Computer Forensics: Blue Coursework

Student:
Alessandro Buonerba

Module Leader:
Dr David Gresty

Computer Science (Cybersecurity)
Computer Forensics
COMP-1812

Department of Computing & Mathematical Sciences
Liberal Arts & Sciences

University of Greenwich
London, United Kingdom

December 2021

CONTENTS

LIST OF FIGURES

1 TASK 1: IMAGING EXERCISE

1.1 PART A

The file `ImageFile7.001` will be the subject of the following report as specified in the task document. All the steps shown in this report are to guarantee that veracious and accurate procedures are followed to safeguard the preservation of the evidence and are suitable to be served in court. To establish evidence, stages are documented and explained.

1.1.1 *Correct Image*

As a demonstration that the image file is the correct one, verification has been carried out. The following dialog represents the MD5 Hash that confirms it is an exact copy of the original file.

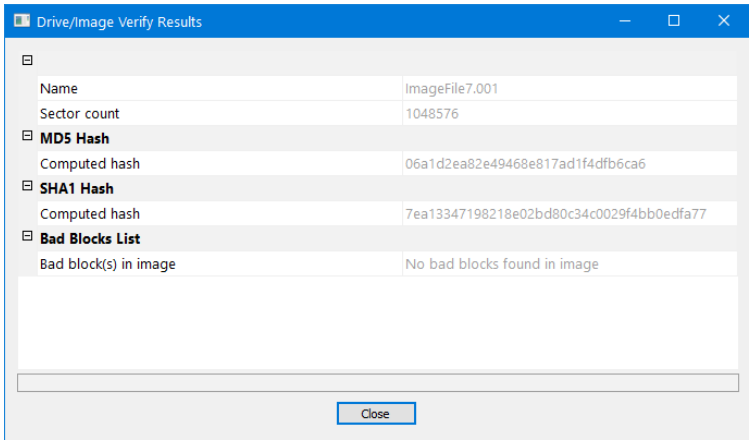

Figure 1.1: Image Hash

1.1.2 *EWF/E01 Image Files*

For this tasks, two different methods and images are being created. To create the images, the dialog to create images has been opened on `FTK Imager`.

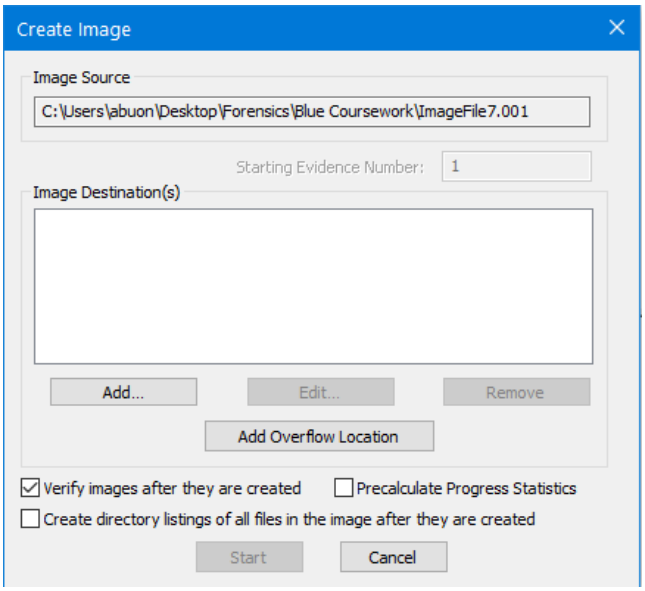

Figure 1.2: Create Images on FTK Imager

Clicking on `Add` will open another dialog that asks for evidence information.

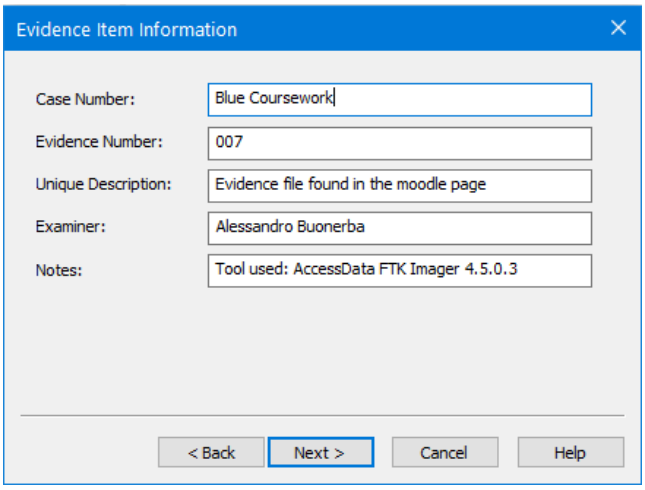

Figure 1.3: Evidence Information

The next step is used to selected the image destination, the filename and various options such as fragmentation and compression.

