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.

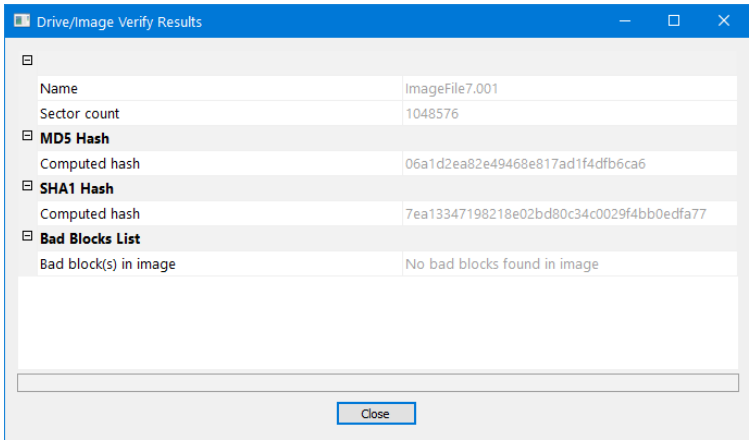

Figure 1.1: Image Hash

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`.

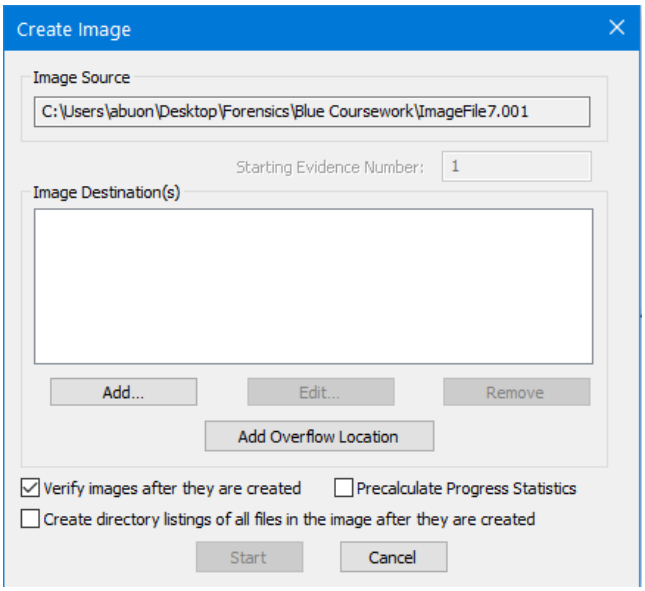

Figure 1.2: Create Images on FTK Imager

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

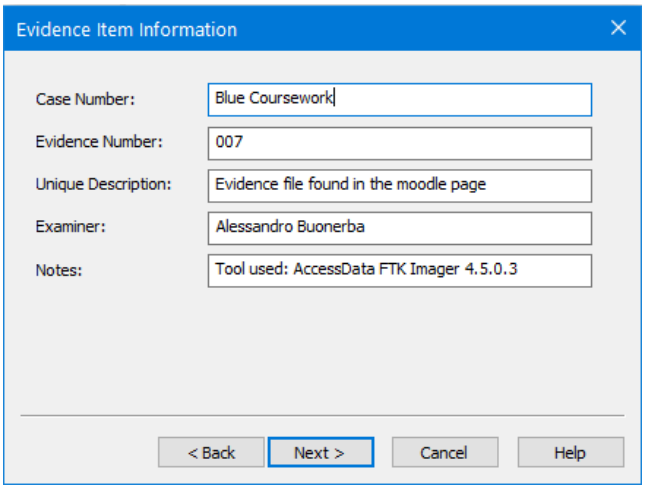

Figure 1.3: Evidence Information

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

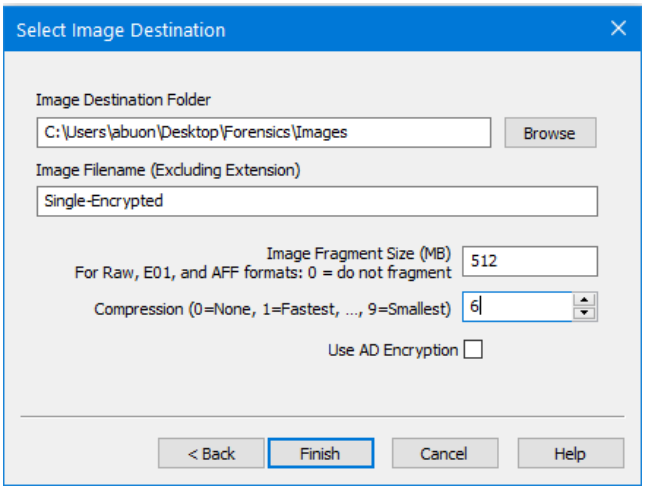

Figure 1.4: Single Encrypted Image

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.

