

# Digital Forensic Investigation Report

12842713

AHMED RASHWAN

## Introduction

This report examine the USB evidence file provided "Animal.E01 which covers the steps taken to ensure the evidence has been preserved, examined, and analysed, according to the digital forensic principles and guidelines. The objective is to investigate if the suspect James Jones "Animalman" has been selling illegal animals.

## Objectives of conducting the investigation

The final objective is to determine if the suspect James Jones with alias "Animalman" is involved in the illegal selling of animals.

## Deliverables

After investigating the case at hand, the result is that the USB image that was given for investigation has a direct link with a website selling illegal animals, the email times and dates to and from James Jones. (animalman@lotmail.com) and its earliest creation times.

## Contents

Introduction .....	1
Objectives of conducting the investigation .....	1
Deliverables.....	1
Methodology.....	3
Collection Stage .....	3
Investigation Warrant .....	4
Original File Location.....	4
Preservation of the original file .....	5
Acquired Image File Summary .....	5
Hash generated before investigation. ....	6
Examination Stage .....	6
Tools Used Throughout Investigation .....	6
Investigation.....	6
Analysis Stage.....	9
Reporting stage .....	9
Recommendation.....	9
References .....	9
Appendix A : Chain of custody .....	10

## Table of figures

Figure 1: Investigation Warrant .....	4
Figure 2: original download image file location.....	4
Figure 3: preservation in cloud using OneDrive.....	5
Figure 4: acquired image file from the copy.....	5
Figure 5: Integrity check before investigation .....	6
Figure 6: email between Bob and Animalman.....	7
Figure 7: Main index page with the private section where animals are sold. ....	7
Figure 8: private page found in metadata .....	7
Figure 9: private.html page.....	8
Figure 10: images of caged, exotic, and illegal stock animal images.....	8
Figure 11: first email to Animalman welcoming animal to their new email mentioning their username and password.....	8
Figure 12: Chain of custody form Part 1 .....	10
Figure 13: Chain of custody form Part 2 .....	11

## Methodology

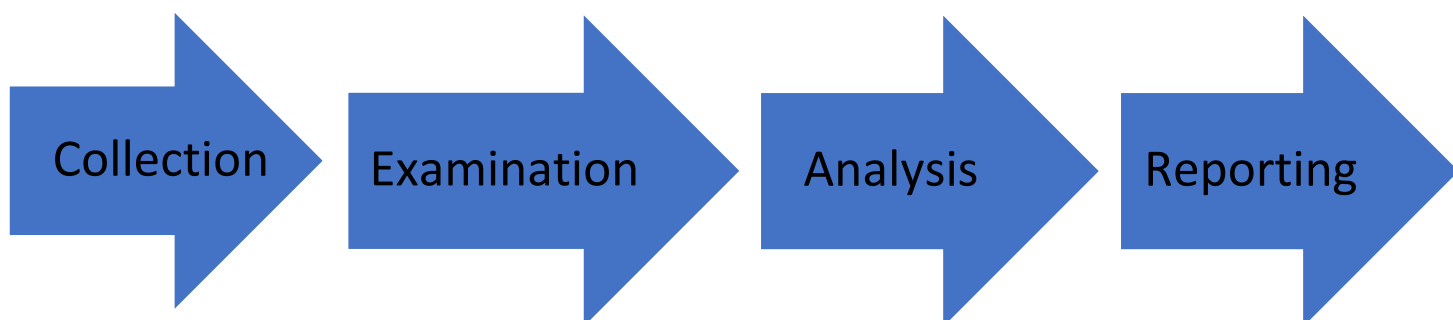
This report follows the NIST (National Institute of Standards and Technology) 800-86 framework which breaks down into 4 steps (collection, examination, analysis, reporting).

