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



Lab 2: Disk and RAM Collection

ITSC 306: Computer Forensics

Table of Contents

[Lab Outcome 2](#_Toc494292512)

[Readings 2](#_Toc494292513)

[Introduction 2](#_Toc494292514)

[1.0 USB Setup 3](#_Toc494292515)

[2.0 Acquiring Ram using DumpIt.exe 4](#_Toc494292516)

[3.0 Acquiring RAM using FTK Imager Lite 7](#_Toc494292517)

[4.0 Acquiring a Disk Image using DCFLDD 10](#_Toc494292518)

[5.0 Mounting a Windows File System with FTK Imager 14](#_Toc494292519)

[References 21](#_Toc494292520)

ITSC 306: Computer Forensics

Lab 2: Disk and RAM Collection

Lab Outcome

* Complete and document the acquisition of RAM and disk images using both Windows and Linux tools.

Readings

* Chapter 3: Forensic Image Formats from your textbook.

Introduction

The best place to discover malware is in RAM. At some point, malware has to run. With the size of RAM steadily increasing, and specialized software to parse through the dump, memory is transforming into a secondary file system.

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

1. USB Setup

To complete this lab, you will acquire and access specific tools through a USB drive. Using a USB drive ensures the response is mobile and the tools are portable.

1. Download the two tools below.

* [FTK Imager Lite version 3.1.1](http://accessdata.com/product-download/ftk-imager-lite-version-3.1.1) (http://accessdata.com/product-download/ftk-imager-lite-version-3.1.1)

FTK Imager and Imager Lite are digital forensic tools used to acquire, authenticate and analyze data. FTK Imager is a product that is primarily accessed from a forensic workstation, while FTK Imager Lite can be used to acquire images in the field for later processing. FTK Imager Lite also has the ability to acquire RAM or acquire specific files and folders without imaging the entire drive.

* [DumpIt](https://my.comae.io/login) (https://my.comae.io/login) Note: You must create an account to access the download file.

DumpIt is a portable executable tool used to acquire or “dump” a system’s RAM. It conveniently combines both win32dd and win64dd into one executable.

1. Configure your USB drive.

Note how much RAM is on the Windows system. The USB can be formatted Fat32; however, remember that up to 4GB of RAM can be acquired using Fat32, so if the suspect machine has RAM greater than 4GB, format the drive NTFS.

1. Plug in your USB drive and ensure it is recognized by Windows in Windows Explorer.
2. Create a folder on the USB named **Tools** with sub-folders named **FTK** and **DumpIt**.
3. Copy the FTK Imager Lite and DumpIt files you downloaded to the corresponding folders.
4. Open a Command Prompt and confirm that you can access the two files, **Tools\FTK\FTK Imager.exe** and **Tools\DumpIt\DumpIt.exe**.

1. Acquiring Ram using DumpIt.exe

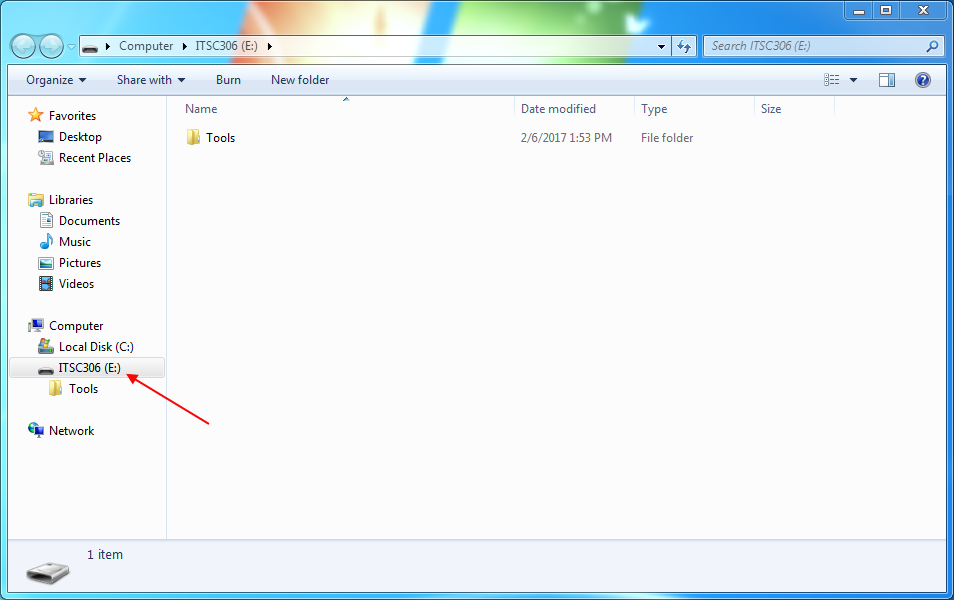
**Example 1: DumpIt.exe**

DumpIt.exe is the easiest tool to use to acquire RAM from a Windows OS. It has no options and it captures RAM from a 32- or 64-bit system. All DumpIt.exe does is to dump the memory of the live system to the same location it is run from, and the memory image will be named according to the system hostname and the current date.

Note: When preparing a USB drive with DumpIt.exe installed, the USB drive must be larger than the amount of RAM you will be obtaining.