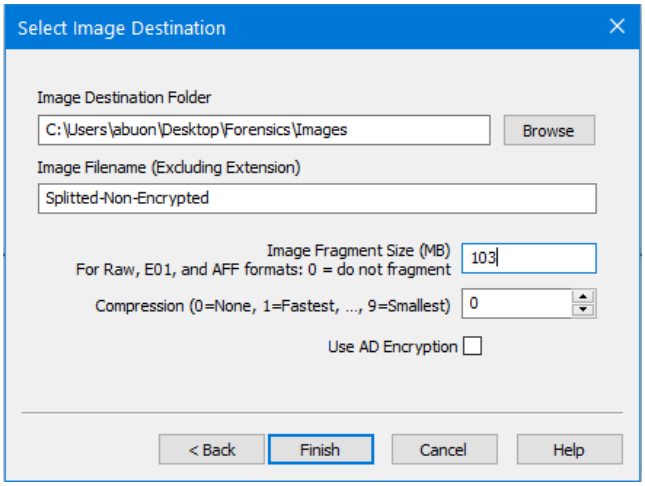

Figure 1.5: Fragmented Image without Compression

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.

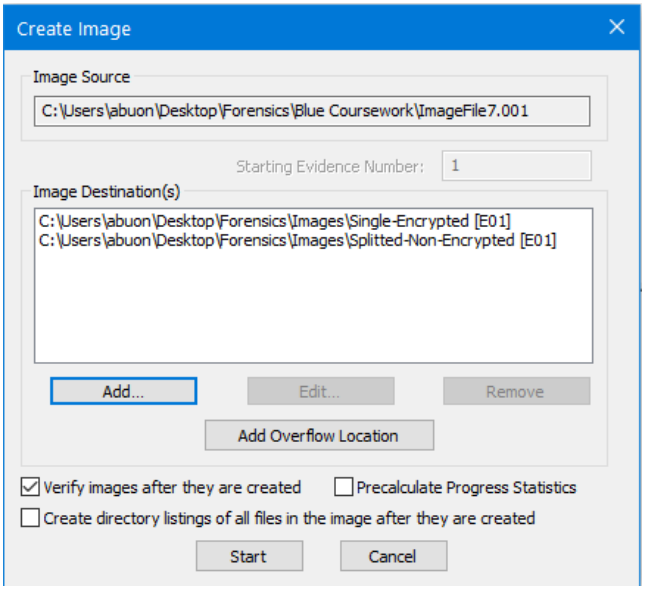

Figure 1.6: Create Image Dialog with Images

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.