During the collection phase, digital evidence is collected, and preserved for analysis. This stage includes taking a forensic copy of the digital evidence and verifying its integrity as well as documenting the steps in a chain of custody form. (Kent et al., 2006)

In the second stage of the digital forensic methodology, this stage is known as the examination stage, which involves examining and extracting the relevant pieces of information and adding figures of the pieces of evidence found. (Kent et al., 2006)

The third stage of the methodology known as analysis is to analyse the evidence gathered from the collection and examination stage and draw out appropriate conclusions based on the analysis of the evidence. (Kent et al., 2006)

The final stage of the 4-step methodology from NIST is the reporting stage and this is where the evidence is reported and presented with the conclusions drawn from the previous stage. This stage also includes giving recommendations on how to prevent this from happening in the future as well as any further actions to be taken. (Kent et al., 2006)



### Collection Stage

The collection stage involves the steps taken to collect the evidence this includes the warrant investigation, the original file's location, the preservation of the original file, acquiring an image of the copy of the original file using FTK imager and finally maintaining integrity using HashCalc.

## Investigation Warrant

This document is for Coventry University students for their own use in completing their assessed work for this module and should not be passed to third parties or posted on any website. Any infringements of this rule should be reported to [facultyregistry.eee@coventry.ac.uk](mailto:facultyregistry.eee@coventry.ac.uk).

Faculty of Engineering, Environment and Computing

Coventry University

4060CEM Digital Forensics Fundamentals

Assignment Brief

Module Title: Digital Forensics Fundamentals	Individual	Cohort (Sept)	Module Code 4060CEM
Coursework Title: Coursework			Hand out date: 16/01/2023
Lecturer: Musa Muhammad			Due date and time: 10/4/2023 at 18:00
Word Limit: 1000 words	Coursework type: Report		100% of Module Mark
Submission Arrangement: Online via Aula			
File types: Word or PDF files			
Mark and Feedback Date: 24/04/23 (electronic via Aula)			

**Module Learning Outcomes Assessed:**

1. Apply good practice to the capture of digital evidence, based on published rules and guidelines.
2. Select appropriate methods and tools for forensic capture and investigation of digital evidence.
3. Write a report based on standards for forensic investigation.

**Task and Mark distribution:**

In this assignment you are required to analyse a case at hand. You are expected to examine the evidence file (Animal.E01) provided in Aula in accordance with digital forensic principles and guidelines. Then, write a report that addresses the necessary steps to ensure that the digital evidence is preserved, examined and analysed. In your findings you should determine whether or not the USB device has any connection to a web site concerned with the sale of animals, device contains images of animal stock that maybe considered illegal pets. In addition, the email times and dates to and from James Jones. (animalman@lotmail.com) and earliest creation times and dates of image files

To ensure that you have achieved the learning outcomes, you are required to include your findings and recommendations following the steps below.

Task 1:

- Discuss and Justify the forensic investigation methodology you have adopted and apply each step in the remaining tasks (20 Marks)
- The steps you have taken to ensure proper chain of custody for the evidence, the tools used for the investigation and the processes you have followed to preserve the evidence (20 Marks)
- The findings you have made in identifying the evidence and what evidence you have found

Figure 1: Investigation Warrant

## Original File Location





Search Results in Downloads				
Name	Date modified	Type	Size	
 4060CEM Assignment Brief (3)	06/04/2023 11:09	Microsoft Word D...	41 KB	
▼ Earlier this week				
 4060CEM Assignment Brief (2)	03/04/2023 13:12	Microsoft Word D...	41 KB	
▼ Last week				
 Sample-Chain-of-Custody-Form	28/03/2023 12:18	Microsoft Word D...	28 KB	
▼ Last month				
 AnimalE01	23/03/2023 09:52	E01 File	29,898 KB	

Figure 2: original download image file location

# Preservation of the original file

My files

	Name	Modified	Modified By	File size	Sharing
	Attachments	March 23	Ahmed Rashwan	0 items	Private
	CW2-Networking-Portfolio	February 23	Ahmed Rashwan	4 items	Shared
	Portfolio4_Networking	Sunday at 12:50 PM	Ahmed Rashwan	3 items	Private
	Preserving_of_evidence_animal...	March 23	Ahmed Rashwan	1 item	Private
	40060CEM-Investigation-Chain-of-Custody...	Tuesday at 12:18 PM	Ahmed Rashwan	33.7 KB	Private