1. Plug the prepared USB drive into the Windows system and note the drive letter.

In this example, the drive is **E:**



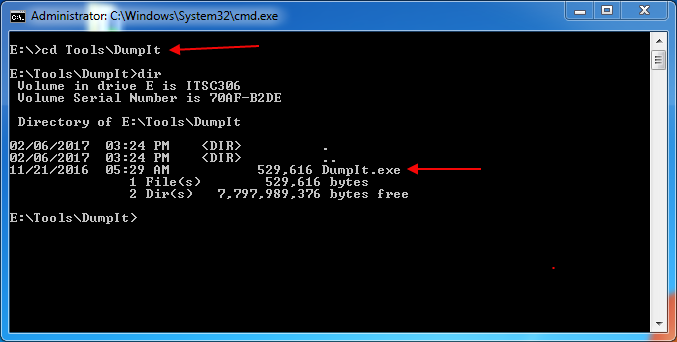
**Figure 1: Drive Letter Identification**

Used with permission from Microsoft.

1. Open a Command Prompt with Administrator privileges and change the drive letter to match that of your USB drive. In this case, the drive letter is **E:** and the executable is in the **Tools\DumpIt** folder. Type the following commands into the Command Prompt:

[E:]

[cd Tools\DumpIt]

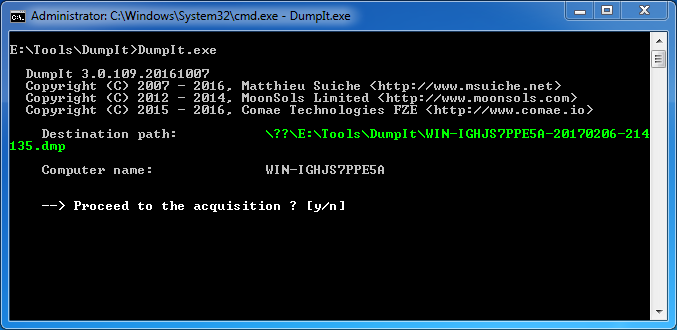


**Figure 2: Command Prompt**

Used with permission from Microsoft.

1. Run the command.
2. Once in the **DumpIt** directory, run the following command:

[DumpIt.exe]

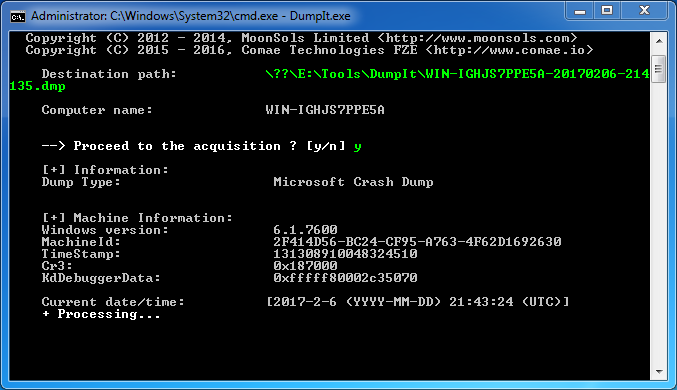


**Figure 3: Destination Path**

Used with permission from Microsoft.

The program reports the Destination Path and provides a file name for the RAM capture.

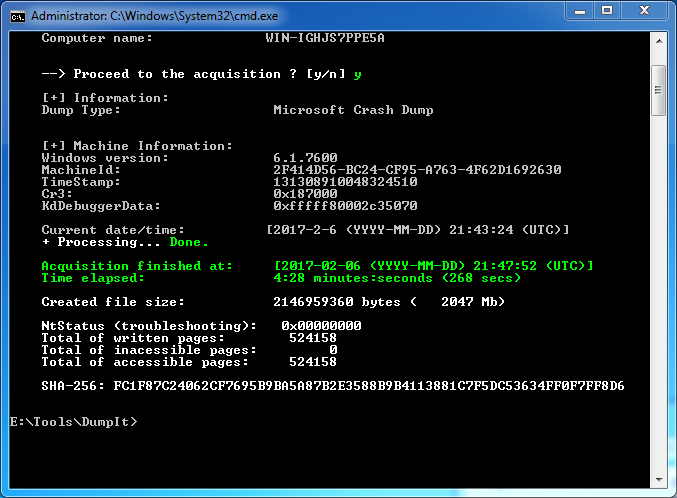
1. When prompted with: Proceed to the acquisition ? [y/n], type **Y** to run the program.



**Figure 4: Run the Program**

Used with permission from Microsoft.

Once completed, the program reports that the processing is done. It reports the date and time of completion and the amount of time taken to complete the acquisition. The program will also report the size of the file that was created and will provide a SHA-256 hash value of the acquisition.



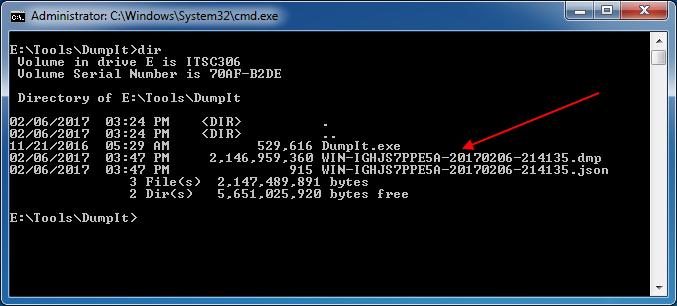
**Figure 5: Completed Process**

Used with permission from Microsoft.

1. To confirm the file was created, run a dir command from the **Tools\DumpIt** directory.

E:\Tools\DumpIt

dir



**Figure 6: Dir Command**

Used with permission from Microsoft.

3.0 Acquiring RAM using FTK Imager Lite

FTK Imager and ImagerLite from AccessData are free Windows acquisition tools. Imager is a tool that would be installed on your forensic workstation. Imager Lite is portable and can be placed on a USB drive. This portability allows you to capture memory or data from a live system, as well as imaging systems.

Note: When preparing a USB drive with FTK Imager Lite installed, the USB drive must be larger than the amount of RAM you will be obtaining.