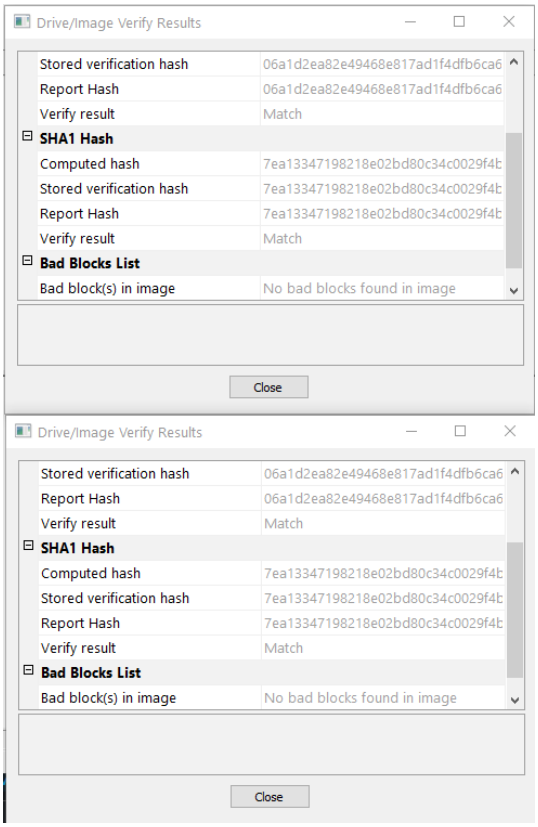

Figure 1.7: Verify Result Dialog

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

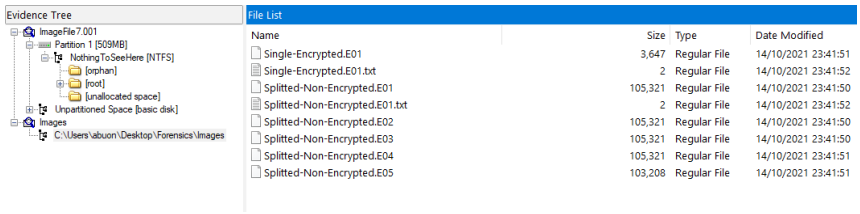

Figure 1.8: File Structures

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.

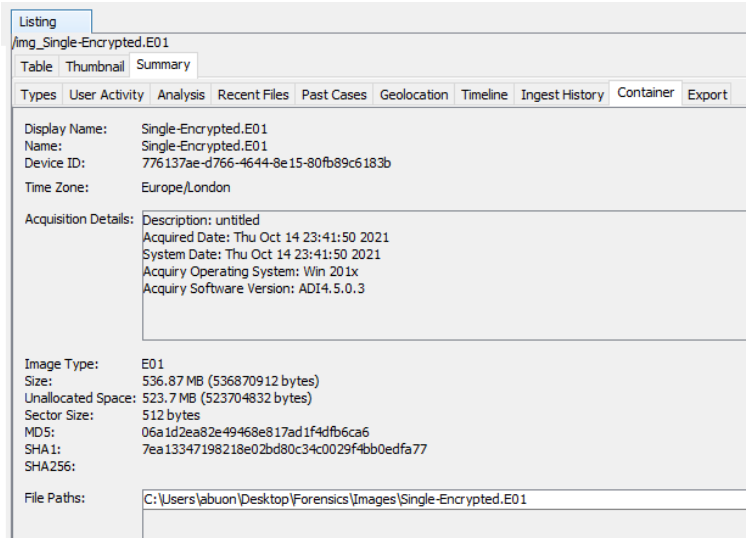

Figure 1.9: Autopsy Dual Tool Verification

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

Below the plan for the search and seizure task, coupled with the pictures and their descriptions.

2.1 PLAN

1. **Safety:** A bedroom is the subject of the examination. It is a double bedroom owned by a single person, meaning that control measures for entering or leaving the room are not followed.
2. **Scene:** The scene setting as previously mentioned is for a double bedroom. It has two desks with desktop computers and general hardwares such as keyboards, mouses and monitors. A TV is also present on the right side of the room. A super-king bed is also found in the middle of the scene.
3. **Assistance:** If large items need to be kept in costudy, then assistance would be required in order for the item to be taken in custody. For small devices, even though they can be easily handled, assistance might still be needed to isolation and prevention of any kind of damage.
4. **Inteview:** Some questions could be asked to the suspect, such as passwords or additional informations.

2.2 PICTURES OF SCENE

In this section, all pictures related to the investigation are listed and described.

2.2.1 *Full Scene*

The picture below pictures the whole scene that is subject to the investigation.

Figure 2.1: Full scene of the investigation

2.2.2 *Left Desk*

The picture below shows the left desk of the scene. It has a monitor, speakers, keyboard, mouse, mousepad and an Apple Watch. The Apple Watch has been taken into custody for further investigation. See AB/5 (2.3.5).

Figure 2.2: Left Desk

2.2.3 *Right Desk*

The picture below shows the right desk of the scene. It has a monitor, speakers, keyboard, mouse, mousepad, microphone, laptop, HDD, soundbar, subwoofer, controller, an amp sound card and a smartphone. The items taken in costudy are the Laptop (2.3.1), HDD (2.3.2) and the smartphone (2.3.3).