More details

Type  
Folder

Modified  
3/23/2023 10:03 AM

Path  
Ahmed Rashwan > Documents > Preservin  
g\_of\_evidence\_animal.E01

Size  
29.2 MB

Figure 3: preservation in cloud using OneDrive

## Acquired Image File Summary

```
Created By AccessData® FTK® Imager 3.1.2.0
Case Information:
Acquired using: ADI3.1.2.0
Case Number: 001
Evidence Number: 001
Unique description: disk image to be used to acquire evidence
Examiner: Ahmed Rashwan
Notes: disk image to investigate
-----
Information for C:\Users\Ahmed\Desktop\Investigation\Animal_Investigation_Created-Image\InvestigateAnimal:
Physical Evidentiary Item (Source) Information:
[Device Info]
Source Type: Logical
[Verification Hashes]
MD5 verification hash: c00fd4ce8d3b7145243fab14fe608ef1
SHA1 verification hash: 1205eb6f1ca7db056e9b2456d6e50241b31b4ed8
[Drive Geometry]
Bytes per Sector: 512
Sector Count: 2,015,231
[Image]
Image Type: E01
Case number: Peters Case
Evidence number: animal
Examiner: Bhishak Pankhania
Notes:
Acquired on OS: Windows 7
Acquired using: 6.19.7
Acquire date: 07/02/2014 14:12:33
System date: 07/02/2014 14:12:33
Unique description: animal
Source data size: 583 MB
Sector count: 2015231
[Computed Hashes]
MD5 checksum: c00fd4ce8d3b7145243fab14fe608ef1
SHA1 checksum: 1205eb6f1ca7db056e9b2456d6e50241b31b4ed8
Image Information:
Acquisition started: Thu Mar 23 10:38:48 2023
Acquisition finished: Thu Mar 23 10:38:52 2023
Segment list:
C:\Users\Ahmed\Desktop\Investigation\Animal_Investigation_Created-Image\InvestigateAnimal.E01
Image Verification Results:
Verification started: Thu Mar 23 10:38:52 2023
Verification finished: Thu Mar 23 10:38:56 2023
MD5 checksum: c00fd4ce8d3b7145243fab14fe608ef1 : verified
SHA1 checksum: 1205eb6f1ca7db056e9b2456d6e50241b31b4ed8 : verified
```

Figure 4: acquired image file from the copy.

Hash generated before investigation.

