

Digital Forensics Project

Demonstrating Practical Forensic Skills through University Coursework

Irfan Ahmed | Irfan1043ahmed@gmail.com

Tools used: Autopsy, EnCase, FTK Forensic Toolkit, HashMyFiles

This document presents a series of simulated digital forensics and eDiscovery projects conducted as part of a university coursework. The projects were designed to mimic real-world scenarios and were performed in a controlled academic environment. The tasks included imaging exercises, search and seizure operations, and the preparation of expert witness statements. All activities and findings documented within this portfolio are based on theoretical and practical exercises using standard digital forensics tools and methodologies. The intent of this portfolio is to demonstrate proficiency in digital forensics practices and to showcase the skills developed through rigorous academic training. This work does not involve actual forensic investigations on live or real-world data and should be viewed as educational exercises aimed at preparing for professional roles in digital forensics and eDiscovery.

Introduction

This project portfolio showcases a series of practical digital forensics and eDiscovery exercises completed during my university coursework. The assignments involved critical tasks such as forensic imaging, verification of forensic images, conducting search and seizure operations, and providing expert witness statements. Utilizing a variety of industry-standard tools and methodologies, these projects demonstrate my ability to handle real-world forensic investigations and produce comprehensive, professional reports. Each project is meticulously documented with detailed explanations and visual evidence, illustrating my proficiency in digital forensic techniques and my commitment to accuracy and thoroughness.

Overview

This portfolio is divided into several key projects, each designed to cover different essential components of digital forensics and eDiscovery:

1. Imaging Exercise

- **Objective:** To demonstrate the ability to create, verify, and manage forensic images using various tools.
- **Tasks:**
 - Verify the integrity of a forensic image using hashing tools.
 - Create a single EWF/E01 image file with compression and split it into multiple parts.
 - Verify the accuracy of the created images using dual tool verification.
 - Explain the concept and use of write blockers to a non-technical audience.

2. Search and Seizure

- **Objective:** To simulate the search and preservation of potential digital forensic evidence in a controlled environment.
- **Tasks:**
 - Set up a simulated domestic environment for evidence search.
 - Document the search process with detailed diagrams and photographs.
 - Create an Exhibits Record table for all seized items, including improvised sealing methods.
 - Report on the search and seizure process, highlighting key findings and methodologies used.

3. Written Evidence and Opinion

- **Objective:** To produce an expert witness statement based on the analysis of provided digital evidence.
- **Tasks:**
 - Conduct an individual analysis of a provided image file.
 - Answer specific questions posed by the Crown Prosecution Service (CPS) based on the analysis.
 - Produce an MG11-style statement detailing the analysis results, findings, and expert opinion.

Project 1: Imaging Exercise

Introduction

This project focuses on demonstrating the fundamental skills required in digital forensics through an imaging exercise. The tasks involve verifying the integrity of a provided forensic image file, creating forensic image copies in different formats, and verifying these images using multiple forensic tools. This exercise simulates real-world forensic practices, where the accuracy and integrity of data are paramount.

The primary objectives of this project are to:

1. Verify the integrity of a forensic image file using hash values.
2. Create a compressed EWF/E01 image and a split EWF/E01 image, ensuring data integrity during the process.
3. Use dual tool verification to confirm the accuracy of the created images.
4. Explain the concept and function of a write blocker in a manner understandable to non-technical audiences, such as a jury.

Throughout this project, various industry-standard tools such as HashMyFiles, FTK Imager, and the FTK Forensic Toolkit are utilized. Each step is meticulously documented with clear and legible screenshots, providing a transparent view of the forensic process and ensuring the reproducibility of results.


This project is designed to showcase my ability to handle forensic imaging tasks, a critical component of digital forensics and eDiscovery. By demonstrating proficiency in these essential techniques, I aim to highlight my readiness for professional roles in the field.

Task 1

1.1. Hash Verification: Demonstrate working on the correct image file

Part A:

Image file - ImageFile.021.dd

Filename	MD5	SHA1
 ImageFile.021.dd	097cccb8e3de1e474680191d191c7a43	c0a5ccba53af3886217302e25f8ca7c9fcbe94bb

Full Path	Modified Time	Created Time	Entry Modified...	File Size
C:\irfan\BLUE CW\ImageFile.021.dd	23/11/2023 08:...	23/11/2023 08:...	23/11/2023 08:...	536,870,912

Verification image:

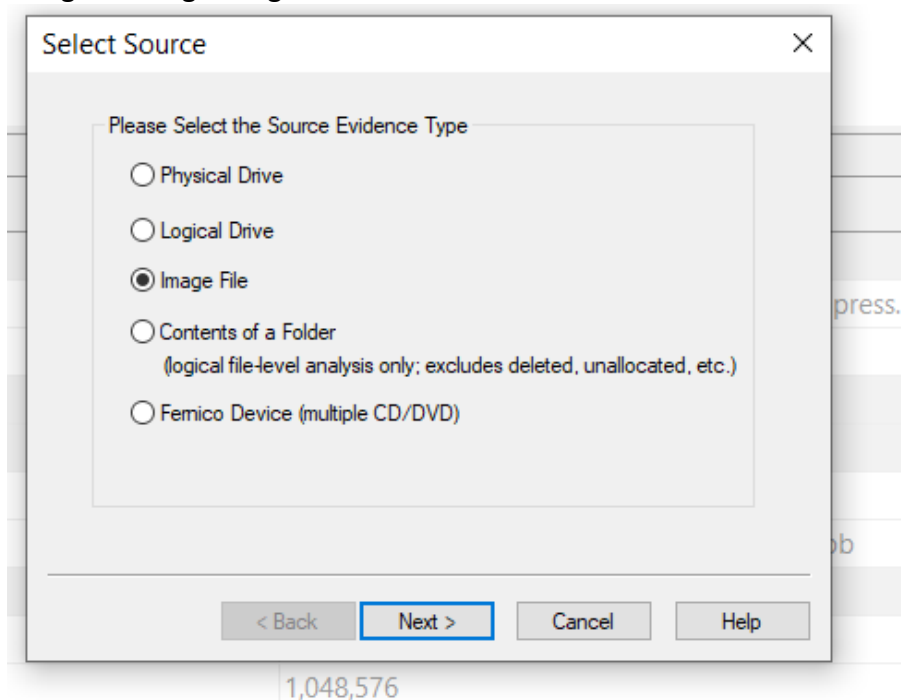
ImageFile.021.dd	097cccb8e3de1e474680191d191c7a43	c0a5ccba53af3886217302e25f8ca7c9fcbe94bb	536,870,912
------------------	----------------------------------	--	-------------

As you can see above, I have verified that we are working with the correct image file. I used HashMyFiles to verify that the .dd file that we were given is the same and this was verified by the hash values and the size of the file. As they are identical, this confirms that we are working with the correct .dd file.

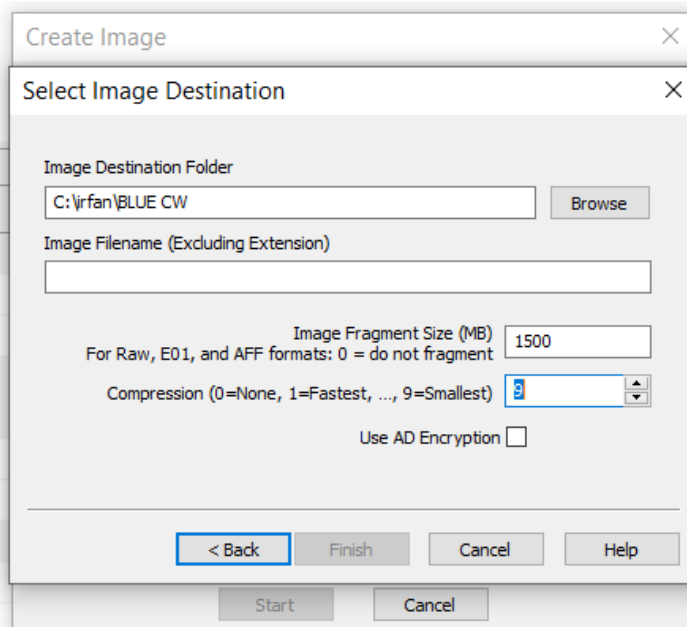
1.2. Image file at max compression

Documentation of process:

In order to create the image file with the max compression we have to create a new disk image using the image file given.