Figure 2.3: Right Desk

2.2.4 *Chest of Drawer*

The picture below shows a chest of drawers used as a stand for a TV. On top of it there is also a portable usb that has been taken in custody (AB/4).

Figure 2.4: Chest of Drawer with TV

2.3 PICTURES OF EVIDENCES

In this section, all pictures of the evidences that have been taken in custody.

2.3.1 *Exhibit AB/1 (MacBook Pro)*

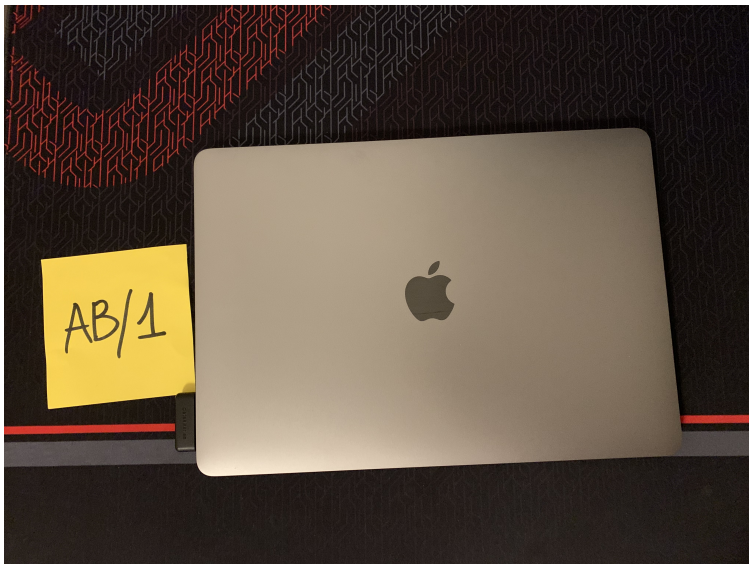

Figure 2.5: Macbook Pro: Front

Figure 2.6: Macbook Pro: Back

2.3.2 *Exhibit AB/2 (HDD)*

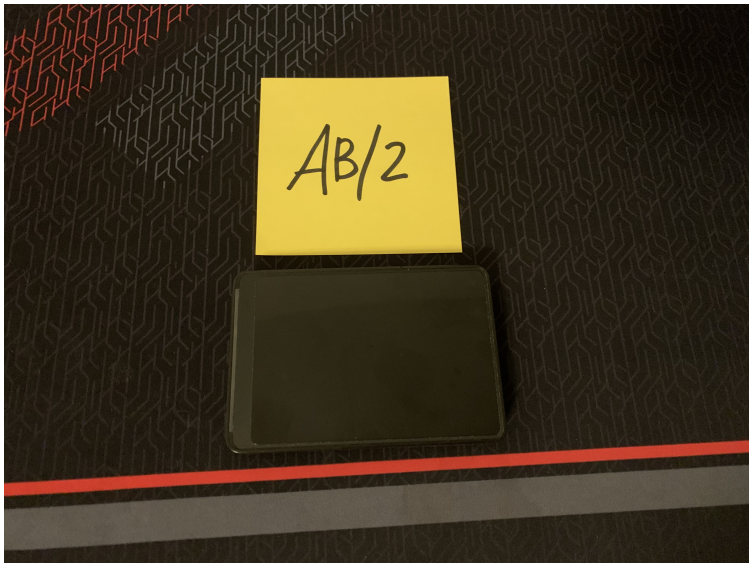

Figure 2.7: HDD: Front

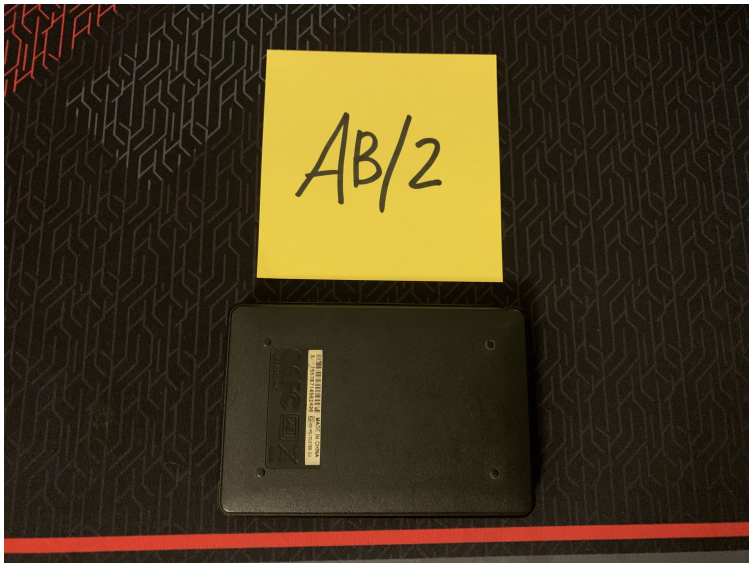

Figure 2.8: HDD: Back

2.3.3 *Exhibit AB/3 (Smartphone)*

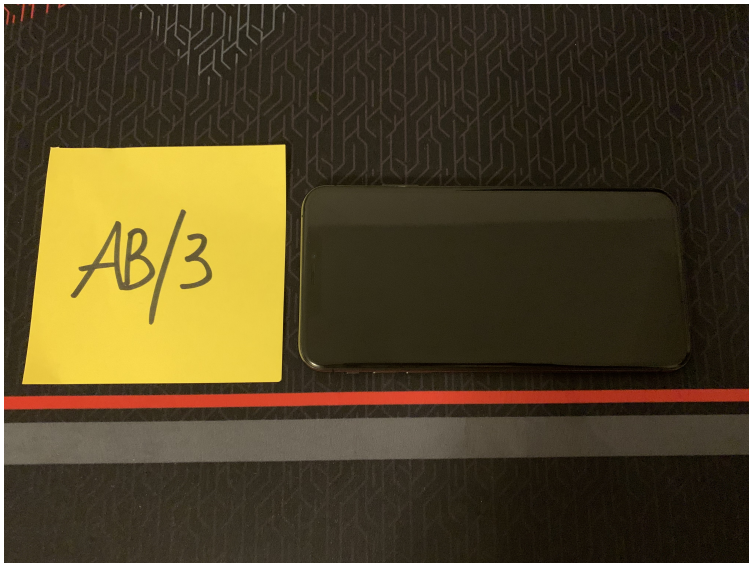

