**Chapter 6**

**File and Hash Analysis**

**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](#_Toc160195769)

[**Objective** 2](#_Toc160195770)

[**1.0** **File Hash Export** 3](#_Toc160195771)

[**2.0 Creating and using a Hash Set** 6](#_Toc160195772)

# **Introduction**

The sixth chapter covers file and hash analysis allowing an investigator to verify and validate digital data. This chapter aims to teach the reader how to firstly export file hash using FTK Imager and then create and use a hash set using Autopsy.

# **Objective**

* Export file has using FTK Imager
* Create and use a Hash Set using Autopsy.

1. **File Hash Export**

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 Magnet Process Capture found in the tools folder on the **Desktop. Desktop>Tools> FTK Imager**

A screenshot of a computer

Description automatically generated

3. Go **File>Add Evidence Item…**

A screenshot of a computer

Description automatically generated

4. Tick ‘Contents of a folder’ and click ‘Next’.

A screenshot of a computer

Description automatically generated

5. Click browse and locate the ‘FAKE DOCS’ folder from ‘**Desktop>Evidence>FAKE DOCS**’ then click ‘OK’ then ‘Finish’

A screenshot of a computer

Description automatically generated

6. Cick the plus symbol next to ‘FAKE DOCS’ and click ‘C:\Users\Digital…’ then you should see 5 images.



7. Click on the images to reveal what they are like the figure below

A close up of a passport

Description automatically generated

8. Right click on ‘C:\Users\Digital…’ then click ‘Export File Hash List…’.

A screenshot of a computer

Description automatically generated

9. Save the file as ‘CHAPTER 7 HASH LIST’ in the **‘Desktop>EVIDENCE>FILE HASH LIST’** folder

A white rectangular object with black lines

Description automatically generated

10. Locate the file you just saved and double click to open it.

A screenshot of a computer

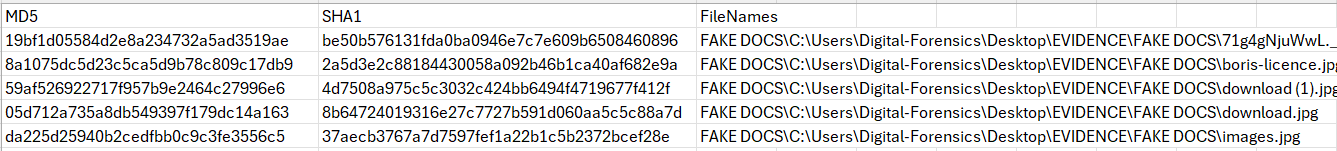
Description automatically generated

11. Click ‘OK’.

A screenshot of a computer

Description automatically generated

12. You can now see the MD5 and SHA1 hash with the file location and name.



# **2.0 Creating and using a Hash Set**

1. Launch Magnet Process Capture found in the tools folder on the ‘**Desktop. Desktop>Tools> Autopsy’.**

A screenshot of a computer

Description automatically generated

2. Once loaded click ‘New Case’.

A screenshot of a computer

Description automatically generated

3. Name the Case name ‘Chapter 7’ and click browse to locate the Evidence folder on the Desktop then click next.

A screenshot of a computer

Description automatically generated

4. Fill in the boxes like the figure below and click ‘Finish’.

A screenshot of a computer

Description automatically generated

5. Wait for the loading bar to complete then click ‘Next’.

A screenshot of a computer

Description automatically generated

6. Select ‘Logical Files’ and then click ‘Next’

A screenshot of a computer

Description automatically generated

7. Click browse and locate the ‘HDD.E01’ file in the Evidence folder on the Desktop then click ‘Neext’.A screenshot of a computer

Description automatically generated

8. Click Deselect all then tick ‘Hash Lookup’ like the figure below.

A screenshot of a computer

Description automatically generated

9.Click ‘Global Settings’.