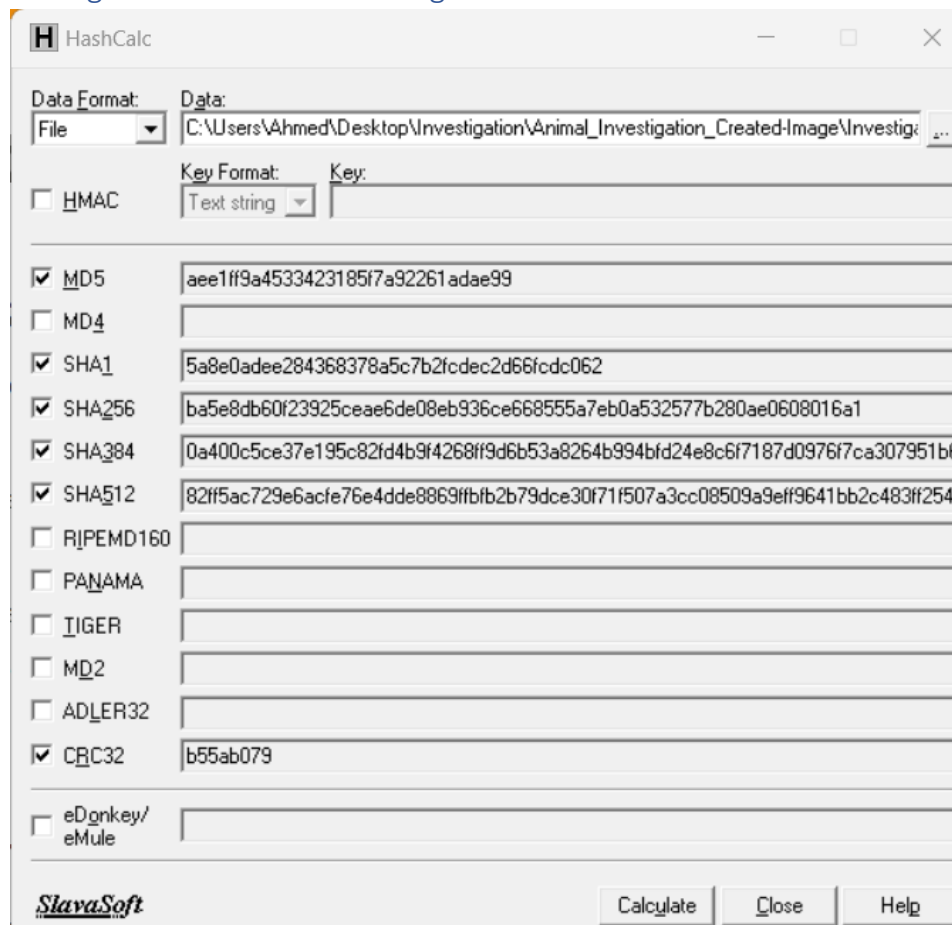


Figure 5: Integrity check before investigation

## Examination Stage

This stage of the investigation is used to show the steps taken throughout the investigation and find out evidence on suspect James Jones with alias Animalman related to the illegal selling of animals as well as the tools used to achieve this.

### Tools Used Throughout Investigation

- FTK Imager for acquiring the evidence.
- Autopsy for examination of the evidence.
- Microsoft Word for presentation and writing of the report.
- Snipping tool to obtain screenshots to add to the report.
- HashCalc to obtain the hashes and the integrity before and after the investigation.
- Microsoft OneDrive to preserve the evidence in the cloud.

### Investigation

Using Autopsy, the email communication between the buyer named Bob and the seller is found and this is where Animalman is pointing Bob to go to the private section of his website where all the animals are being sold on Wednesday and will be up for 20 minutes as shown in [figure 6](#).

