**Chapter 1**

**Creating a Forensics Image**

**V1**

**A blue outline of a bird with a crown and text

Description automatically generatedSID: 2103022**

**Anglia Ruskin Final Project**

**Table of Contents**

[**Introduction** 2](#_Toc159598849)

[**Objective** 2](#_Toc159598850)

[**1.0** **FTK Imager** 3](#_Toc159598851)

[**2.0** **Create a Forensic image.** 4](#_Toc159598852)

[**3.0**  **Logical Drives** 7](#_Toc159598853)

[**4.0** **Verify the image.** 8](#_Toc159598854)

# **Introduction**

This first chapter covers the imaging portion of the process within digital forensics. The aim is the educate a user how to create a court-admissible forensic image using free digital forensic tools.

# **Objective**

* Use FTK Imager.
* Create a forensic image in Windows 10.
* Verify image to ensure integrity.

1. **FTK Imager**

1.Login as Digital-Forensics and use the password **‘password’** to login to the VM.

A login screen with a beach and rocks

Description automatically generated

2. Launch FTK imager found in the tools folder on the Desktop. **Desktop>Tools> FTK imager**.

A screenshot of a computer

Description automatically generated

3. Four windows appear within the application as seen and explored in the figure and table below.

A screenshot of a computer

Description automatically generated

|  |  |  |
| --- | --- | --- |
| **Box** | **Name** | **Description** |
| Top Left | Evidence Tree | Shows tree of evidence |
| Top Right | File List | Lists all files from path selected |
| Bottom Left | Custom Current Source | Allow for addition, editing or removal. |
| Bottom Right | View Pane | Displays content from file list |

1. **Create a Forensic image.**

1.To start creating your forensic image go to File>Create>Disk image.

A screenshot of a computer

Description automatically generated

2. To create the disk image select physical drive then select next

A screenshot of a computer

Description automatically generated

3. All available drives will be listed select ‘PHYSICALDRIVE1’ it should be 104MB large.

A screenshot of a computer

Description automatically generated

4. You will now have multiple options:

|  |  |
| --- | --- |
| **Option** | **Description** |
| Add | Follow step 5 to find more |
| Add Overflow location | Allows you to combine multiple disks to store an image larger than 1 disk available space. |
| Verify Image after they are created | Compares hashes before and after creating the image to ensure no changes have been made. |
| Precalculate Progress Statistics | Checks the estimate time and storage of the creates image before committing. |
| Create directory listings | Allows you to output the image to a file with a tree-style list of folders within it. |

5. Click Add and you will have 4 options, select E01 and then click next.

A screenshot of a computer

Description automatically generated

Below explores the 2 relevant formats.

|  |  |
| --- | --- |
| **Option** | **Description** |
| Raw(dd) | Full image dump, no compression, and no metadata. |
| E01 | Common forensic format, compression and segmentation are possible, stores metadata for verification of image. |

6. Copy the following image and inserting your name where appropriate then click next.

A screenshot of a computer

Description automatically generated

7. Browse for the ‘EVIDENCE’ folder and click OK, insert a name for the file such as the one below and click finish.

A screenshot of a computer program

Description automatically generated

8. Click start.

A screenshot of a computer error

Description automatically generated

9. Wait for the image to complete and the verify result pop up will appear, like below. If the hashes are the same and no bad blocks have been found, for this chapter the creation is complete, but this is now where you can close the pop up and continue the investigation.

# **3.0 Logical Drives**

You can also create logical drive images such as for USB drives.

Instead of selecting Physical you select logical as seen below.

A screenshot of a computer

Description automatically generated

Then select the Drive you want to image in this case the USB Drive.

A screenshot of a computer

Description automatically generated

Now return to step 4 and rename where necessary.

1. **Verify the image.**

1.If we find the text file created with the image, we can see all the metadata associated with it.

A white background with black and white text

Description automatically generated

2. First we see the information we filled in about the image in section 1.6.

A white screen with black text

Description automatically generated

3. At the bottom of the file we can see the image start and finish time along with the verification start and finish date and time as well.

A screenshot of a computer

Description automatically generated

4. Another way to test is to open the file in FTK imager. Reopen FTK and got to File>Add Evidence Item...

A close-up of a computer screen

Description automatically generated

5. Select image file and click next.

A screenshot of a computer

Description automatically generated

6. Click browse find the E01 File in the evidence folder on the desktop and open the file, then click finish.

A screenshot of a computer

Description automatically generated

7. You can now expand the Evidence Tree to see all folders on the image.

A screenshot of a computer

Description automatically generated

|  |  |
| --- | --- |
| **Folder** | **Description** |
| Orphan | Contains deleted orphaned files |
| Root | Main directory |
| Unallocated space | Unallocated spaced represented as files. |

8. Being able to access root means that the image was successfully.

9. The chapter is complete you can now create a forensics image and verify its validity. You can close all applications and return to the desktop for Chapter 2 or shutdown if you wish to continue later.