1. Plug the prepared USB drive into the Windows system and note the drive letter.
2. If autorun is enabled on the Windows system, open the Window, navigate to **Tools\FTK** and double-click **FTK Imager.exe** to run the program. Otherwise, open a Command Prompt with Administrator privileges and change the drive letter to that of your USB drive (in this case, **E:**). The executable is in the **Tools\FTK** folder. Run the following commands from the Command Prompt:

E:

cd Tools\FTK\FTK Imager.exe

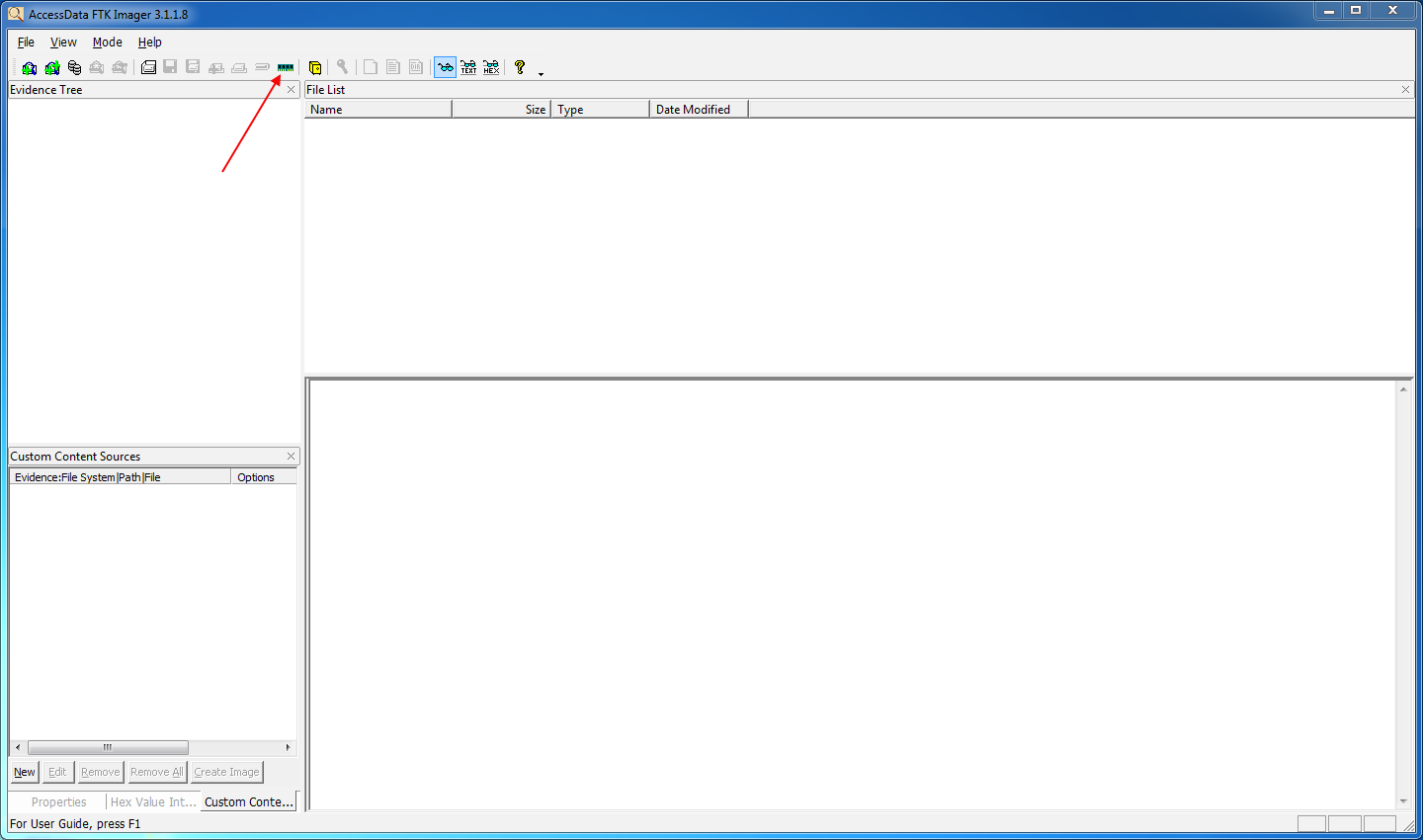


**Figure 7: Tools/FTK**

Used with permission from Microsoft.

The program opens.