Figure 2.9: Smartphone: Front

Figure 2.10: Smartphone: Back

2.3.4 *Exhibit AB/4 (Portable USB)*

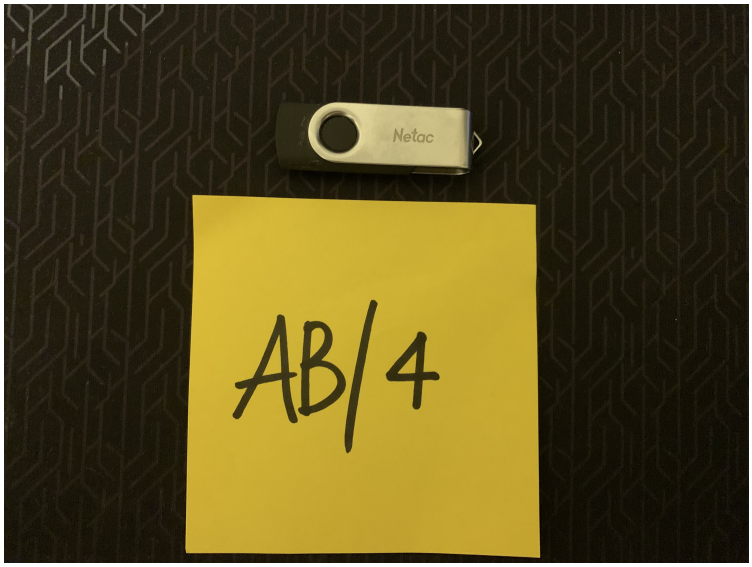

Figure 2.11: Portable USB: Front

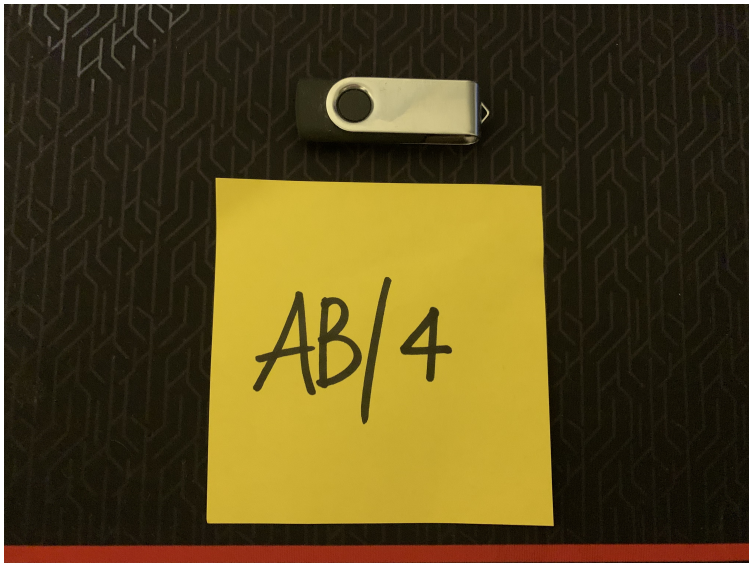

Figure 2.12: Portable USB: Back

2.3.5 *Exhibit AB/5 (Apple Watch)*

Figure 2.13: Apple Watch: Front

Figure 2.14: Apple Watch: Back

2.4 EXHIBIT RECORDS

2.4.1 *AB/1: Laptop*

Location: Right Desk

Seized by: Alessandro Buonerba

Time: 29/10/2021 at 16:00

2.4.2 *AB/2: HDD*

Location: Right Desk

Seized by: Alessandro Buonerba

Time: 29/10/2021 at 16:10

2.4.3 *AB/3: Smartphone*

Location: Right Desk

Seized by: Alessandro Buonerba

Time: 29/10/2021 at 16:15

2.4.4 *AB/4: Portable USB*

Location: Chest of drawer