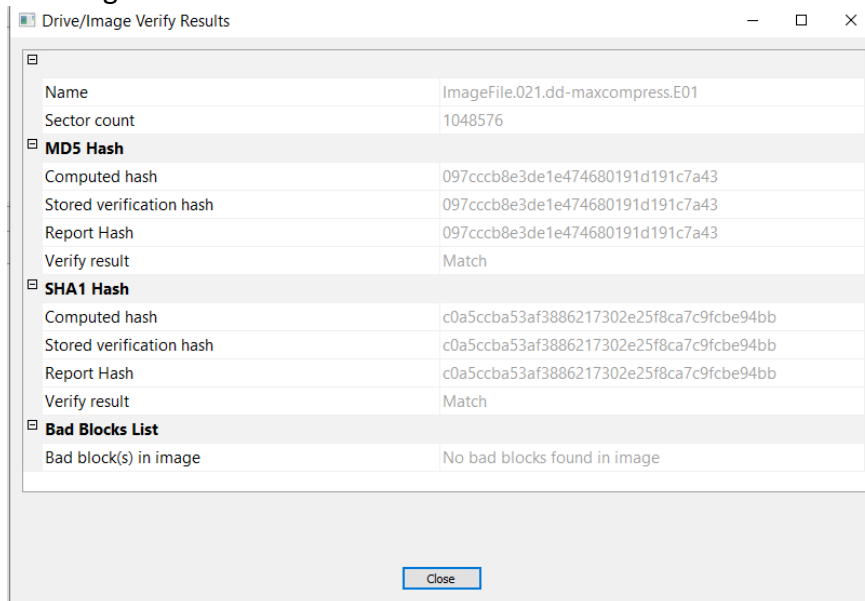
Since we have the image file we select that option and then select next in which we must locate the image file within the device in order to create the max compression version for it.



Then we have to select the destination folder for our new image file and within this section we can set the compression to maximum as stated within the screenshot. The max compression is 9 so that is what I set it to.

Verification of image:

FTKImager:



HashMyFiles:

Filename	MD5	SHA1
ImageFile.021.dd-maxcompress.E01	4dcbd89c889695a0868fb6c0f570ab4	8e2f875866e6087c50ae04c2aeb8e7c2df81c927

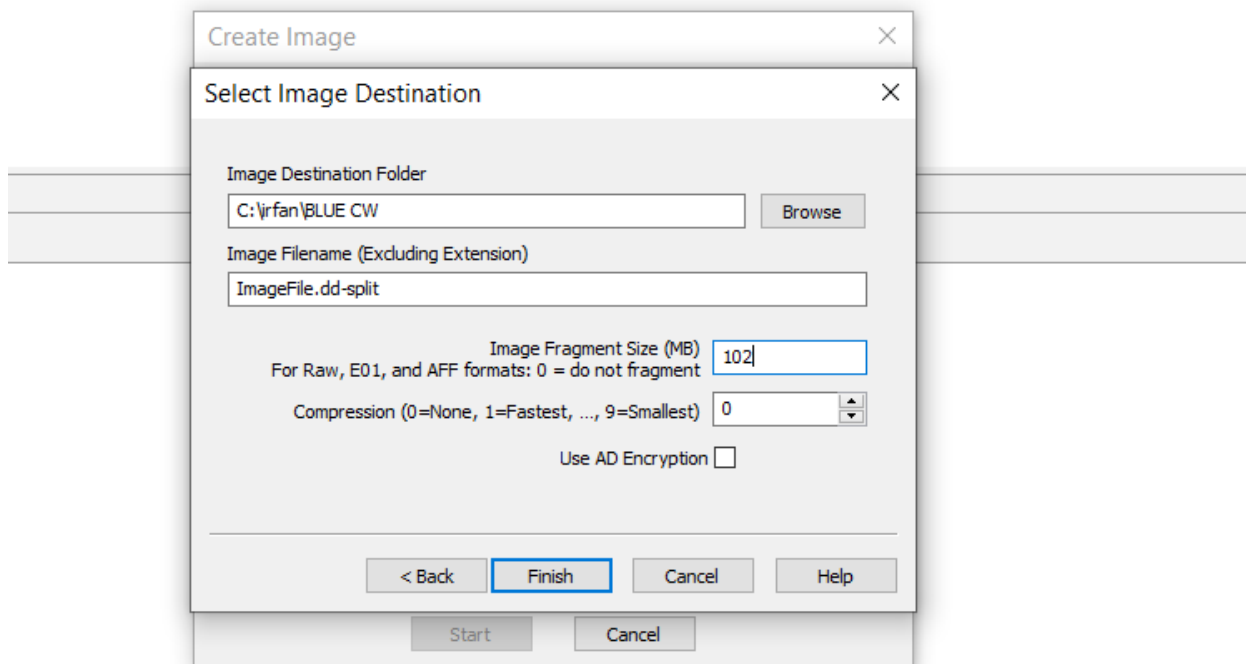
Full Path	Modified Time	Created Time	Entry Modified...	File Size
C:\irfan\BLUE CW\ImageFile.021.d...	23/11/2023 08:...	23/11/2023 08:...	23/11/2023 08:...	3,724,688

These are the verification of the image file with max compression, the first is from FTKImager just after the file was created and the second is from HashMyFiles to check if it is correct and to see the file size.

ImageFile.021.dd	097cccb8e3de1e474680191d191c7a43	c0a5ccba53af3886217302e25f8ca7c9fcbe94bb	536,870,912
------------------	----------------------------------	--	-------------

The image above is the original image file and its file size is shown and we can tell that our compression worked as our file size is smaller which shows that the compression worked. As we can see within the verification image from FTKImager, the has values are similar to the original .dd file and shows that the data within the EO1 file is accurate and has not been changed compared to the original. The screenshot from HashMyFiles shows that the compression was successful as the hash values are different and the file size is smaller compared to the original. This is because the hash values are for the EO1 file itself and not the content within which was shown in the FTKImager screenshot and the file size being smaller shows the success of the compression. The reduced file size confirms the success of the compression process, therefore, while FTKImager verifies the integrity of the data content within the EO1 file against the original file, HashMyFiles calculates the hash of the EO1 file as a whole, accounting for the differences observed.

1.3. EO1 file split into 5 parts



As you can see above, to create an EO1 with at least 5 splits, we had to set the fragment size to 102 mb. This is because the total file size was 512mb and to get at least 5 splits we had to divide the total size by the amount of splits we wanted which was 5 thus we set the fragment size to 102 as this ensured 5 splits with a size of 102mb and the remainder of the file within the sixth split. The image below shows the successful completion of the splits. Here we can see the 6 splits of the EO1 file as requested.