A white background with black text

Description automatically generated

10. Click ‘New Hash Set’.



11. Name it ‘Chapter 7 Hash’ and save the file path in the Evidence folder on the desktop.

A screenshot of a computer

Description automatically generated

12. Click ‘Add Hashes to Hash Set’.

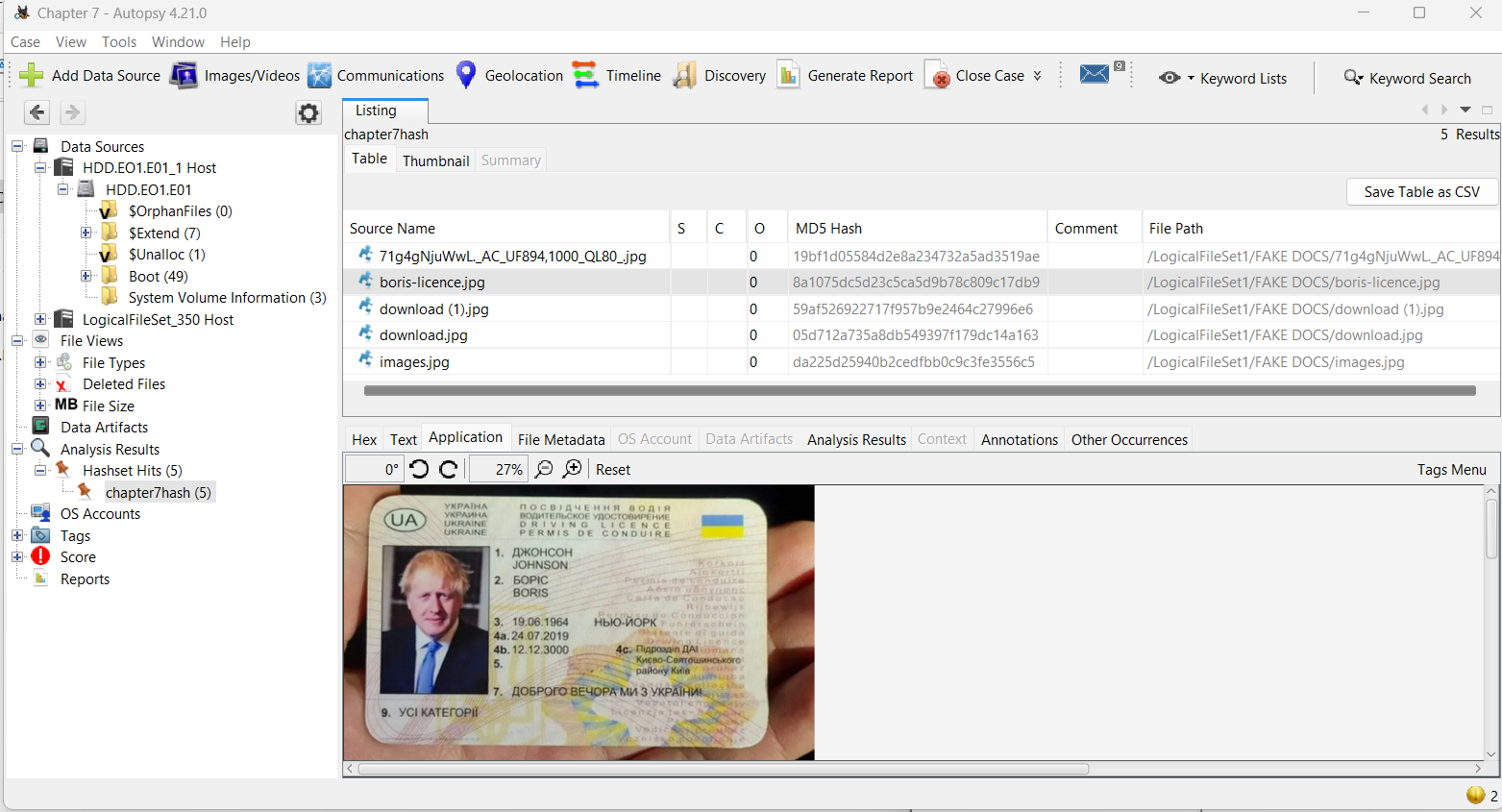


13. Copy the MD5 hash from the OpenOffice Calc document we created earlier then click ‘OK’ and ‘Next’ then ‘Finish’.

A screenshot of a computer

Description automatically generated

14. Open the Chapter7 Hash section and compare the images with the hashes from before.



15. The chapter is complete, and you can now export a file hash list using FTK Imager as well as creating and using a hash set. You can close all applications and return to the desktop for Chapter 7 or shutdown if you wish to continue later.