1. Select the green “chip” icon from the toolbar, or select **File > Capture Memory**.

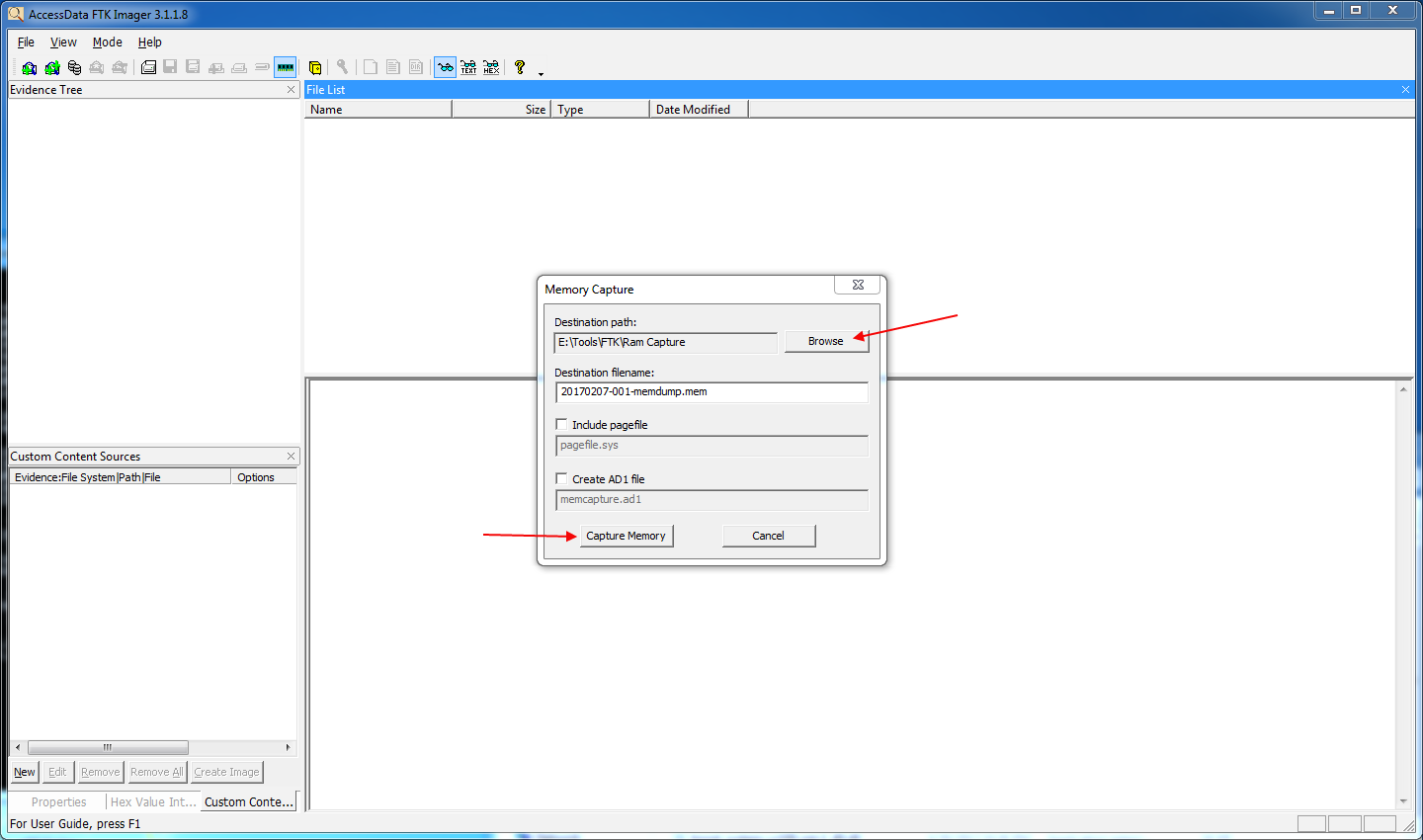


**Figure 8: Capture Memory**

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.

The *Memory Capture* window opens.

1. Browse to a path on your USB drive, and name the destination filename as: date – reference number – description. The default extension is **.mem**.
2. Do not select either the **Include pagefile** or **Create AD 1 file** check boxes.. The AD1 file is an AccessData file type.

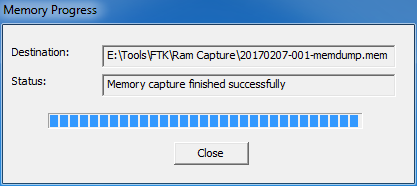


**Figure 9: Memory Capture Window**

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. Select **Capture Memory**.

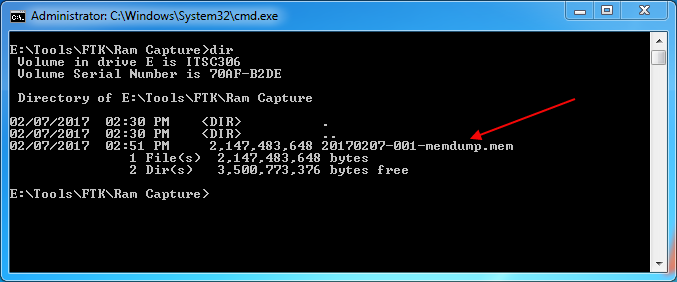
Imager starts and a *Memory Progress* window appears. Once the memory has been acquired, the status changes to *Memory capture finished successfully*.



**Figure 10: Memory Progress Window**

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. Confirm that the file was created.



**Figure 11: File Confirmation**

Used with permission from Microsoft.

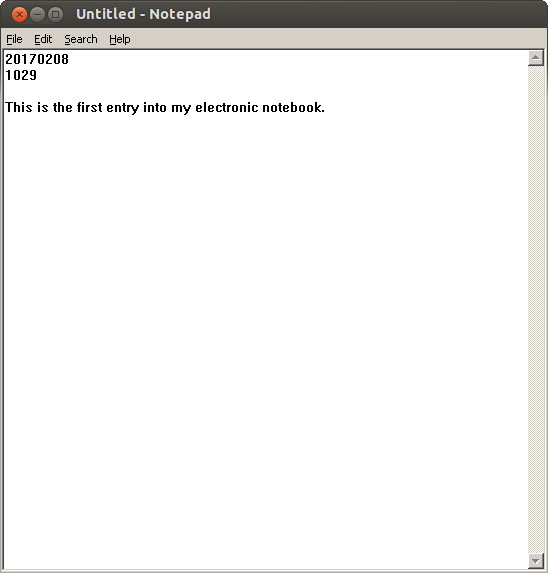
4.0 Acquiring a Disk Image using DCFLDD

In this example, we will use Linux and the SIFT workstation to acquire media. The SIFT workstation includes DCFLDD by default.

