:19:14 2017** |
| OS used | **Linux** | **Linux** |
| File Format | **EnCase 6** | **EnCase 6** |
| Compression Method/Level | **Deflate/no compression** | **Deflate/no compression** |
| Hash Type | **MD5** | **MD5** |
| Hash Value | **eb4393cfcc4fca856e0edbf772b2aa7d** | **eb4393cfcc4fca856e0edbf772b2aa7d** |

|  |  |  |
| --- | --- | --- |
|  | **.E03** | **.E04** |
| Case Number | **11-1111-2017** | **11-1111-2017** |
| Examiner Name | **Barry J. Grundy** | **Barry J. Grundy** |
| Evidence Number | **11-1111-2017-001** | **11-1111-2017-001** |
| Evidence Notes | **This image is for artifact recovery.** | **This image is for artifact recovery.** |
| Acquisition Date | **Mon May 1 22:19:14 2017** | **Mon May 1 22:19:14 2017** |
| System Date | **Mon May 1 22:19:14 2017** | **Mon May 1 22:19:14 2017** |
| OS used | **Linux** | **Linux** |
| File Format | **EnCase 6** | **EnCase 6** |
| Compression Method/Level | **Deflate/no compression** | **Deflate/no compression** |
| Hash Type | **MD5** | **MD5** |
| Hash Value | **eb4393cfcc4fca856e0edbf772b2aa7d** | **eb4393cfcc4fca856e0edbf772b2aa7d** |

1. **Why do you think the md5 hashes are the same?** 
   1. **I think that the md5 hashes are the same because they are either the same image or copies of an image. These md5 hashes will have very similar if not the same value but the difference lays in the SHA-1 sum values.**

Use the ewfverify command to see a condensed version of the ewfinfo output.

**ewfverify NTFS\_Pract\_2017.E0#**

## Part 2.1: Working with Autopsy

Open a new terminal window, the issue the follow command to start Autopsy.

**sudo autopsy**

Once Autopsy is running, leave this terminal open. Use Firefox to enter the following URL bar to open the program’s GUI.

**http://localhost:9999/autopsy**



Select the ‘New Case’ button and enter the following details:

* Case Name: **112233-430**
* Description: **Thumb drive seized from suspect**
* Investigator Name: **Your\_NKU\_ID**

After the above is entered, click ‘New Case’ button. On the next screen, select ‘add host’, leave everything else as is and hit the “Add Host” button

Next, select ‘Add Image’, then the ‘Add Image File’ button. On the following the screen, provide the full path to the RHINOUSB.dd file

**/home/sansforesnics/Downloads/SuspectImages/DFRWS2005-RODEO/RHINOUSB.dd**

* Type should be **Disk**
* Import method should be **Symlink**

On the following screen, leave the settings at their default and select ‘ok’.

On the “Image File Details” screen, select the “Calculate” hash value radial, then hit “Add”

1. **Screenshot the MD5 hash calculated by Autopsy and insert it below:**

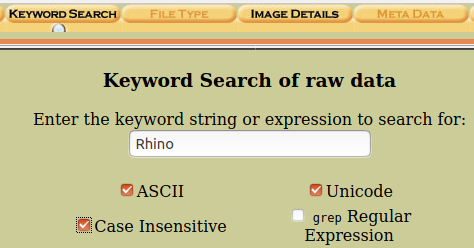
Graphical user interface, text, application

Description automatically generated

Hit Ok, then select ‘Analyze’ to begin the next section.

## Part 2.2: Suspect Image Analysis with Autopsy

Select the ‘Keyword Search’ button, then use the configurations and search term as pictured below.

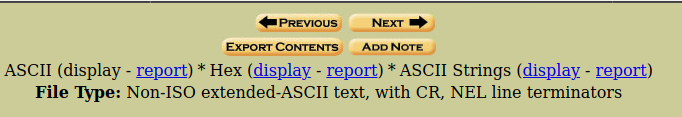


Once everything is entered, select the search button

Explore the output using the links returned on the left side of the screen to answer the following questions:

1. **Where was the string ‘Rhino’ found within the .dd image?** 
   1. **String 335034**
2. **Based on the data returned, briefly describe the activities of the suspect?**
   1. **Are rhino pictures illegal? He simply hid the photos, zapped the hard drive, and threw it in the Mississippi River and is “gonn”.**

Only a portion of the keyword searched for is returned. You can further explore the data within the image by selecting the “Previous” and “Next” arrow buttons in the topmost window pane.