Image File Name	Size	File Type	Size
ImageFile.dd-split.E01	23/11/2023 10:44	E01 File	104,297 ...
ImageFile.dd-split.E01	23/11/2023 10:44	Text Document	2 KB
ImageFile.dd-split.E02	23/11/2023 10:44	E02 File	104,296 ...
ImageFile.dd-split.E03	23/11/2023 10:44	E03 File	104,296 ...
ImageFile.dd-split.E04	23/11/2023 10:44	E04 File	104,296 ...
ImageFile.dd-split.E05	23/11/2023 10:44	E05 File	104,296 ...
ImageFile.dd-split.E06	23/11/2023 10:44	E06 File	3,011 KB

Below is the verification of the first EO1 file as it shows the hash values and these match the original .dd file hash value which confirms that the data within the EO1 files have not been altered and accurately reflects the original data.

Drive/Image Verify Results	
Name	ImageFile.dd-split.E01
Sector count	1048576
MD5 Hash	
Computed hash	097cccb8e3de1e474680191d191c7a43
Stored verification hash	097cccb8e3de1e474680191d191c7a43
Report Hash	097cccb8e3de1e474680191d191c7a43
Verify result	Match
SHA1 Hash	
Computed hash	c0a5ccba53af3886217302e25f8ca7c9fcbe94bb
Stored verification hash	c0a5ccba53af3886217302e25f8ca7c9fcbe94bb
Report Hash	c0a5ccba53af3886217302e25f8ca7c9fcbe94bb
Verify result	Match
Bad Blocks List	
Bad block(s) in image	No bad blocks found in image

Part B: Use two different forensic tools to verify the image

Verification of EO1 file:

Using FTKImager:

Drive/Image Verify Results	
Name	ImageFile.021.dd-maxcompress.E01
Sector count	1048576
MD5 Hash	
Computed hash	097cccb8e3de1e474680191d191c7a43
Stored verification hash	097cccb8e3de1e474680191d191c7a43
Report Hash	097cccb8e3de1e474680191d191c7a43
Verify result	Match
SHA1 Hash	
Computed hash	c0a5ccba53af3886217302e25f8ca7c9fcbe94bb
Stored verification hash	c0a5ccba53af3886217302e25f8ca7c9fcbe94bb
Report Hash	c0a5ccba53af3886217302e25f8ca7c9fcbe94bb
Verify result	Match
Bad Blocks List	
Bad block(s) in image	No bad blocks found in image

Close

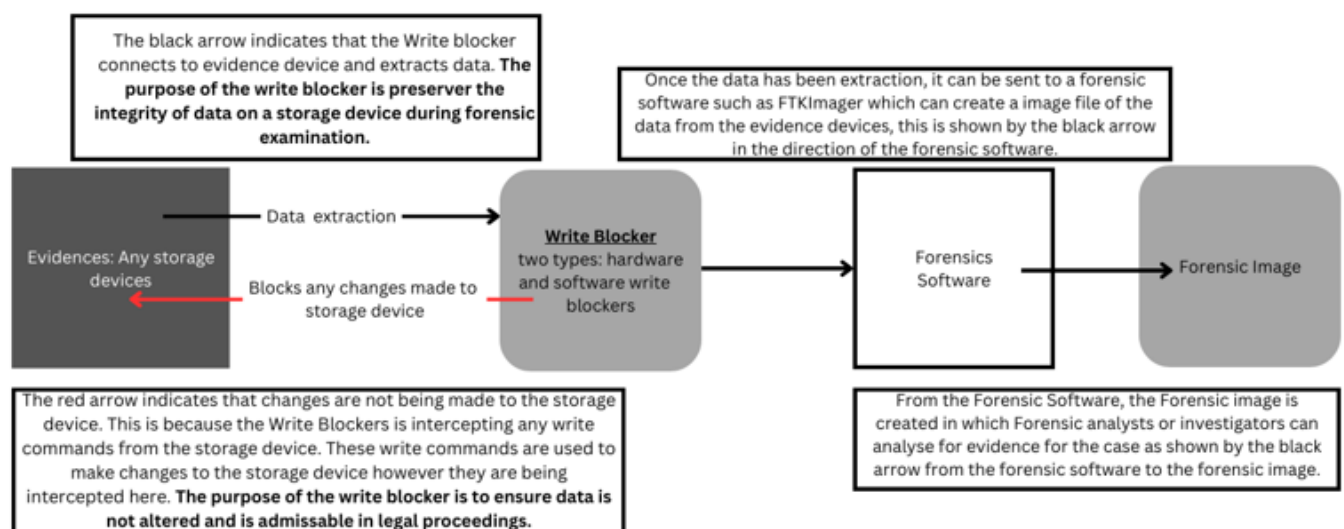
This is the verification results for the file we created in Part A, this was acquired using FTKImager after creating the image file and it shows the hash values associated with it. To complete the dual verification we have to use a different forensic tool and I chose to use Autopsy to verify the results.

Metadata	
Name:	/img_ImageFile.021.dd-maxcompress.E01
Type:	E01
Size:	536870912
MD5:	097cccb8e3de1e474680191d191c7a43
SHA1:	c0a5ccb8a53af3886217302e25f8ca7c9fcb94bb
SHA-256:	Not calculated
Sector Size:	512
Time Zone:	Europe/London
Acquisition Details:	Description: untitled
:	Case Number: 1
:	Evidence Number: 1
:	Acquired Date: Thu Nov 23 08:31:00 2023
:	System Date: Thu Nov 23 08:31:00 2023
:	Acquiry Operating System: Win 201x
:	Acquiry Software Version: ADI4.5.0.3
Device ID:	e4699409-d42b-4aed-8e7f-65fb1073105a

As you can see here, we have the verification results from Autopsy and it shows the hash values and they are identical to the values shown in FTKImager which confirms that the image is verifiably correct.

Part C: Explain the concept of a write blocker with a diagram suitable for a jury

Diagram depicting the purpose and function of a Write Blocker:



Project 2: Search and Seizure

Introduction

The Search and Seizure project is a comprehensive exercise designed to simulate the real-world process of searching a physical environment for digital forensic evidence and accurately documenting the findings. This exercise aims to demonstrate the practical application of digital forensics principles in a controlled scenario, emphasising the meticulous planning, execution, and documentation required for a successful forensic investigation.

In this project, I set up a mock crime scene in a bedroom, which includes a variety of digital devices and potential sources of evidence. The primary objective is to conduct a thorough search, identify and seize relevant items, and produce detailed documentation that would be admissible in a court of law. This includes creating a diagram of the scene, photographing the items in situ, cataloguing the evidence, and properly sealing and labelling each item.