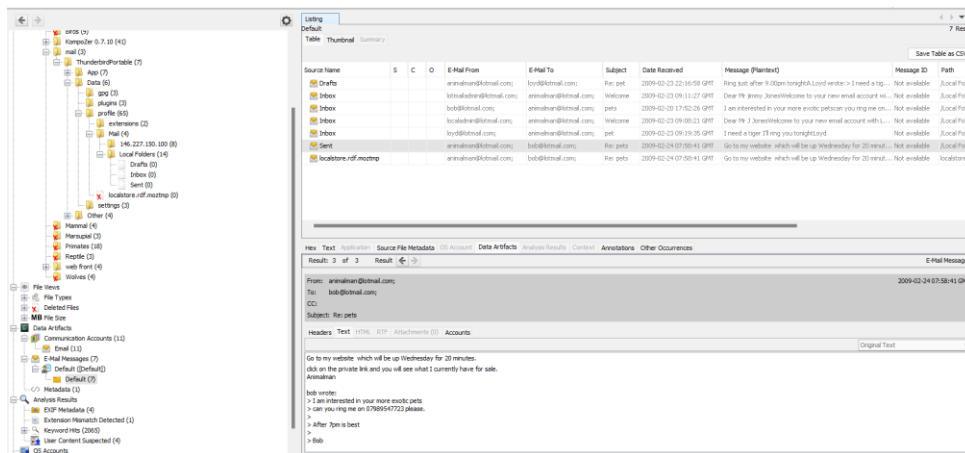


Figure 6: email between Bob and Animalman

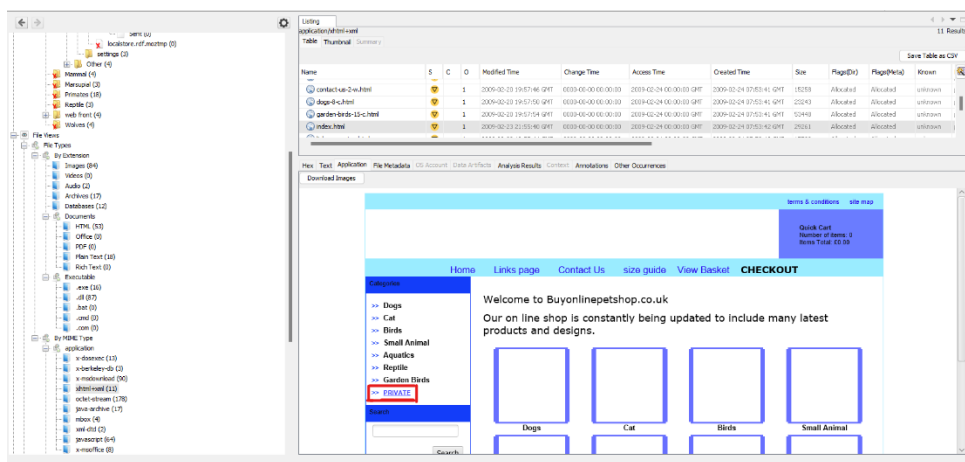


Figure 7: Main index page with the private section where animals are sold.

This is the private section where Animalman told Bob to go to and when the site will go live this is where the animals are being sold.

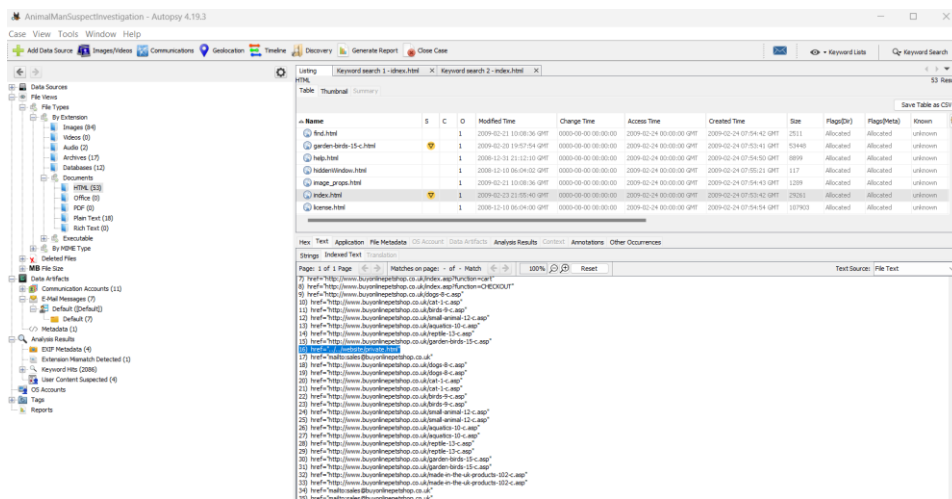


Figure 8: private page found in metadata

This is where the private html page was found in the metadata of the index page.