**Example 1**

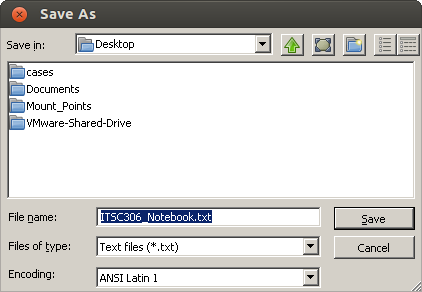
In this example, copy files using DCFLDD to illustrate that a bit-for-bit image is acquired using DCFLDD.

1. From your SIFT workstation, open Notepad.
2. Create a text document (Figure 12) and save it with a unique file name to your Desktop (Figure 13).



**Figure 12: Notepad Screen**

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 13: Save As Window**

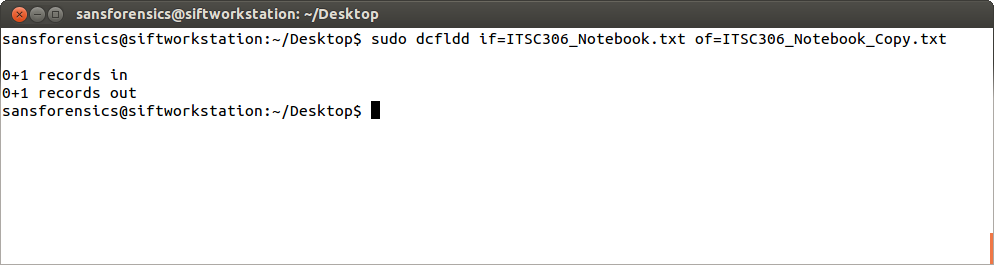
Source: SANS Institute. Reproduced and used in accordance with the fair dealing provisions in section 29 of the Canadian Copyright Act for the purposes of education, research or private study. Further distribution may infringe copyright.

1. Open a Terminal and navigate to your Desktop. Create an exact copy of the text document using DCFLDD by running the following command.

sudo dcfldd if=(Filename.txt) of=(Filename\_Copy.txt)

In this example, the command would be:

sudo dcfldd if=ITSC306\_Notebook.txt of= ITSC306\_Notebook\_Copy.txt



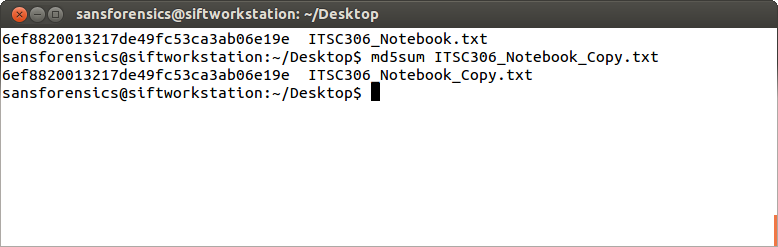
**Figure 14: Copy Text**

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. To authenticate, open and view each document. They should be the same.
2. Use md5sum to create a hash value of each document. The hash values should match.

md5sum ITSC306\_Notebook.txt

md5sum ITSC306\_Notebook\_Copy.txt



**Figure 15: Hash Value Creation**

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.

**Example 2**

Use DCFLDD to image a USB drive.

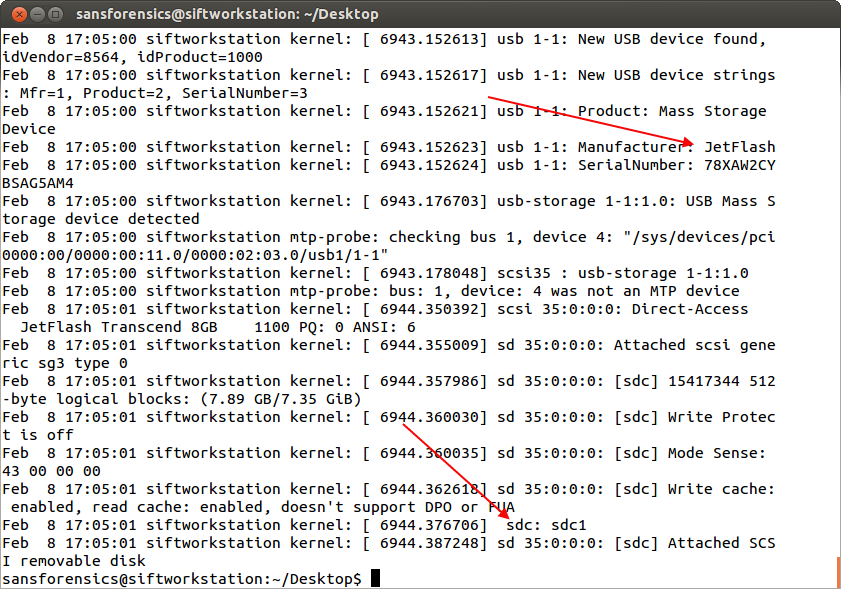
1. In your SIFT workstation, open notepad and document your actions associated to the following exercise. From a Terminal, run the following command:

tail –f /var/log/syslog

The /var/og/syslog contains system log information. By running tail you can watch the log file being written to in real time. By using the -f switch, you are identifying the file to follow.

1. Insert your USB drive into the system.

**Note:** The syslog identifies the USB drive and providse a mount point. In this example, the USB has been identified as a JetFlash and a serial number has been provided. You can mount the drive at **/dev/sdc1** to view the data, and image the physical device at **/dev/sdc**.