1. **Is there another area (i.e. Unit) with additional information of evidentiary value revealing the suspect’s activities?** 
   1. **Yes, there is multiple different areas and messages revealing information on the suspects activates.**
2. **Create a report of the content from questions 4 and 5, using the ASCII Strings report link. You’ll need to do this for each area determined be of forensic value. Screenshot the header information included in the General Information section of the report below.** 
   1. **Graphical user interface, text, application

      Description automatically generated**
   2. **Graphical user interface, text, application, email

      Description automatically generated**
   3. **Graphical user interface, text, application, email

      Description automatically generated**
      1. **ETC**

Once the questions above have been answered, close the session as follows:

* Close the Keyword Search window:



* Close the Host:



* Close the case, then close Firefox.
* Use ctrl+z to terminate the session in the terminal

## Part 3.1: Viewing and Verifying an image file’s structure

Next, you’ll use several commands to view and verify the structure of a raw image file, as well as, carve out some data.

* mmls = displays the partition layout of a volume system (i.e. partition tables)
* fdisk = used to manipulate disk partition tables
* dd = converts and copy files

From your terminal, use wget to download the able2.tar.gz image file then untar it.

**wget http://linuxleo.com/Files/able2.tar.gz**

**tar xzvf able2.tar.gz**

Both the mmls and fdisk commands are administrative utility programs. Do a little outside research and briefly write how these commands can be used for forensic investigation purposes in the table below.

|  |  |
| --- | --- |
| **mmls** command | **The mmls command parses and displays the media management structures of an image file or disk. This meaning that we can locate and identify parsons of a file helping is identify key characteristics such as OS type and much more.** |
| **fdisk** command | **The fdisk command simply lets you create, delete, and a manage partitions. This can be helpful as a forensics investigator because this command allows you to manipulate partitions.** |

Issue the commands below and answer the following questions. Note: the command options use a lowercase L.

**mmls -l able2.dd**

**fdisk -l able2.dd**

1. **How is the information provided by the commands similar and dissimilar?** 
   1. **This information is similar in that we can identify and see such things as bytes, sectors, Mib, type, etc. What is different about these commands is how information is presented and how much is presented. For example, the fdisk command prints out almost a graph type of view of information instead of entering specific commands with the mmls. We can also see start and end lines while viewing fdisk compared to mmls.**
2. **Which command provides the most forensically useful information?** 
   1. **I would say using fdisk provides the most forensic information that is useful and quick. If you want to know something specific, I would use mmls.**
3. **If the Partition Table in the MBR for the able2.dd image file was examined in a hex viewer, what hex value would be at byte range 4 for each entry?**
   1. **83 which is the Linux OS.**

## Part 3.2: Analyzing Image File Content

In this final section, you’ll use the dd command to carve out one of the partitions within the able2.dd image file. Then you’ll mount this partition to explore its content.

With the information provided in the mmls and fdisk command outputs, the options used in the dd command are known. In other words, you will not need to view the content in a hex viewer and convert offset rows to decimal for determining the starting and size of bytes to be carved. To get started issue the following command:

**dd if=able2.dd of=able2\_carve.dd bs=512 skip=178695 count=496755**

1. **Briefly explain the values used in the bs, skip and count options. Which partition in the able2.dd file is being carved out?** 
   1. **The value used in bs is going to be your set block size, count is going to be what copies a certain number of blocks, and skip is obviously the number of blocks you skip in the input stream to start. The partition in the able2.dd file that is being carved out is the blocks between 178695 through the count which is 496775 which would be 675470 which is an image file.**

This new image file needs to be mounted before we can do any additional analysis. Issue the following commands to create a logical device and add the previously carved data.

**sudo mkdir /mnt/430\_Temp1**

**mount -o loop able2\_part4.dd /mnt/430\_Temp1**

Once the image file is mounted, cd to the 430\_Temp1 directory, then navigate to the directory listed below to answer the remaining questions.

**cd /mnt/430\_Temp1**

**cd doc**

**cd HTML**

Open index.html using cat to review its content.

1. **What message is displayed when a user opens the web browser?**
   1. **Welcome to Red Hat Linux 6.2**
2. **How many image files are contained in the img directory?** 
   1. **7**
3. **What are these image files in reference to? You can use the eog program to view them.**

**eog image\_file\_name**

**These image files are in reference to the images on the red hat Linux website, rather that be the image of the company’s logo and name, signup now, bullet points, grey and white pixel images, etc.**

Unmount your image using the following commands:

**cd ~**

**sudo umount /mnt/430\_Temp1**

## Submission:

Upload a completed copy of this document to Canvas by the due date.