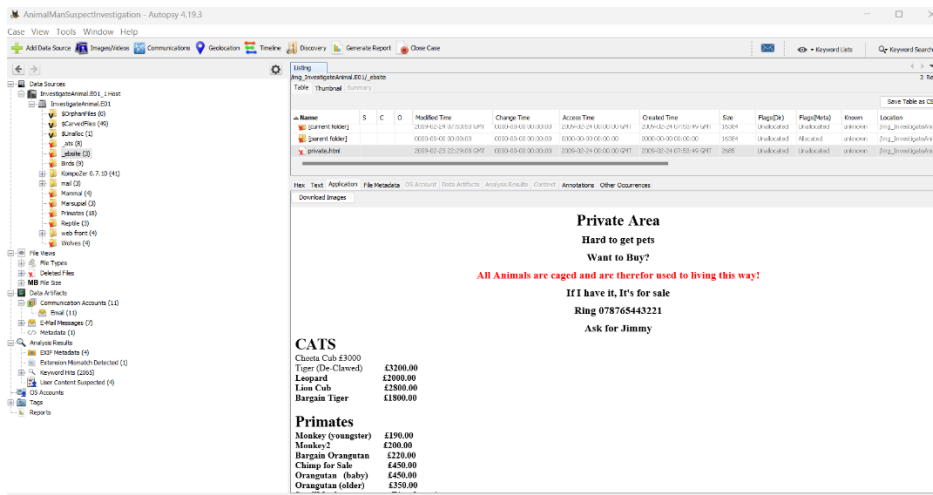


Figure 9: private.html page

This is the private page that was found which is where Animalman (James Jones / Jimmy Jones is selling the animals to the buyers such as Bob)

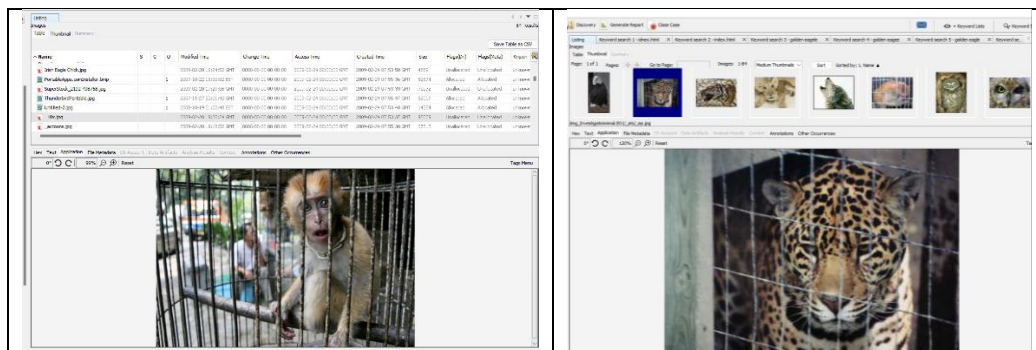


Figure 10: images of caged, exotic, and illegal stock animal images

The earliest creation time of the [Animalman@lotmail.com](mailto:Animalman@lotmail.com) email was found where it was setup by [localadmin@lotmail.com](mailto:localadmin@lotmail.com) on 23<sup>rd</sup> of February 2009 at 09:08:21 GMT in localadmin's email to Jimmy Jones also known as James Jones welcome email, this is shown in [figure 11](#).

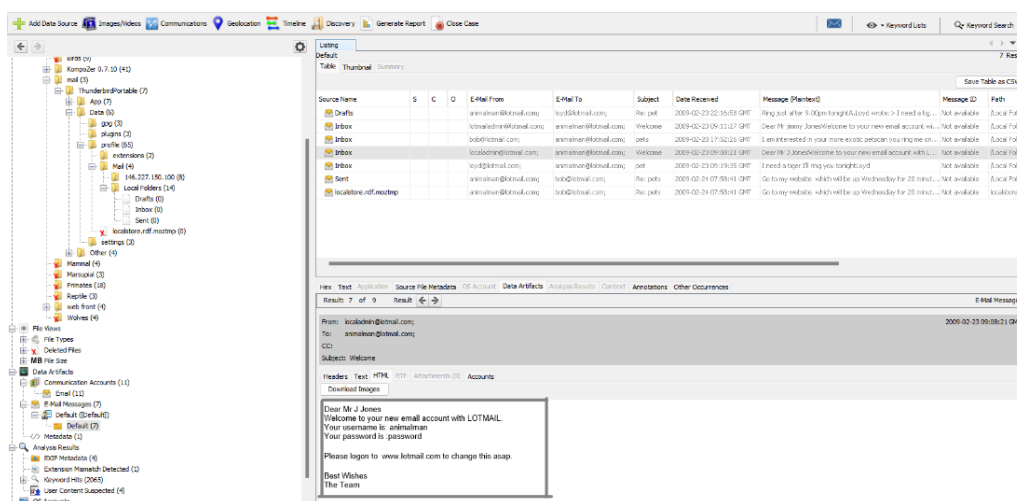


Figure 11: first email to Animalman welcoming animal to their new email mentioning their username and password

## Analysis Stage

During the previous examination phase the original email between Bob who was interested in the exotic animals that Animalman had to offer, the reply from Animalman mentioned that his website will be up on Wednesday for 20 minutes and that during this time the private area on his website will contain all the animals he is selling as shown from *figures 6 to 11* this means that after animalman told Bob to visit his website where all the animals and different sizes of cages are sold.