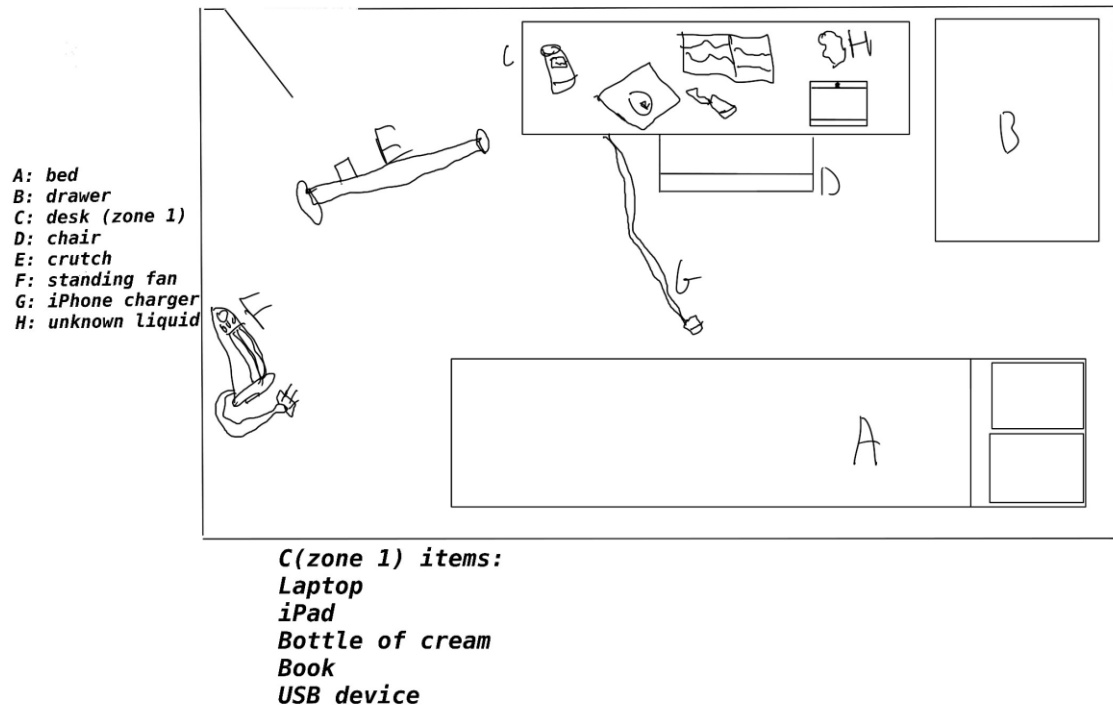
This exercise not only highlights the importance of methodical search techniques and precise evidence handling but also underscores the necessity of clear and comprehensive documentation. The skills demonstrated in this project are critical for ensuring the integrity and admissibility of digital evidence in legal proceedings. Through this project, I am to showcase my ability to apply digital forensic methodologies effectively, ensuring that evidence is collected, preserved, and documented in accordance with best practices and legal standards.

Task 2

Introduction of task:

For this task, I have designated my bedroom as the crime scene. The desk located right of the door to the room will be the key zone and will contain the items. I have chosen a few items, ranging from one large item to several smaller items. These items will include a laptop, designated as the large item, an iPad, and bottle of cream, a USB device and a book. The digital artefacts are the laptop, iPad and USB device and the non-digital items is the bottle of cream and book. The book is a notebook and is open on a page which has content relevant to the crime scene. The zone, which is the desk, will be processed and presented below.

A. Diagram of scene:



This sketch diagram presents an aerial view of the crime scene, showcasing the layout and items of interest in the room. Key objects are labelled A to G, with 'H' marking an unidentified substance on the desk, designated as Zone 1. There are notable safety concerns within the crime scene including an iPhone charger on the floor, posing a tripping hazard, and a crutch placed in the entry walkway, both warranting caution markers. The liquid spill on the desk required further attention, as its nature is unknown. Specialised assistance may be necessary to analyse this potential hazard. The desk area is the focus point of interest and will be the primary zone for detailing and collection of evidence.

B. Photograph of crime scene: Overview of Crime Scene
Image 1



Image 2

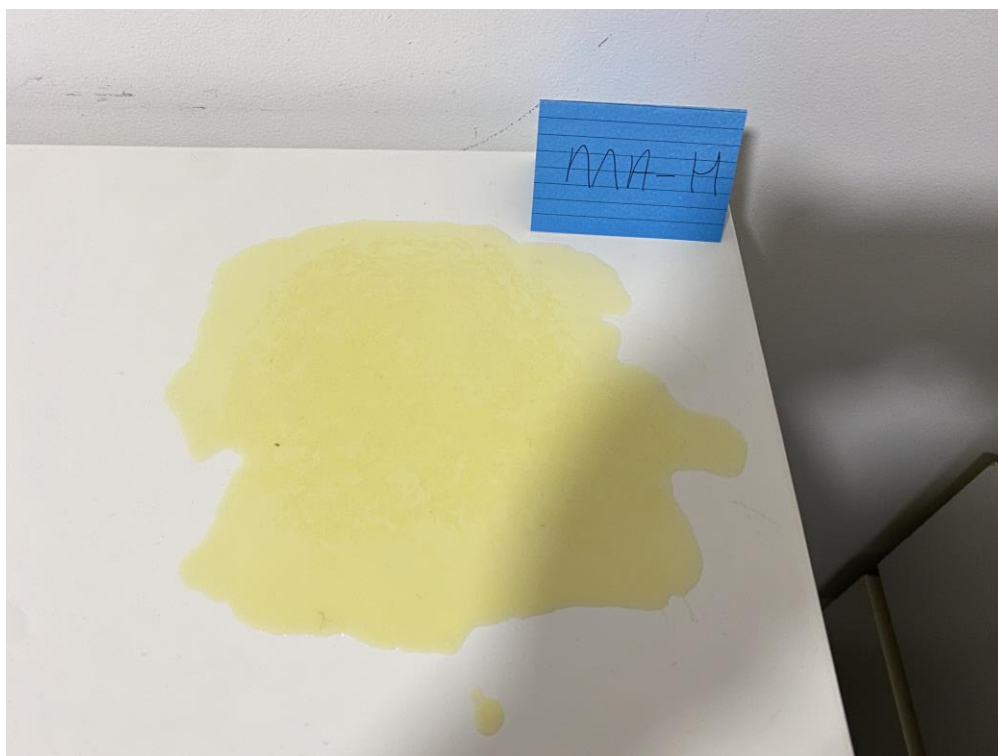


The above images are the complete crime scene which matches the sketch diagram. The zone is located on the left of the room as shown in the image above and shows the items of interest in situ. Within the images you can see a desk, with items, zone 1, a bed, drawer, crutch and a standing fan as described in the sketch diagram.

C. Photograph of zone



The image above is the aerial view of the zone located in the crime scene. The items of interest are as seen in situ; all items have an evidence marker assigned to them. The items shown above is a laptop marked MA-1, an iPad marked MA-2, a bottle of cream marked MA-3, an opened book marked MA-4, a USB device marked MA-5 and a unknown liquid spill.



Closer look at the unknown substance which appears to be a liquid spill. It has been labelled with a marker, MA-H, which corresponds with the sketch diagram of the scene. The substance has been labelled for further investigation into its identity.

D. Photographs of items: photographs of items in different angle

Item MA-1:

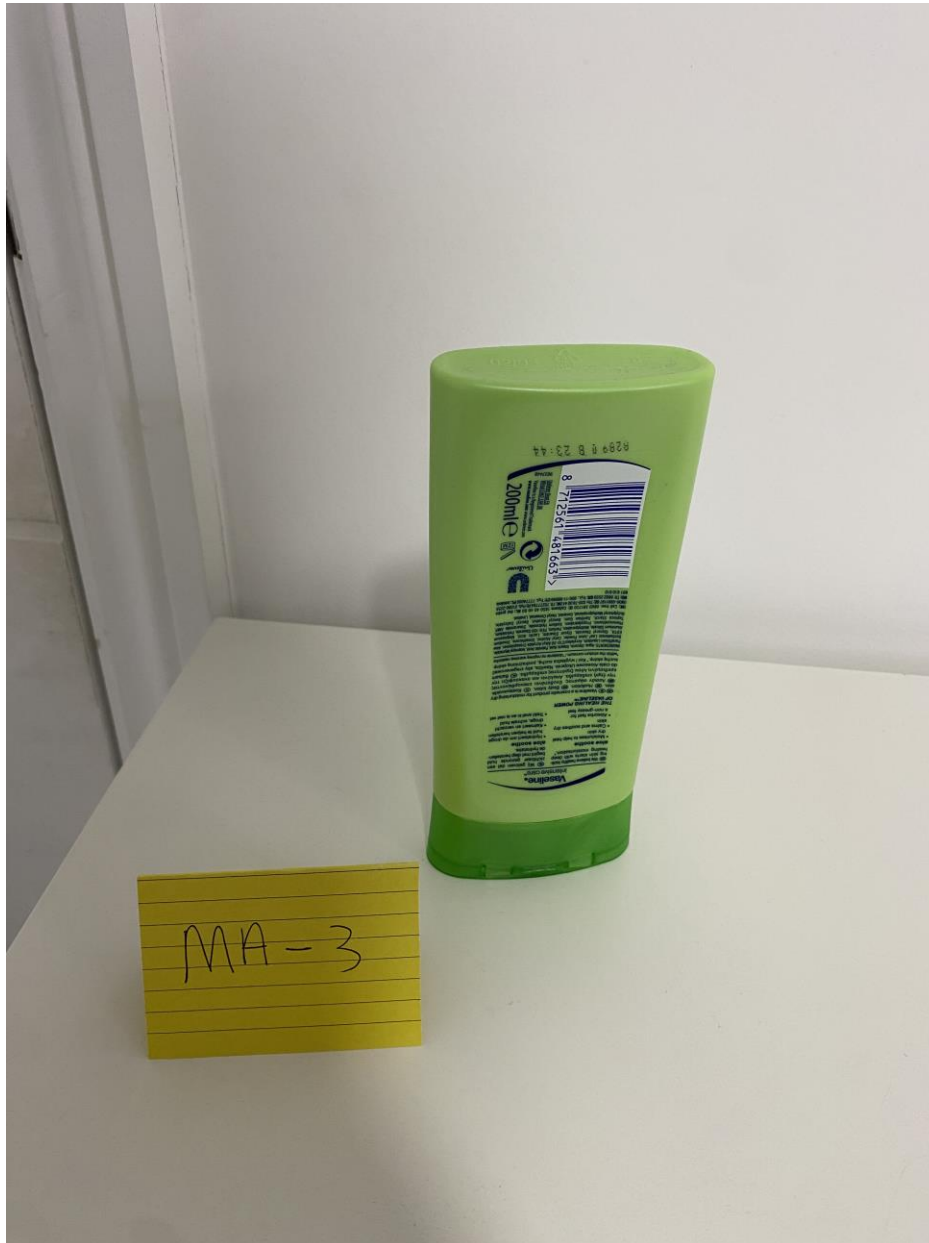


The photograph of the aerial view of the zone captured the items of interest in situ which showed the front view of the items and these photographs show the items in a different angle. The above image is item MA-1 which is the laptop that was found on the desk. This angle shows the bottom of the item and any identifiable information for the device.

Item MA-2:



Item MA-3:



Item MA-4:



Item MA-5:

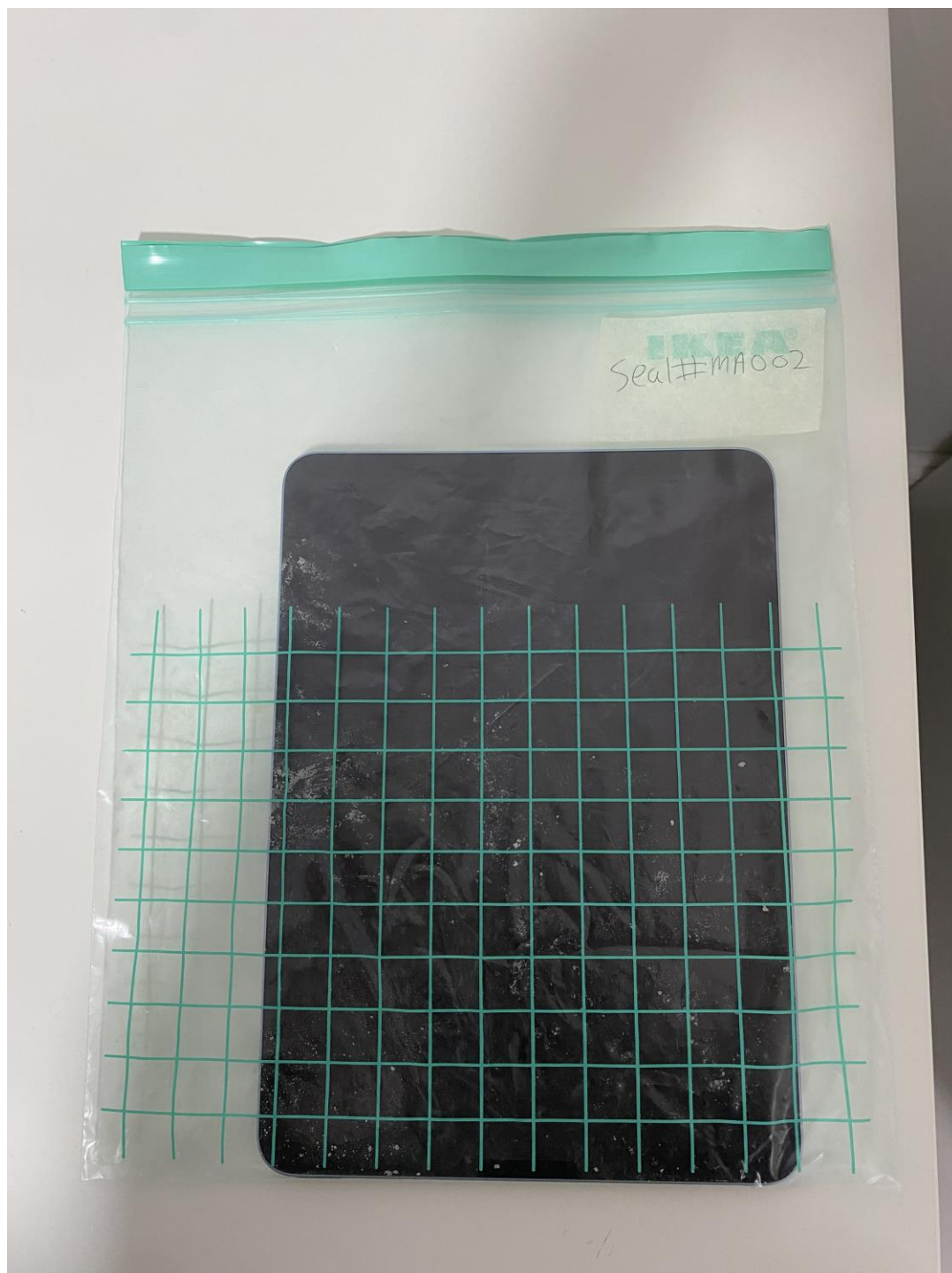


E. Bagged evidence: the photographs below show the items bagged within a see-through bag with an exhibit reference to refer to the evidence table and correspond with the images and sketch diagram

MA-1:



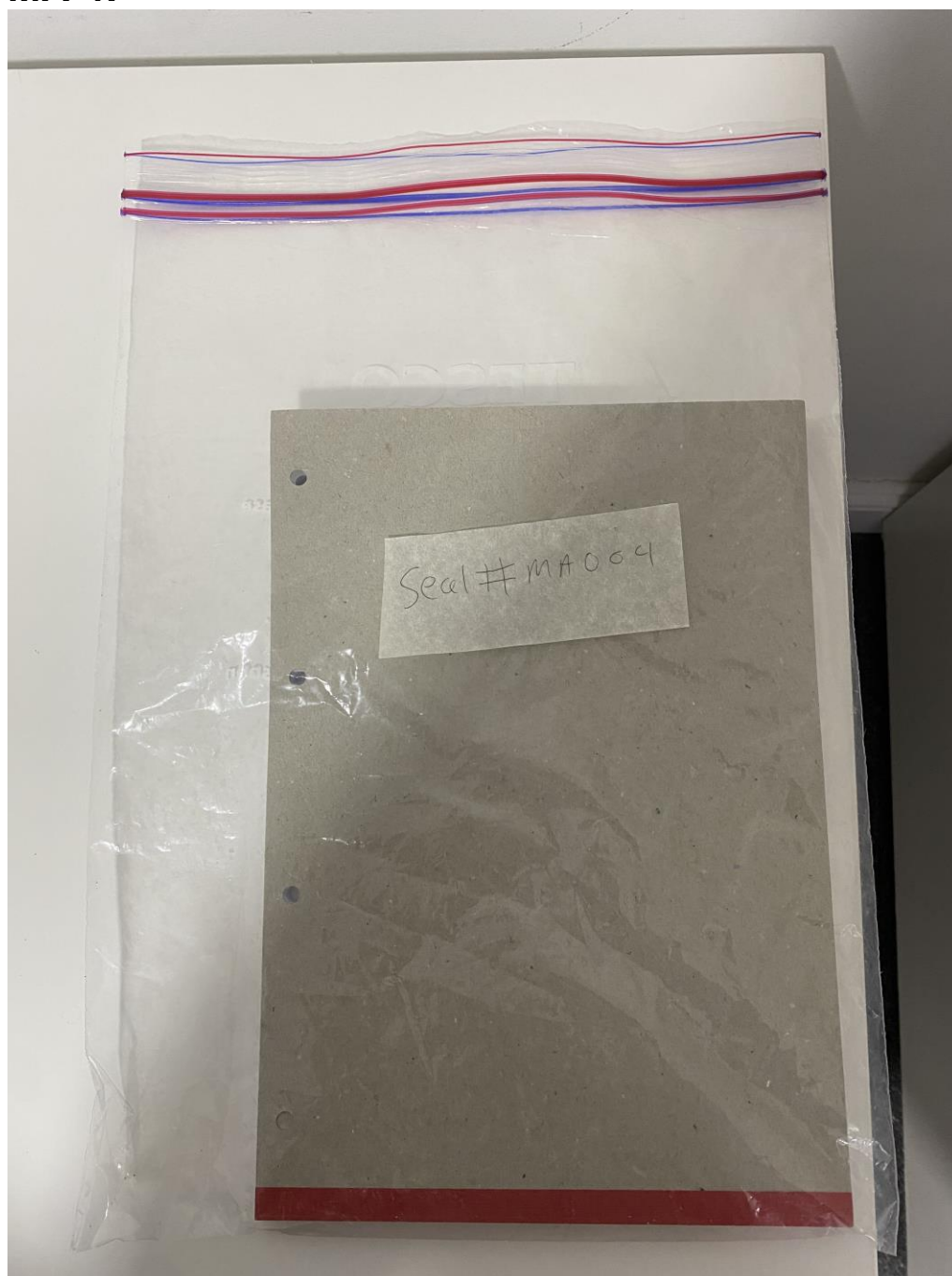
MA-2:



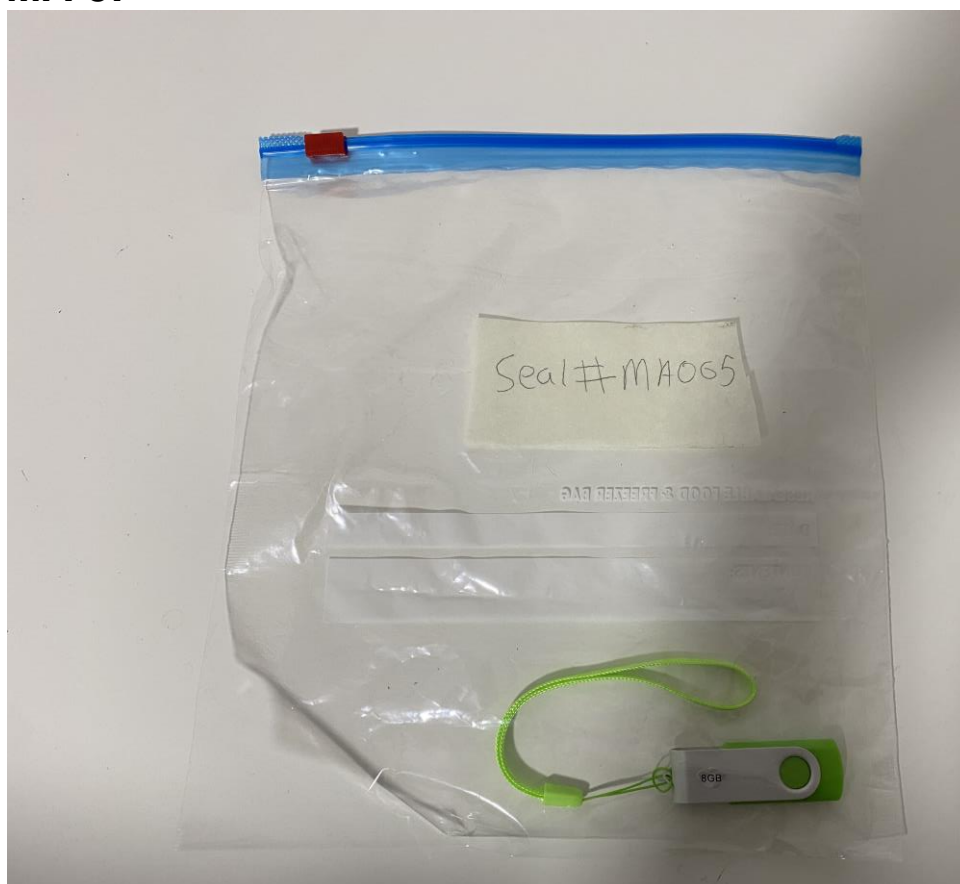
MA-3:



MA-4:



MA-5:



F. Exhibits record table

Zone	Item	Seized by	Time seized	Seal number	Exhibit reference
Bedroom Desk	Laptop	MA	10:00	Seal#MA001	MA-1
Bedroom Desk	Ipad	MA	10:05	Seal#MA002	MA-2
Bedroom Desk	Bottle of Cream	MA	10:15	Seal#MA003	MA-3
Bedroom Desk	Book	MA	10:25	Seal#MA004	MA-4
Bedroom Desk	USB device	MA	10:32	Seal#MA005	MA-5

The table above shows the items within a table view. This was done to record the items after the search and seizure is completed to ensure that the chain of custody is documented. By documenting the chain of custody for each item, it details who handled the item, when and where from. It also outlines the references for the item so that they can easily be found. The record table also provides a way to track all items collected from the scene, ensuring that nothing is misplaced or forgotten during the investigation process. The records table also detailed who seized the item which provides accountability if ever a situation arises where the item is misplaced or lost. The references allow for quick reference to identify the items of interest.

Project 3: Written Evidence and Opinion

Introduction

In the field of digital forensics, the ability to analyse digital evidence and provide clear, concise, and accurate reports is critical, especially when these reports are intended for legal proceedings. Project 3 focuses on developing and demonstrating these skills through the analysis of a provided forensic image file. This project involves conducting a thorough investigation based on specific questions posed by the Crown Prosecution Service (CPS) and producing an expert witness statement. The expert witness statement follows the MG11 format, commonly used in legal contexts to provide factual findings and expert opinions.

This project emphasizes the importance of dual tool verification, a standard practice in digital forensics to ensure the accuracy and reliability of forensic analysis. It also requires the articulation of complex technical information in a manner that is comprehensible to non-technical stakeholders, such as jurors and legal professionals.