Seized by: Alessandro Buonerba

Time: 29/10/2021 at 16:25

Seal Number : AB

2.4.5 *AB/5: Apple Watch*

Location: Left Desk

Seized by: Alessandro Buonerba

Time: 29/10/2021 at 16:40

2.5 SEALED EVIDENCES

The evidence that have been sealed is Exhibit AB/4 (2.3.4). They have been stored in a sealed envelope that cannot be tempered without leaving tracks of it. If the seal breaks, there would be noticeable traces of it as shown in figure 2.18.

2.5.1 *Sealed Exhibit AB/4 (Portable USB)*

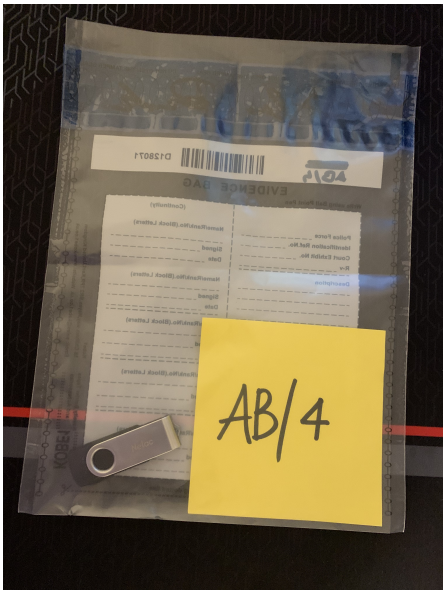

Figure 2.15: Sealed Portable USB: Back

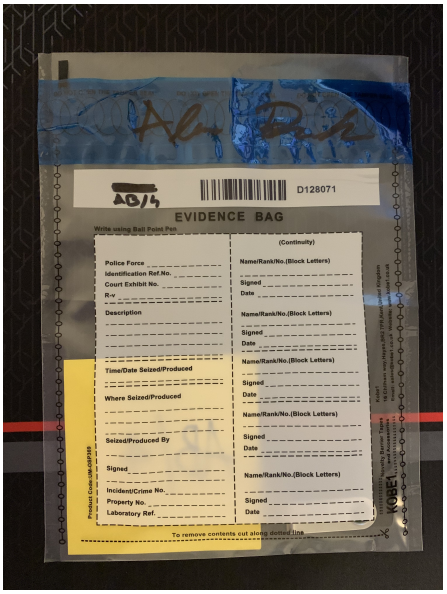

Figure 2.16: Sealed Portable USB: Front

2.5.2 *Seal*

Below a close-up of the seal is shown.