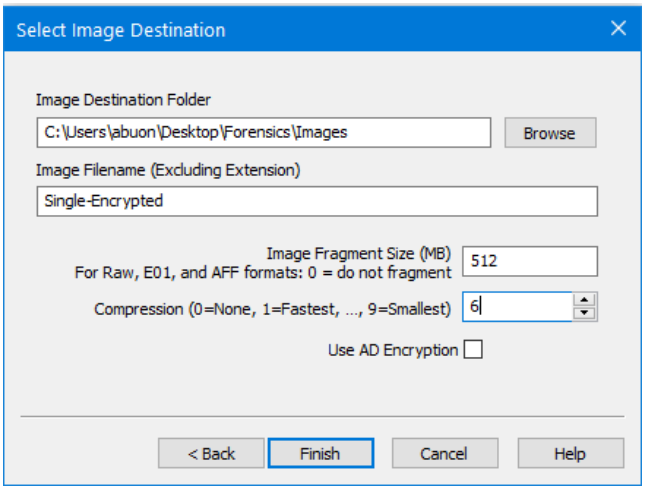

Figure 1.4: Single Encrypted Image

The figure above represents the first requirements that asks to create a single E01 image file with enabled compression that in this case is set on 6, while the figure below represents the splitted version without compression.

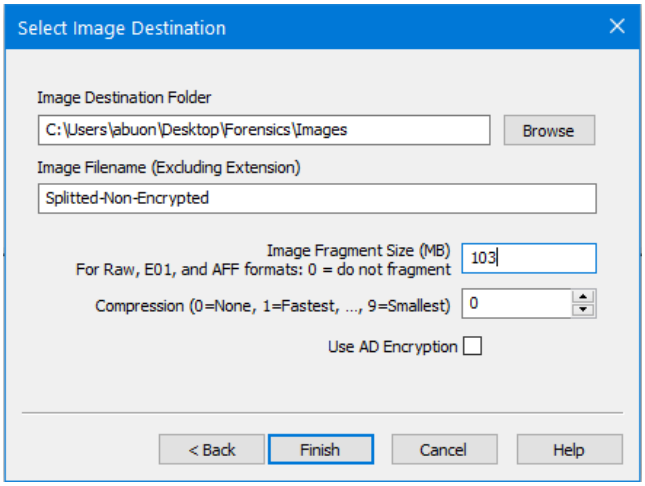

Figure 1.5: Fragmented Image without Compression

Since the image to be split is 512mb and the new E01 must be split in 5 files, the image fragment size has been set dividing the two numbers, resulting in 103mb. After closing the dialog, the previous create image dialog is shown again with the image destinations and configurations that has been set previously for the two tasks.

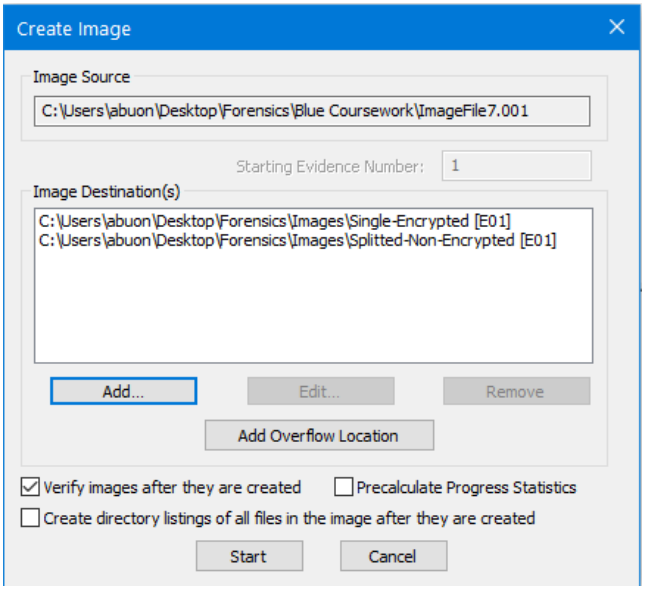

Figure 1.6: Create Image Dialog with Images

Clicking on start will initialise the creation of both and at the end of the process a verify result dialog will pop up with informations on both image output and their hashes.

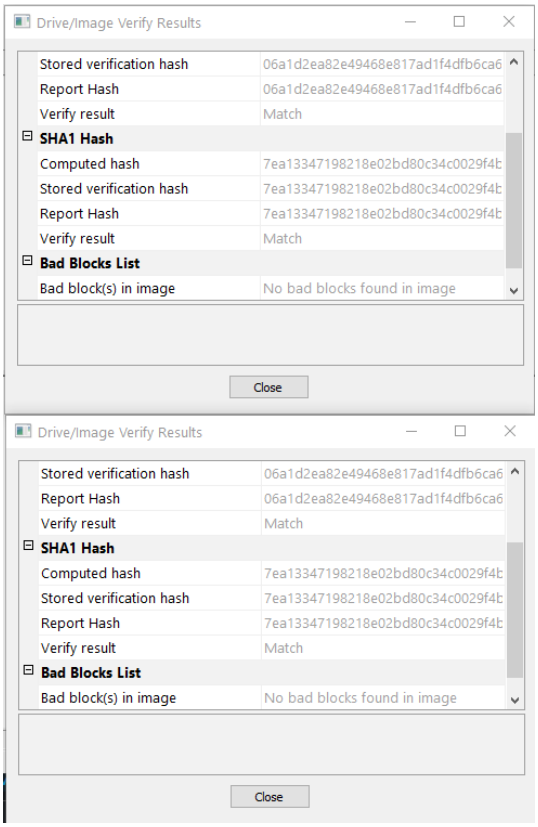

Figure 1.7: Verify Result Dialog

The following image captures the structure of the output files we previously created. It confirms that the splitted files are indeed 5.

