

|  |
| --- |
| Court Report : John Doe Case  Snow White – [2302444@uad.ac.uk](mailto:2302444@uad.ac.uk)  Kieran Bissett –  Annie Place –  Digital Forensics 1 – CMP209  BSC Ethical Hacking Year 2 2023/2024 |

*Information contained in this document is for educational purposes.*

|  |  |  |
| --- | --- | --- |
| **Group Member Name** | **Student Number** | **Worked on Section?** |
|  |  |  |

|  |  |
| --- | --- |
| **JOINT REPORT of**  **First Analyst: Snow White**  **Second Analyst: Kieran Bissett**  **Third Analyst: Annie Place**  **Unit name and Force: Digital Forensic Unit of 3ensic Force**  **Case against: John Doe**  **Police Reference No: (if applicable)**  **Case Reference No: (CCU or equivalent ref)**  **PF Reference No: (if applicable)** | A logo of a person's face and a fingerprint  Description automatically generated |

Contents

[1 Introduction 1](#_Toc161266578)

[1.1 Description of Crime 1](#_Toc161266579)

[2 Description of investigation 2](#_Toc161266580)

[2.1 Job Description and Instructions 2](#_Toc161266581)

[2.2 Description of Recovered/Examine items 2](#_Toc161266582)

[2.3 Analysis Methodology 3](#_Toc161266583)

[2.3.1 Disk Imaging 3](#_Toc161266584)

[2.3.2 Physical Searching 3](#_Toc161266585)

[2.3.3 Disk Analysis 3](#_Toc161266586)

[2.3.4 Autopsy 3](#_Toc161266587)

[2.3.5 File Carving 3](#_Toc161266588)

[2.3.6 Images 3](#_Toc161266589)

[2.3.7 Communications 3](#_Toc161266590)

[2.3.8 Recent documents 3](#_Toc161266591)

[2.4 Analysis 4](#_Toc161266592)

[2.4.1 Disk Analysis 4](#_Toc161266593)

[2.4.2 Summary of Partition Table 4](#_Toc161266594)

[2.4.3 Registry 4](#_Toc161266595)

[2.4.4 Browsing History 4](#_Toc161266596)

[2.4.5 Bookmarked History 4](#_Toc161266597)

[2.4.6 Downloaded Files 4](#_Toc161266598)

[2.4.7 Audio/Videos 4](#_Toc161266599)

[2.4.8 Emails 4](#_Toc161266600)

[2.4.9 Documents 4](#_Toc161266601)

[2.4.10 Emails 4](#_Toc161266602)

[2.4.11 Images 4](#_Toc161266603)

[2.5 Production List and Associated Description 5](#_Toc161266604)

[3 Conclusions 6](#_Toc161266605)

[4 Contributions 7](#_Toc161266606)

[5 Equipment Required for court proceedings 8](#_Toc161266607)

[6 Glossary 9](#_Toc161266608)

[References 10](#_Toc161266609)

[Appendices 11](#_Toc161266610)

[Appendix A - Images 11](#_Toc161266611)

[Appendix B 11](#_Toc161266612)

[Appendix C 11](#_Toc161266613)

# Introduction

## Description of Crime

# Description of investigation

## Job Description and Instructions

The Digital Forensic Unit of 3esnic has been approached by the University of Abertay in conjunction with Police Scotland to investigate into Mr John Doe, an individual who has been accused of the crimes Ornithological Misconduct, Bird Abuse, Possession of Indecent Bird-Related Imagery and Possession with Intent to Distribute Indecent Bird-Related Imagery. This will come in the form of a digital forensic examination of the alleged offender’s personal devices.

The 3esnic team is comprised of 3 investigators Snow White, Kieran Bissett and Annie Place will be the primary analysts working on the personal devices looking for images and videos of bird abuse. However, all bird related content will be recorded for the record examples like browser search history, internet messaging relating to the procurement or the distribution of bird images and other documents that may provide evidence relevant to the investigation.

Prior to the report being written which will serve as a report for the court to deliberate over, all necessary information was passed on to the relevant teams either to ensure a thorough and well-informed investigation or to make sure any victims receive help they may need.

## Description of Recovered/Examine items

The 3ensic forensic team were called out to the suspects' home to document and collect any digital evidence to then be taken back to the lab to be further analyzed.

The team found a PC which was turned off with an external HDD hard drive connected which was documented in the chain of evidence form and then bagged to be taken back to the lab to be analyzed in a forensic safe environment.

See Appendices A for images of HDD drive.

When the drive was taken back to the lab it was copied using

It was also partitioned to see what space was unallocated on the drive and to see what file system it was using.

By doing the partitioning it was found out that this drive has 3 partitions, the primary partition is known as 002 which is formatted in the NTFS/exFat format and is xx in size.

## Analysis Methodology

### Disk Imaging

### Physical Searching

### Disk Analysis

### Autopsy

### File Carving

### Images

### Communications

### Recent documents

## Analysis

### Disk Analysis

### Summary of Partition Table

### Registry

### Browsing History

### Bookmarked History

### Downloaded Files

### Audio/Videos

### Emails

### Documents

### Emails

### Images

## Production List and Associated Description

# Conclusions

# Contributions

**Kieran**

**Annie**

**Snow**

# Equipment Required for court proceedings

For the findings of this report to be presented to the court, the following equipment is required:

**Hardware:**

* Computer that has internet access, which can run various tools.
* A display device which is of adequate size which has an HDMI port (this can be a monitor, projector, or television.)
* HDMI Cable
* Any relevant power cables.
* The image of the John Doe drive
* A keyboard
* And a mouse.

**Software:**

* A Linux-based operating system(the analysts used Debian-based operating systems such as Ubuntu or Kali Linux for the case.)
* Microsoft Windows Operating System
* Autopsy/Sleuth Kit
* Md5 hash command line feature
* Foremost
* Metacam
* Forensic Registry Editor (FRED)
* OSFMount

# Glossary

# References

# Appendices

## Appendix A - Images

## Appendix B

## Appendix C