Figure 2.17: Close-up Seal

This is an example of possible tempered evidence.

Figure 2.18: Broken Seal

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: Alessandro Buonerba BSc(Hons) Computer Science (Cyber Security)

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

This statement (consisting of 7 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: **Alessandro Buonerba** Date: 29/10/2021

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 2018. I have Bachelor of Science degree in Computer Science (Cyber Security) 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.

Continuation of Statement of Alessandro BUONERBA

4. This statement should be read in conjunction with that of my colleague, Mr. A. Aaron Adamson who is the imaging technician in this case.

5. The exhibit to which my examination refers is as follows: A forensic image file called 'Operation Blue 3 - 2021.E01', relating to exhibit ABL/1, a USB drive.

6. Following instructions from the investigating officer I have conducted an examination of the of the image file in order assist the investigation into alleged drugs offences.

7. My examination was conducted using sound forensic methodology, tools and practices. I have followed the 'Good Practice Guide for Digital Evidence' produced by the Association of Chief Police Officers (ACPO).

8. During my examination I recorded my actions and observations in my original notes. These notes provide more detailed technical aspects of the forensic image of the exhibit and the processes and tools that I used. They can be produced if required.

Summary of Findings

9. 1 (one) artefact that present password hiding techniques

10. 2 (two) artefacts present on device that show conversations between two entities

11. 5 (five) artefacts are present that link towards a website

12. 1 (one) artefact of a CV

13. 25 (twenty-five) artefacts related to drugs

14. 4 (four) artefacts of child pornography

15. 5 (five) artefacts of pornography

Signature: Alessandro Buonerba ..... Signature witnessed by: Not Required for Professional Witnesses .....

Detailed Findings for Exhibit ABL/1

16. The file 'Operation Blue 3 - 2021.E01' is the forensic image of the USB drive of exhibit ABL/1. For the remainder of the statement, I will refer to my examination as being on exhibit ABL/1.

17. ABL/1 contains the NTFS file system and is 2045MB in size. My examination shows that the last recorded use of the computer was on 18/10/2021 at 18:11:09.

18. The currently installed operating system is Windows 10 Enterprise Evaluation with a recorded installation/update date of 19th of March at 12:59:35. The registered owner is recorded as Piet and there is a single (1) user account present named IEUser which has a password set for it. My examination shows that the last recorded use of the computer was on 18/10/2021 at 18:11:09.

Documents and Notable Files

19. I searched ABL/1 using the Autopsy version 4.19.1.

20. One of the documents found is "Note to self.txt" created on 2021-10-19 12:30:30 BST and located in the "/Work/" folder. This file contains the following sentence: "better yet, make a website where we can just mail this stuff to people without the stupid driving around".

21. 4 (four) more documents are found in the "Work/Home sweet home_files/" folder. The files are named "Home sweet home.html", "How much do drugs cost_ – DrugWise.html" and "How much do drugs cost_ – DrugWise.html", which are artifacts 4, 5 and 6 in the order presented. These files are web pages that are related to inform and sell drugs to the viewer of the page. The meta-data of all the files are also included in the evidential extraction.

22. A CV in a format of a Rich Text File has been found in the Work directory. The CV has some information about "Simon Piet van der Valk" and it emphasise the fact that is still doing University

and that he has web design skills. The CV seems to be only a draft as it contains unfinished sentences. I have included the notable files on the evidential extraction, AB/1.

Pictures and Video

23. 25 (twenty-five) artefacts (from 11 to 36) related to drugs have been found in the folder "/Work". All images listed here depict pictures of drugs which were found on the device.

24. 4 (four) artefacts representing child pornography have also been found in a folder hidden inside another folder named "delete.jpg". The name of the folder containing the material is "nawty kitty" and has been create on 2021-10-19 at 12:30:30 BST.

25. 5 (five) more images of pornography have been found in the "Work/Fun times/Fun times/" folder where they have been created on 2021-10-19 at 12:30:30 BST. I have included the notable pictures on the evidential extraction, AB/1.