**Figure 16:Log File Creation**

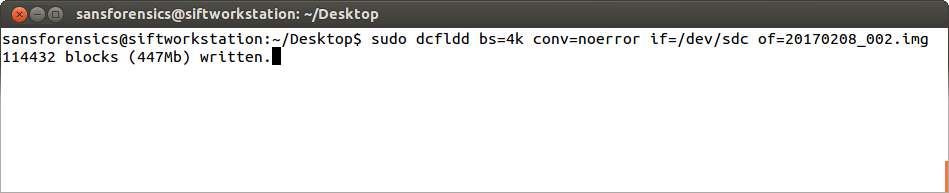
Source: SANS Institute. Reproduced and used in accordance with the fair dealing provisions in section 29 of the Canadian Copyright Act for the purposes of education, research or private study. Further distribution may infringe copyright.

1. Type CTRL+C to stop the current process.
2. Type the following command to image the USB drive to your Desktop.

sudo dcfldd bs=4k conv=noerror if=/dev/sdc of=(Filename).img

The default block size is 512 bytes. Using the default block size is slow, so unless the drive has numerous errors, increase the block size to speed up the imaging. The option conv=noerror ensures that the imaging continues after any read errors. The default is to stop.

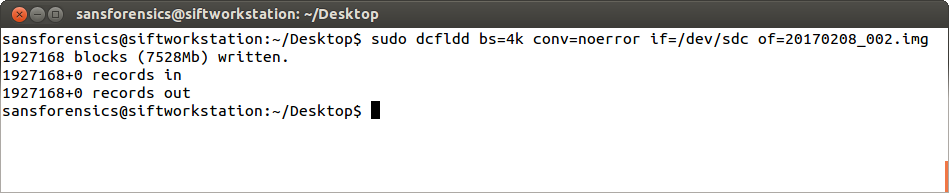
sudo dcfldd bs=4k conv=noerror if=/dev/sdc of=20170208\_002.img



**Figure 17:Block Size**

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 process completes. An image file is created on the Desktop.



**Figure 18:Created 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. Save your notes.

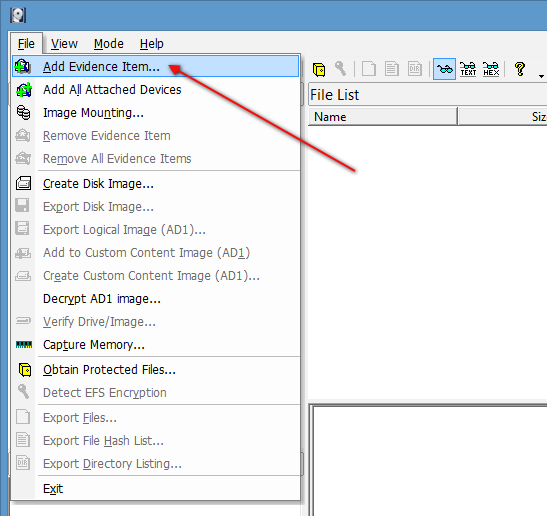
5.0 Mounting a Windows File System with FTK Imager

This section illustrates how to mount a Windows file system, how to export files and how to create a hash list of files on the system so that you understand how to use FTK Imager.

1. Create a folder called **Suspect** on your Windows Desktop.
2. Add several files to the folder.
3. Run **FTK Imager.exe** from your USB drive.

FTK Imager opens.