Methodology

Step 1: Individual Analysis of the Provided Image File

- **Objective:** Conduct a comprehensive analysis of the forensic image file provided as part of the coursework.
- **Tools Used:** Utilize two different forensic analysis tools to ensure the reliability of the findings. These tools may include FTK Imager, Autopsy, or other industry-standard forensic software.
- **Procedure:**
 1. Load the provided image file into the first forensic tool.
 2. Perform a thorough analysis, including file system examination, keyword searching, and identification of significant artefacts.
 3. Document all findings, ensuring detailed notes are taken for each step of the analysis.
 4. Repeat the analysis using a second forensic tool to verify the initial findings.
 5. Compare the results from both tools to confirm the consistency and accuracy of the evidence identified.

Step 2: Answering CPS Questions

- **Objective:** Address specific questions provided by the CPS regarding the analysis of the forensic image.
- **Procedure:**
 1. Review the questions provided by the CPS, ensuring a clear understanding of what is being asked.

2. Refer to the documented findings from the analysis to answer each question accurately.
3. Provide detailed responses, supported by evidence from the forensic tools used.

Step 3: Producing an MG11-Style Statement

- **Objective:** Create an expert witness statement in the MG11 format, presenting the results of the analysis and the answers to the CPS questions.
- **Structure of the Statement:**
 1. **Introduction:**
 - Introduce yourself, including your qualifications and role as an expert witness in digital forensics.
 - Outline the purpose of the statement and the context of the investigation.
 2. **Analysis and Findings:**
 - Present the findings from the forensic analysis, structured in a clear and logical manner.
 - Include relevant technical details and evidence identified during the investigation.
 3. **Answers to CPS Questions:**
 - Address each question posed by the CPS, providing comprehensive and evidence-backed responses.
 4. **Expert Opinion:**
 - Offer your expert opinion based on the analysis and findings.
 - Ensure that the opinion is clearly distinguished from factual findings.
 5. **Conclusion:**
 - Summarize the key points of the statement.
 - Reiterate the reliability and thoroughness of the forensic analysis conducted.

WITNESS STATEMENT

CJ Act 1967, s.9; MC Act 1980, ss.5A(3) (a) and 5B; Criminal Procedure Rules 2020, Rule 16.2, 19.4

URN

HT

FU

1234

23

Statement of: Muhammad Irfan Ahmed B.Sc(Hons)Age if under 18: Over 18 (if over 18 insert 'over 18') Occupation: Digital Forensics Specialist

This statement (consisting of 9 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: Muhammad Irfan Ahmed Date: 8/12/2023**Qualifications and Experience**

1. I am employed as a Digital Forensics Specialist at Greenwich Police HiTech Forensics Unit (HTFU). I have worked in the field of Digital Forensics since 2022. I have Bachelor of Science degree in Computer Security and Forensics 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 HTFU in the case referred to as Operation Amsterdam Central.
4. I was not the person who imaged the original device (exhibit BXS/1), and for details relating to that please refer to the statement and notes of Mr. A. Aaron Adamson who is the imaging technician in this case. I however at the start of my examination performed a verification on the image that was supplied to me (called 'BXS-1.E01') and it was found to be correct.

RESTRICTED**Continuation of Statement of Muhammad Irfan Ahmed**

5. I have received instructions from the Crown Prosecution Service and have been asked to conducted an examination of the of the image file in order to consider the following questions:
- i) **Question 1:** Is there material of a personally identifying nature on exhibit BXS/1 for KOZINSKI, CRUYER, HARRINGTON, or any other person.
 - ii) **Question 2:** Is/or has there been, material on exhibit BXS/1 that relates to SAMSON.
 - iii) **Question 3:** Is/or has there been, material on exhibit BXS/1 that can be characterised as being related to Militant Veganism.
 - iv) **Question 4:** Are there details of any other offences recorded on exhibit BXS/1.
 - v) **Question 5:** In your opinion is the USB, exhibit BXS/1, the property of HARRINGTON as claimed by KOZINSKI, is it the property of KOZINSKI, is it the property of any other third party, or are you unable to make a determination.
6. 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).
7. 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

8. With respect to question 1, I found personal identifying material for Frank Harrington on Exhibit BXS/1, indicated by a CV linked to his name as well as a text file hidden within a jpeg file. No personal identifying material was conclusively found for Kozinski and Cruyer.
9. With respect to question 2, material on Exhibit BXS/1 related to Samson was identified, an image file titled 'Samson', and a text file that was hidden within a jpeg file.
10. With respect to question 3, the analysis revealed content related to Militant Veganism, including image files and text, suggesting an interest or involvement in these activities.

RESTRICTED

RESTRICTED**Continuation of Statement of Muhammad Irfan Ahmed**

11. With respect to question 4, I found images categorised as indecency as defined in the briefing. Additionally, screenshot images of conversations between two individuals suggests an intent to commit an act of violence against a person being discussed, though it cannot be explicitly confirmed without further context or investigation.
12. With respect to question 5, it is inconclusive whether Exhibit BXS/1 is the property of Harrington as claimed by Kozinski, is the property of Kozinski or the property of any other third party. The SID associated with the incriminating material suggests a link to Harrington, but a definitive ownership cannot be determined solely on this basis.

Detailed Findings for Exhibit BXS/1

13. The file 'BXS-1.E01' is the forensic image of the exhibit, which is a USB thumb drive device. The image contains the NTFS file system, is of 17.1GB size and my examination shows that the last recorded use of the device was on the 22nd November 2023.

Question 1: Is there material of a personally identifying nature on exhibit BXS/1 for KOZINSKI, CRUYER, HARRINGTON, or any other person.

14. With regards to Question 1, the evidence that linked with Frank Harrington was a docx file called \$RS13NPS, located in the recycle bin, and this included the name Frank Harrington within the contents of the file. The presence of this artefact could indicate potential ownership or usage of the device by the suspect Frank Harrington however with this artefact alone, it cannot be said conclusively whether Frank Harrington used or owned the device. The SID linked to the file is SID S-1-5-21-2466885413-8855001234-3844283957-1001 and this is also present within other artefacts found. The second piece of evidence found was a text file hidden within a jpeg file using steganography. The text file seemed to address Frank Harrington as I quote 'Enjoy yourself frank, make him pay'. This could suggest that the text file was addressed to Frank

RESTRICTED

RESTRICTED**Continuation of Statement of Muhammad Irfan Ahmed**

Harrington however without more conclusive evidence it cannot be said. There was an associated file that contained the password to unhide the text file from the jpeg file. A steganography tool called 'OpenPuff' was downloaded on the device and this was the very same tool used to unhide the artefact. The use of steganography here shows a conscious attempt to hide information that is identifiable which suggests that the user was aware of the implications of their actions.

Question 2: Is/or has there been, material on exhibit BXS/1 that relates to SAMSON.

15. With regards to Question 2, I identified an image file which was named Samson.jpg. The content of the jpeg file contained an image of a knife with the text 'Soon Piggie' written on the blade. The SID of the file was linked to S-1-5-21-2466885413-8855001234-3844283957-1001. The presence of this artefact could indicate a link to the individual Samson as shown by the title of the file however the presence of this artefact alone does not establish a strong connection to the specific individual. The second artefact found that links to Samson is the text file that was hidden within a jpeg file using steganography. The second sentence within the file appeared to be the home address for Mr Samson, this could be further substantiated by the fact the file is named 'address.txt', this method of concealing the address within an otherwise harmless file again points to a conscious effort to hide crucial information, possibly to evade detection. Also an image file was found within the recycle bin of Exhibit BXS/1 that was a street view of the address named within the text file, 'address.txt' and another file which was an aerial view of the address was identified. This file was hidden; the method used was to change the magic numbers to obscure the png file so that the content of the file does not open for view. The SID associated with the jpeg file that contained the text file was SID S-1-5-21-2466885413-8855001234-3844283957-1001 and this is consistent with the other artefacts found. The SID

RESTRICTED

RESTRICTED**Continuation of Statement of Muhammad Irfan Ahmed**

associated with the other files, the street view and aerial view of the address, were SID S-1-5-21-2466885413-8855001234-3844283957-1001 also.