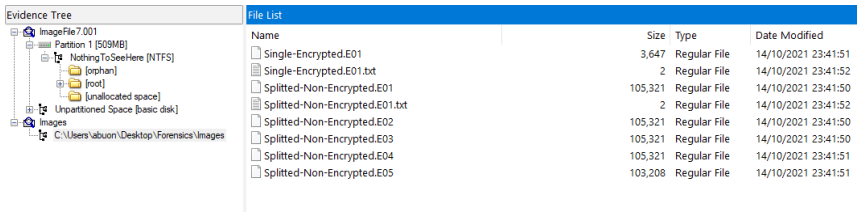

Figure 1.8: File Structures

1.2 PART B

Previously, `FTK Imager` has been used to accomplish the tasks, and the previously screenshots to document the hashes of the images created. To perform Dual Tool Verification, `Autopsy` is also used on this task to double-check the image hashes. The following screenshots confirm that the hashes are the same, meaning that nothing has been tempered.

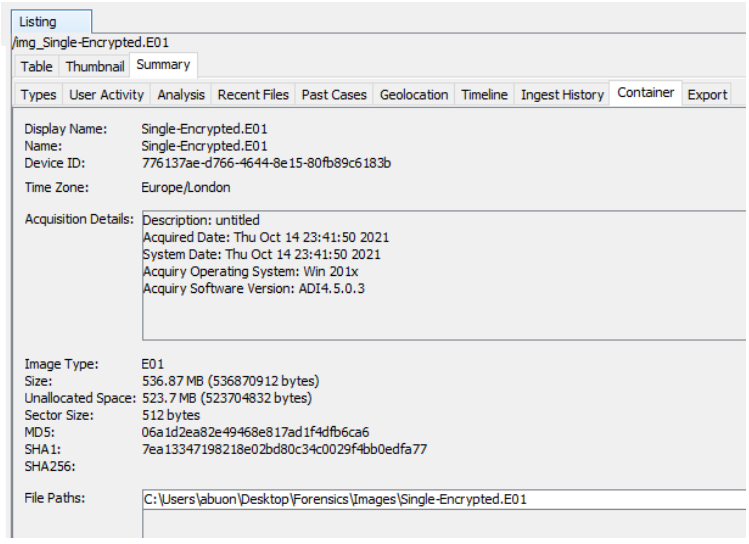

Figure 1.9: Autopsy Dual Tool Verification

1.3 PART C

The following would be a description suitable for the members of a jury without technical knowledge.

1.3.1 *Write blocker*

A `Write blocker` is a small portable device used by investigators to examine USBs or other removable media without tempering the evidences that are being examined, preserving authenticity.

2

TASK 2: SEARCH AND SEIZURE

Task 2 Forensics

3

TASK 3: WRITTEN EVIDENCE

Task 3 Forensics

WITNESS STATEMENT

CJ Act 1967, s.9; MC Act 1980, ss.5A(3) (a) and 5B; Criminal Procedure Rules 2020, Rule 16.2

URN | | | | |

Statement of: Firstname SURNAME B.Sc(Hons) MBCS

Age if under 18: Over 18 (if over 18 insert 'over 18') Occupation: Digital Forensics Specialist

This statement (consisting of XXX pages each signed by me) is true to the best of my knowledge and belief and I make it knowing that, if it is tendered in evidence, I shall be liable to prosecution if I have wilfully stated in it, anything which I know to be false, or do not believe to be true.

Signature: **Type Yourname** Date: XXX

Tick if witness evidence is visually recorded ☐ *(supply witness details on rear)*

Qualifications and Experience

1. I am employed as a Digital Forensics Specialist at Greenwich Police High Tech Forensics Unit. I have worked in the field of Computer Forensics since XXX. I have Bachelor of Science degree in XXX from the University of Greenwich. I have undertaken specialist training in Digital Forensics as part of my degree from the University of Greenwich.

2. I have performed various examinations for both law enforcement and commercial organisations. I have previously given evidence in Court as an expert witness in relation to forensic computing cases.

Background

3. This witness statement refers to actions I have undertaken during the examination of a forensic image supplied to me at the Greenwich Police High Tech Forensics Unit in the case referred to as Operation Blue 3.

4

CONCLUSION

This is the conclusion.