1. Select **File > Add Evidence Item**.

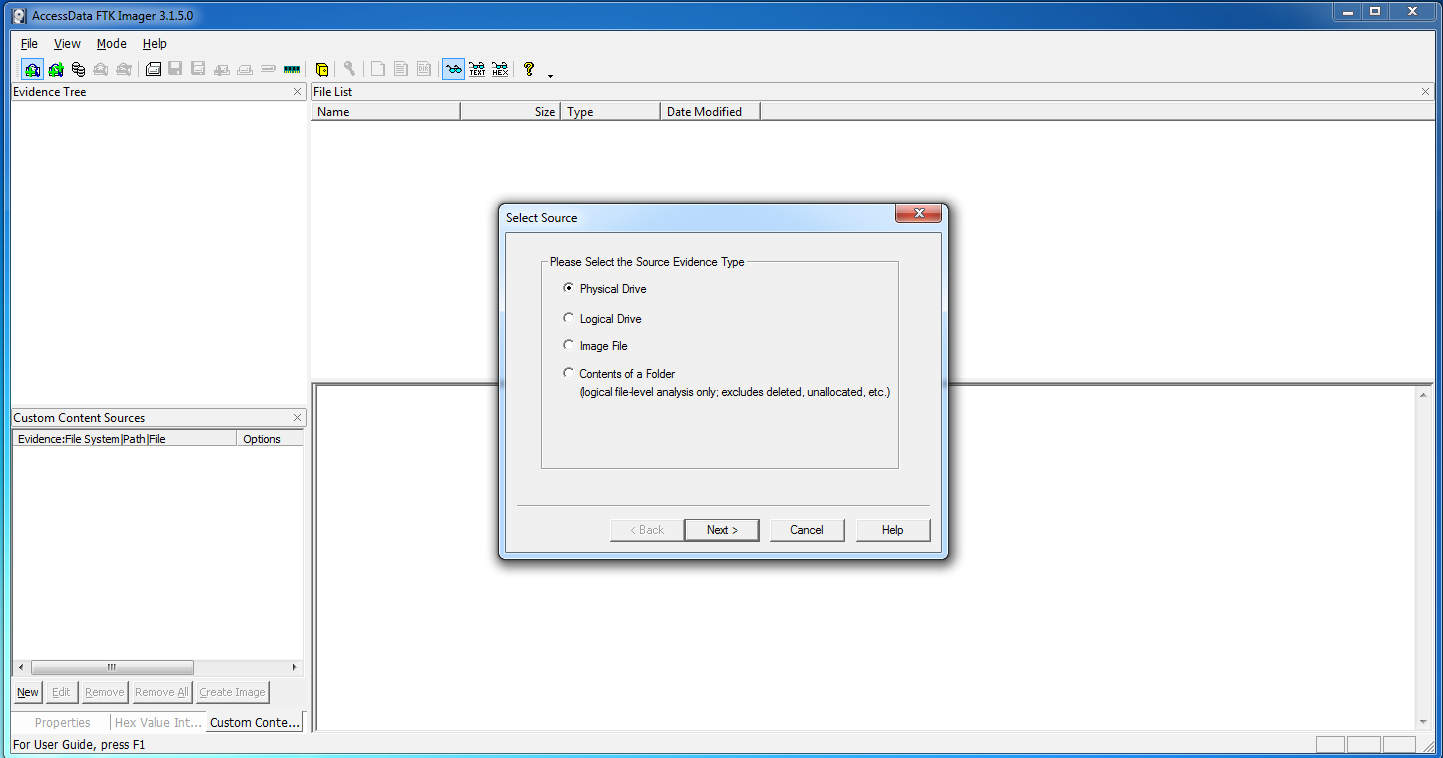


**Figure 19: Add Evidence Item**

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.

The *Select Source* window appears.

1. Select the **Physcial Drive** radio button and then click **Next**.

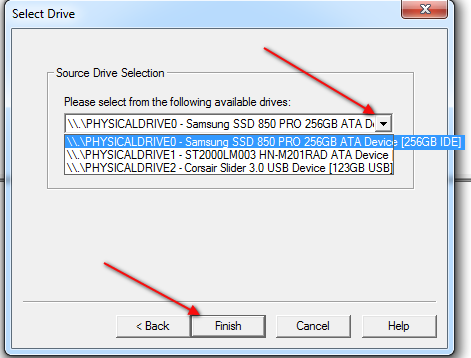


**Figure 20: Physical Drive Buttons**

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.

The *Select Drive* window appears.

1. Click the drop-down arrow, select the OS drive and then click **Finish**.



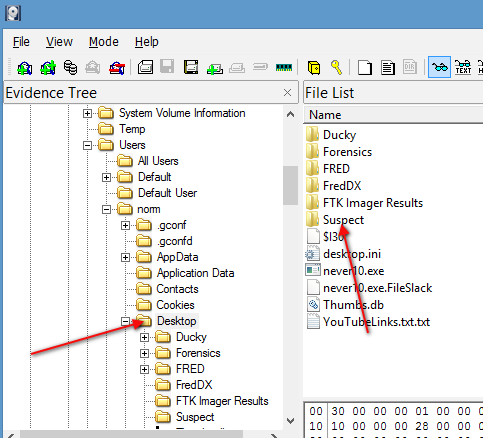
**Figure 21: Select Drive Window**

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.

FTK Imager adds the device to the Evidence Tree.

1. Navigate the partitions and locate the **root** folder, and then expand the root folder and locate the **Desktop** folder for your user account (**root\Users\(user\_account)\Desktop**).
2. Click the **Desktop** folder to list the contents in the *File List* window.

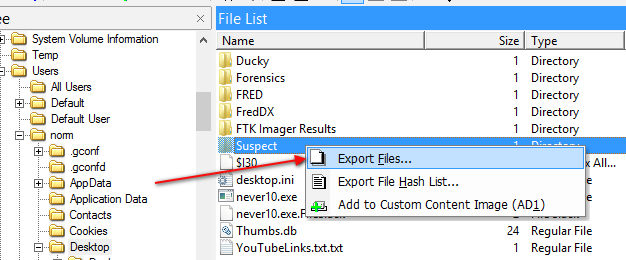
A folder named **Suspect** appears in the File List.



**Figure 22: File List Window**

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.

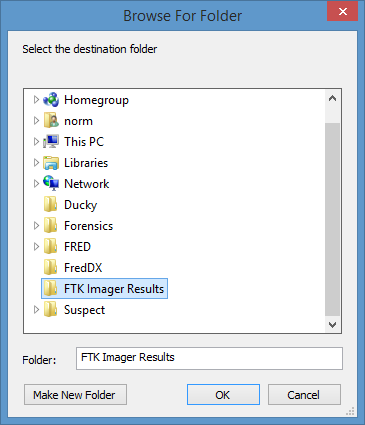
1. Right-click the **Suspect** folder in the *File List* window and select **Export Files**.



**Figure 23: Export Files**

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.

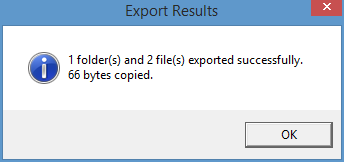
1. In the *Browse for Folder* window, create an **FTK Imager Results** folder and select **OK**.



**Figure 24: Browse Window**

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.