Question 3: Is/or has there been, material on exhibit BXS/1 that can be characterised as being related to Militant Veganism.

16. There were multiple different artefacts found related to militant veganism and they were connected to SID S-1-5-21-2466885413-8855001234-3844283957-1001. There were four image files, two being jpg and two being png files which were related to veganism, with one of the png files labelled they_will_never_stop_the _militant_vegan_mindset_8_1350x0.png. The content of this file depicts three individuals standing with their back turned away from the camera with a banner edited into the image with a logo of different animals with the slogan 'They will never stop the vegan extremist mindset'. There was a jpg file that depicts a protest for veganism. The other png file depicts an individual holding a sign with the word 'vegan' written on it. The fourth image file depicts an individual standing within a water fountain with red smoke flare. The presence of these images on the USB device suggests the user with the SID S-1-5-21-2466885413-8855001234-3844283957-1001 had an interest in material related to militant veganism.

Question 4: Are there details of any other offences recorded on exhibit BXS/1.

17. With regards to Question 4, there were two artefacts found which relate to indecency as stated within the case brief. The image features a cat in a farm setting. Following the case brief's criteria, this image is categorised as 'indecency'. The second artefact found depicts various animals with the text 'Protect the Harvest'. This image includes a dog which would be classed as adult pornography and includes a cat which is classified as indecency as stated in the brief. The SID related to these artefacts was SID S-1-5-21-2466885413-8855001234-3844283957-1001.

RESTRICTED

RESTRICTED**Continuation of Statement of Muhammad Irfan Ahmed**

The presence of these images suggests interest in this topic area by the user with the SID S-1-5-21-2466885413-8855001234-3844283957-1001. Additionally, two screenshots of text messages between an individual named 'Brucie' and another unnamed party were found. The content of these messages raises concerns as they potentially suggest intent to commit an act of violence. Specifically, because of the message, in one of the screenshots, 'Follow the pig home, When he goes home for lunch to fill his face with flesh you know on the door, then knock on his fucking face'. This statement includes derogatory language and appears to incite a physical confrontation. The phrase 'then knock on his fucking face' could be interpreted as an explicit threat or encouragement of assault however without additional context or a thorough investigation, the intent behind these messages cannot be definitively determined. The second screenshot found between the two same people as the first appears that the context of the messages are about a third individual and their address, this is because of the messages 'so where does he live?' to which a reply was given 'not here, ill puff you the details. Same way as normal'. This raises concern as a text file was found with an address for 'Samson' an individual related to the investigation which was hidden using steganography. There was a steganography tool downloaded called 'OpenPuff' as explained in Question 1. The reply 'ill puff you the address' could be referring to the text file found hidden in an image file, 'a puff of wind' in which the text file contained an address. The explanation is given in question 2. The use of the word 'puff' could be a means of revealing the method of transferring of information between individuals, as 'puff' could refer to OpenPuff, however this cannot be conclusively said without fully understanding the context of the messages.

RESTRICTED

RESTRICTED**Continuation of Statement of Muhammad Irfan Ahmed**

Question 5: In your opinion is the USB, exhibit BXS/1, the property of HARRINGTON as claimed by KOZINSKI, is it the property of KOZINSKI, is it the property of any other third party, or are you unable to make a determination.

18. As a forensic expert, I have reviewed the contents of Exhibit BXS/1 and analysed the associated metadata. My findings are as follows: A PDF file mentioned within the brief was located on the USB device. The file's metadata, including creation and last modification dates, aligns with the timeline of events described. The SID associated with the file was S-1-5-21-4161078732-1123737313-172224672-1001. This SID was not associated with the artefacts found to be incriminating but is highlighted to show the connection to the brief and to the suspects. The suspect, Cruyer, stated she downloaded a PDF file and the PDF file found matches with the timeline from her statements. It could be argued that the SID associated with the PDF file is in fact Cruyer's however there is not any definitive evidence to say for certain as there is no identifiable information that directly links to Cruyer. The other artefacts were all linked to the SID S-1-5-21-2466885413-8855001234-3844283957-1001. There were two artefacts that had content identifiable to a suspect, the suspect in question being Frank Harrington and this artefact was linked to SID S-1-5-21-2466885413-8855001234-3844283957-1001. While this connection suggests potential ownership or use by Frank Harrington, it is not definitive proof of personal use without corroborative evidence directly linking the suspects to the act of using the USB or owning it.

Summary of Findings:

19. In summarising the examination of Exhibit BXS/1, key findings point to the involvement of Frank Harrington, as personal data and documents revealed through steganography show a link to the suspect, though this does not unequivocally establish ownership or direct use by the suspect, Frank Harrington. The SID S-1-5-21-2466885413-8855001234-3844283957-1001, associated

RESTRICTED

RESTRICTED**Continuation of Statement of Muhammad Irfan Ahmed**

with these findings, also corresponds to evidence of interest in militant veganism and materials classed as indecent. Messages found suggest a conspiracy to commit an act of violence, raising concerns about the user's intentions. Also the deliberate use of steganography and suggestive language in communications points to an effort to conceal information. The discovery of a steganography tool and its referenced use in text messages, particularly with the term 'puff' which may allude to 'OpenPuff', highlights a method of concealing and transferring information.. Contrarily, a PDF file associated with a different SID, S-1-5-21-4161078732-1123737313-172224672-1001, aligns with Cruyer's statement and the case timeline, yet definitive ownership remains unconfirmed due to lack of direct, identifiable links. Despite these findings, definitive ownership of Exhibit BXS/1 remains indeterminate, with different SIDs indicating multiple users, though the majority of incriminating evidence is associated with one user. This complexity highlights the need for further investigation to fully identify the roles of the individuals involved.

Disclosure

20. 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.
21. In the event my opinion changes on any material issue, I will inform the investigating officer as soon as reasonably practicable and give reasons.

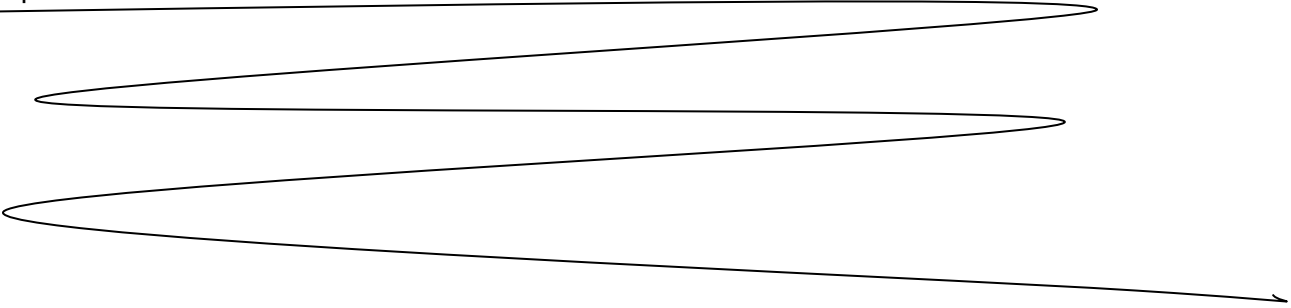
Duty to the Court

22. 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.

RESTRICTED

RESTRICTED**Continuation of Statement of Muhammad Irfan Ahmed**

23. 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. Muhammad Irfan Ahmed

**RESTRICTED**