Chat Artefacts

26. 2 (two) documents containing chat messages sent to "JamesP" and "Ellie" have been found. The files are named after the name of the recipient such as "JamesP.txt" and "Ellie.txt" and are located in the "backups/greSTYLE chat/Logs/" folder. The message exchanges made in the JamesP files states that the subject has recently bought a new laptop. Additionally, he addresses himself as the "dutchman" and to Miss Ellie as "Piet" and shows his preoccupation about the cops to JamesP. I have included the notable Internet history on the evidential extraction, AB/1.

Signature: Alessandro Buonerba ..... Signature witnessed by: Not Required for Professional Witnesses .....

Registry Artifacts

27. Two (2) Registry Files were found on this device located "/img_Operation Blue 3 - 2021.E01/vol_vol2/backups/Registry/". The name of the files is SAM & SOFTWARE. An application called Windows Registry Recovery was used to examine and open these files. The user would need to use specific tools to view the files. Within "SAM" the IEUser is set with the name "Piet" and the last login can be seen as "18/10/2021 18:11:09". The user was online for 6 hours and then changed the password set at "19/10/2021 02:01:47" Meta-data for the registry files has been added to the evidential extraction.

Conclusions

28. As stated in the section 20, there is a note that shows the intention of the creation of a website to sell unknown items. This combined to the evidence of a Drupal website and related images of the items and drugs sold would be a premeditated intention of marketing the illegal substances over the internet to customers around the world.

29. In the section 21, there were files related to a Drupal website containing all drug pictures that have been disclosed previously. Specifically, there was a webpage explaining the cost of the drugs. This could suggest that the owner of the USB wanted to purchase or sell drugs at internet standard price.

30. In section 22, the CV displays information's of the suspect name, being Simon Pier Van Der Valk, this would suggest that he is the owner of the document. The last sentence is: "Blah blah... there is a reason I don't do real jobs blah", which could hide a subliminal message.

31. In section 23, It seems as the pictures are used as a thumbnail for a website that is used as a marketplace where users can buy drugs and get it delivered at home. The name of the files is

Signature: Alessandro Buonerba Signature witnessed by: Not Required for Professional Witnesses

also the name of the drugs that are shown in the pictures. Some images have also been given a different extension (Artifact 33/34/35/36, where the extension has been changed to .php) in hope to hide the content.

32. In section 24 and 25, illegal material such as child-pornography has been found in the USB device. This could link to different crimes not related to drugs.

33. The fact that only a laptop bag has been found in the apartment of the suspect is connected to the section 26, where messages to JamesP states that he would bring his new laptop over to work on something. This suggest that the last statement on the status of his computer made on the scene could not be true, as the evidence suggests otherwise.

34. In section 27 the registry files show that a user named “Piet” logged on to a device containing Windows 10. This time shows that it is in the timeframe of when Mr Piet Van Der Valk claims to not of had access to a computer. The name of the user links to the same name of the suspect who is in question. This name also appears again in section 26.

35. Many files have the same date of creation, meaning that they have been transferred from a device to this USB in batch and are not the main source of truth.

Exhibit Production

36. As a result of my analysis I produce the following exhibit:

Exhibit	Bag Seal	Description of Exhibit
AB/1	Unsealed	Evidential Extraction Document

37. I have attached to this statement the evidential extraction, exhibit your AB/1.

Signature: Alessandro Buonerba ..... Signature witnessed by: Not Required for Professional Witnesses .....

Continuation of Statement of Alessandro BUONERBA

Disclosure

38. I confirm that I have complied with my duties to record, retain and reveal material in accordance with the Criminal Procedure and Investigations Act 1996, as amended.

39. In the event my opinion changes on any material issue, I will inform the investigating officer as soon as reasonably practicable and give reasons.

Duty to the Court

40. I declare that I understand that my duty, including providing written reports and giving evidence, is to assist the court and that this duty overrides any obligation to the party who has engaged me. I can confirm that I believe that I have complied with my duty.

41. I confirm that, to the best of my knowledge and belief, I have acted in accordance with the Code of Conduct published by the Forensic Science Regulator (Issue 4) in all aspects that relate to my personal conduct. Alessandro Buonerba

Signature: Alessandro Buonerba ..... Signature witnessed by: Not Required for Professional Witnesses .....

4

CONCLUSION

This is the conclusion.