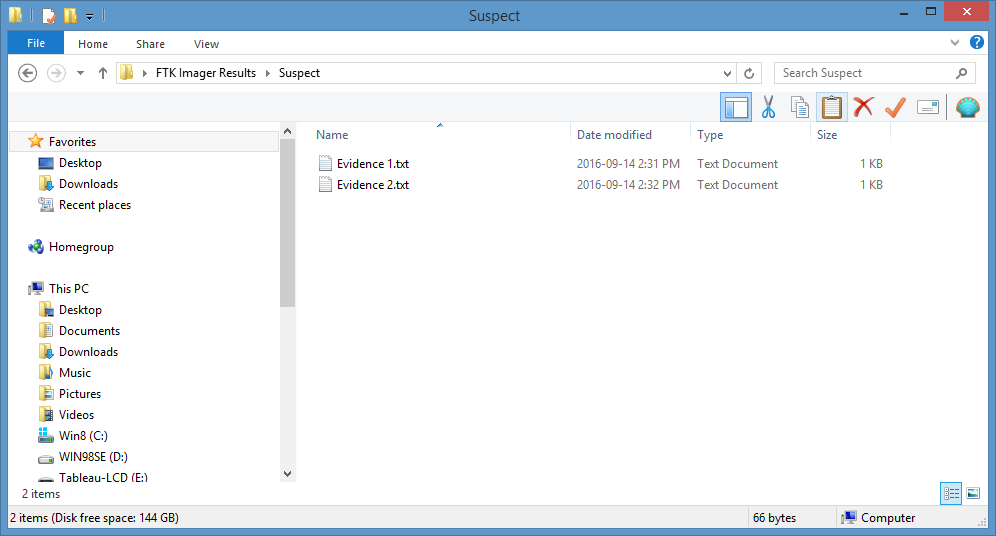
The process starts. When complete, an *Export Results* confirmation window appears advising what was exported and the total size.



**Figure 25: Export Results Window**

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. Open the **FTK Imager Results** folder to confirm that the process was successful.

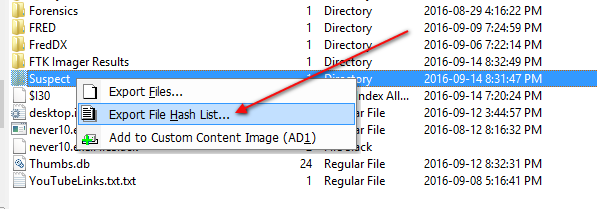


**Figure 26: FTK Image**

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.

This process can also be used to create hash values of files within a folder.

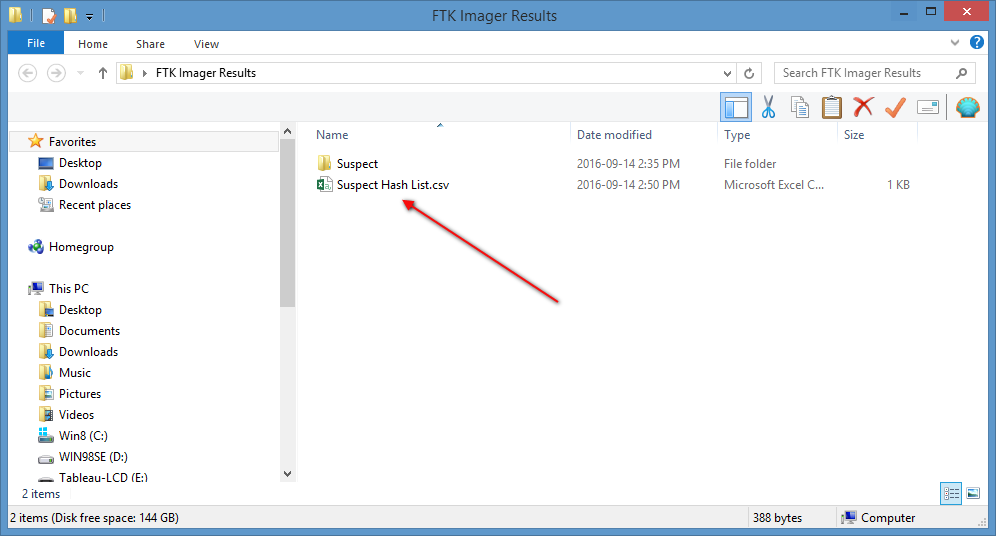
1. Repeat Step 9 above, but instead of selecting **Export Files**, select **Export File Hash List** instead.



**Figure 27: Export File**

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.

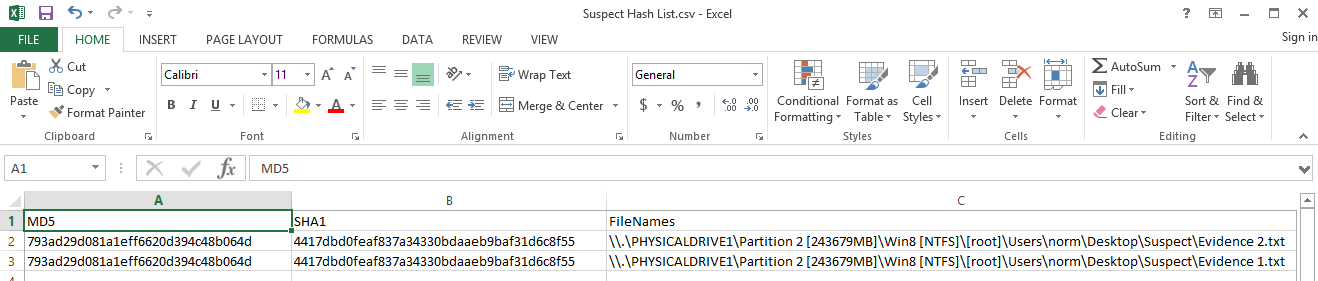
1. Save the results to your **FTK Imager Results** folder and name the file **Suspect Hash List**.
2. Imager defaults the results as a .csv file.



**Figure 28: Saving Image**

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. Open the .csv file to view the results. FTK provides the MD5 Hash, the SHA1 Hash and the Path to the file.



**Figure 29: Open .csv File**

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.

References

AccessData (2017). FTK Imager Lite (version 3.1.1) [Computer software]. Retrieved from http://www.accessdata.com/product-download

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