## Reporting stage

After carefully investigating Animalman on the suspicion of the USB image having been related to the selling of illegal and exotic animals, it is clear that based on the concrete evidence that was found that James Jones (Animalman) is guilty of selling animals without a proper license which is a violation of the Animal Welfare Regulations 2018 and means that James Jones is liable for imprisonment for up to six months, a fine or both<sup>(Gov.uk, 2018)</sup>.

Based on the Animal Welfare Act 2006, James Jones (Animalman) has violated the following sections of the Animal Welfare Act 2006. Section 4 (unnecessary suffering) for making the animals suffering by tying them up with rope or being caged up as found from the evidence that was collected during the investigation and section 13 (Licensing or registration of activities involving animals)<sup>(Gov.UK, 2006)</sup>, for the selling of animals without an appropriate license.

## Recommendation

It is recommended that a follow up investigation is conducted to determine the entire extend of the crime James Jones has committed and what are the appropriate fines / length of imprisonment for the crimes and illegal activities as well as monitoring the individual by the appropriate legal authorities to ensure that no such activities are carried out again without the proper licensing and legal requirements.

## References

Gov.UK. (2006). *Animal Welfare Act 2006*. Legislation.gov.uk.

<https://www.legislation.gov.uk/ukpga/2006/45/contents>

Gov.uk. (2018). *The Animal Welfare (Licensing of Activities Involving Animals) (England)*

*Regulations 2018*. Legislation.gov.uk.

<https://www.legislation.gov.uk/ukdsi/2018/9780111165485>

## Appendix A : Chain of custody

Property Record Number:

Anywhere Police Department

### EVIDENCE CHAIN OF CUSTODY TRACKING FORM

**Case Number:** 001

**Offense:** Suspected of illegal selling of animals

**Submitting Officer (Name/ID#):** Ahmed

**Supervisor:** Dr. Musa Muhamed

**Victim:** endangered animals

**Suspect:** James Jones (animalman)

**File Being Investigated:**

**InvestigateAnimal MD5:** aee1ff9a4533423185f7a92261adae99

**InvestigateAnimal Sha256:** ba5e8db60f23925ceae6de08eb936ce668555a7eb0a532577b280ae0608016a1

**CRC32:** b55ab079

Chain Of Custody					
Item	Date	Time	Description	Investigator	Comments
Animal.E01	23-03-23	09:52	Image file	Ahmed Rashwan	Downloaded the image file from Aula to my local downloads folder
Animal.E01	23-03-23	10:06	Image File	Ahmed Rashwan	Uploaded the downloaded image to a OneDrive folder to maintain preservation. <a href="https://livecoventryac-my.sharepoint.com/:u/g/personal/rashwana2_uni_coventry_ac_uk/EtUMyakw68luXSR98VozwW8duhZc28Hb90Jdx57dhwfe-VEH13">https://livecoventryac-my.sharepoint.com/:u/g/personal/rashwana2_uni_coventry_ac_uk/EtUMyakw68luXSR98VozwW8duhZc28Hb90Jdx57dhwfe-VEH13</a>
Animal.E01	23-03-23	10:11	Image File	Ahmed Rashwan	Copy and pasted the file located in my downloads folder into a folder called investigation in my desktop
Animal.E01	23-03-23	10:17	Image File	Ahmed Rashwan	Renamed the image file inside of my investigation folder to "AnimalCopy.E01"
InvestigateAnimal.E01	23-03-23	10:38	Image File	Ahmed Rashwan	Opened and used FTK imager to create a disk image out of the AnimalCopy.E01 file in my investigations folder and stored the created disk image under a sub-folder called "Animal_Investigation_Created-Image" folder
Screenshot_1_drive_verify_results_ftklmager.png	23-03-23	10:42	Image File	Ahmed Rashwan	Took a screenshot of results from Drive/Image verify results and saved it in "Screenshot_1_drive_verify_results_ftklmager"
hashcalc_snapshot_before_investigation.png	28-03-23	11:33	Hashes from hashcalc	Ahmed Rashwan	Took a screenshot of the hashes calculated from hashcalc for the created image
AnimalManSuspectInvestigation.aut	28-03-23	12:04	Created autopsy case	Ahmed Rashwan	Created autopsy case to look for evidence of the created image file
Webpage_evidence01.png	06-04-23	10:05	Screenshot of private.html	Ahmed Rashwan	Found and screenshotted private.html file and saved in C:\Users\Ahmed\Desktop\Investigation\Animal_Investigation_Created-Image\Snapshots\evidence
email_evidence01.png	06-04-23	10:21	Email evidence	Ahmed Rashwan	An email showing localadmin has activated James Jones email ( <a href="mailto:animalman@lotmail.com">animalman@lotmail.com</a> ) and has provided the username as animalman and its password
email_evidence02.png	06-04-23	10:30	Email evidence	Ahmed Rashwan	Email showing that James Jones is using a fake name called "Jimmy" with <a href="mailto:localadmin@lotmail.com">localadmin@lotmail.com</a>
email_evidence03.png	06-04-23	10:34	Email evidence	Ahmed Rashwan	Inbox email coming to animalman from a buyer <a href="mailto:bob@lotmail.com">bob@lotmail.com</a> saying he is interested on more exotic pets
email_evidence04.png	06-04-23	10:38	Email evidence	Ahmed Rashwan	animalman replied to bob mentioning that his website will be up on Wednesday for 20 minutes and told bob to click on the private link where the animals he has for sale are being sold.
stockImage_evidence01.png	06-04-23	11:47	Image evidence	Ahmed Rashwan	An illegal stock image of a monkey being roped up and strangled screenshotted and saved
stockImage_evidence02.png	06-04-23	11:59	Image evidence	Ahmed Rashwan	An illegal stock image of a monkey being chained from the neck and locked in a caged

Figure 12: Chain of custody form Part 1

Chain Of Custody					
Item	Date	Time	Description	Investigator	Comments
stockImage_evidence03.png	06-04-23	12:01	Image evidence	Ahmed Rashwan	Illegal stock image of a Caged eagle
stockImage_evidence04.png	06-04-23	12:13	Image evidence	Ahmed Rashwan	Illegal stock image of a chained up and captive orangutan
stockImage_evidence05.png	06-04-23	12:16	Image evidence	Ahmed Rashwan	Illegal stock image of 2 caged macaws
Webpage_evidence02.png	06-04-23	12:29	Image evidence	Ahmed Rashwan	The private area shown in the index.html page where all the illegal caged up animals are being sold by animalman and where the buyers will go to purchase the animals, they want
email_creation_time_evidence01.png	06-04-23	13:07	Email evidence	Ahmed Rashwan	Metadata showing the earliest creation time of the <a href="mailto:animalman@lotmail.com">animalman@lotmail.com</a> email made by <a href="mailto:localadmin@lotmail.com">localadmin@lotmail.com</a>
Webpage_evidence03.png	07-04-23	13:30	Webpage evidence	Ahmed Rashwan	Found the link to the private.html page
stockImage_evidence05.png	07-04-23	13:42	Webpage evidence	Ahmed Rashwan	Found exotic stock image of the animal leopard
hashcalc_snapshot_after_investigation.png	08-04-23	02:14	Hashcalc snapshot	Ahmed Rashwan	Took a screenshot of the investigateAnimal.E01 file that was created at the start of the investigation to check that integrity was maintained and that the image is unchanged

Figure 13: Chain of custody form Part 2