CASE STUDY

Computer Forensics

Kyle Chew Jing Khye
10362396
Jchew0@our.ecu.edu.au

Contents

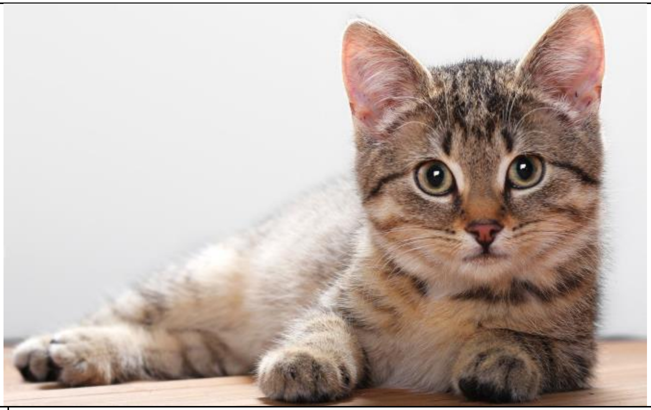
Summary

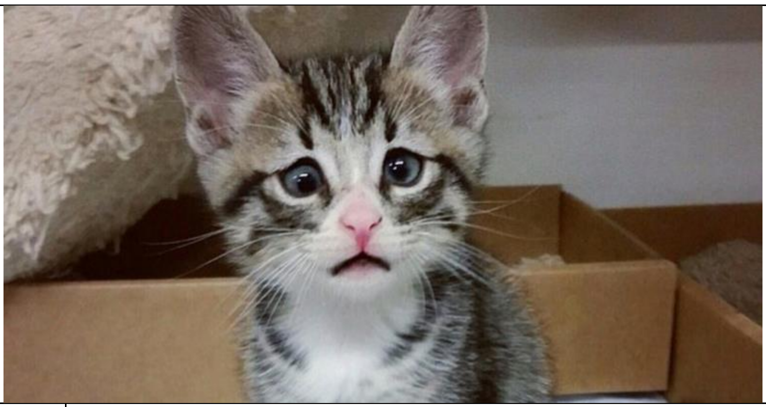
The purpose of this report is to investigate the machine that Clark Kent used in order to find data that is relating to cats, identify the owner of the materials found and figure out if the owner is viewing these materials deliberately based on how many files relating to cats there are and what are the software installed in the system during the investigation. The report will record all actions that was taken to investigate the case study in the running sheet and a chronological order of events that took place in the machine that was illegal in appendix B.

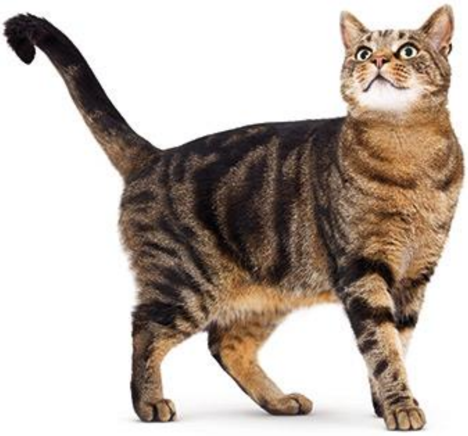
Presentation of content relating to offence

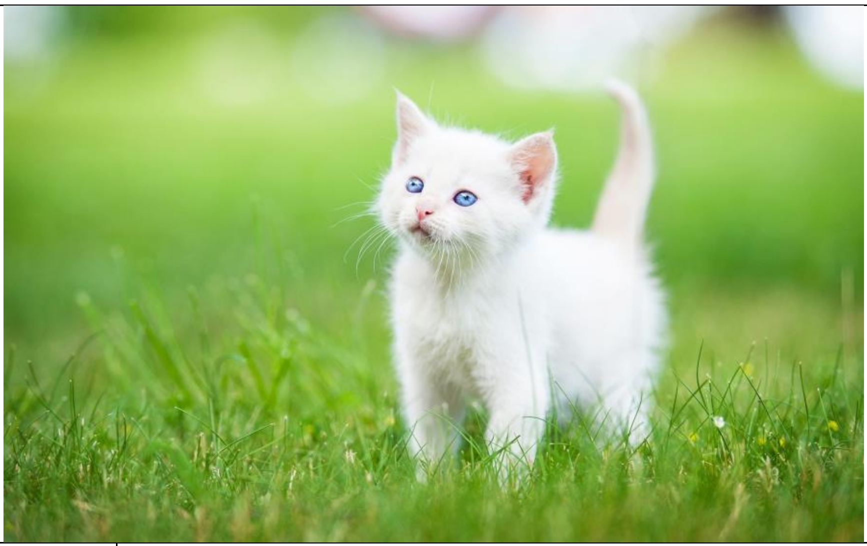
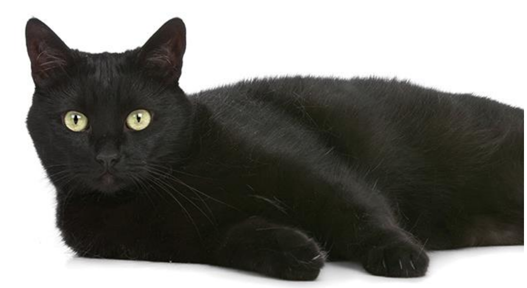
Pictures

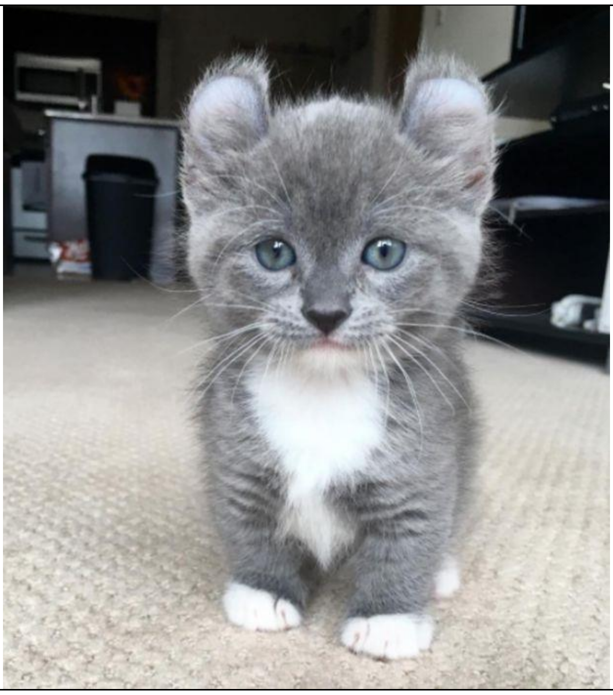
During the exploration of the folder and directories on the machine documents I managed to find a zip file named *thestuff.zip* containing 7 pictures of cats on the document file located in the directory */users/computer/documents*. Other than that ,11 additional cat pictures were also found in the directory /users/computer/pictures. The picture found on the system are images relating to illegal content that ranges from kittens to adult cats. What value this images holds to the investigation is since it's in a zipped folder, it is highly possibly that it is used to send it to another individual. Based on the time and date of the images, they were most probably downloaded together. Each of the evidence means that Clark Kent has possession of illegal material relating to cats since the material were found on his computer system.

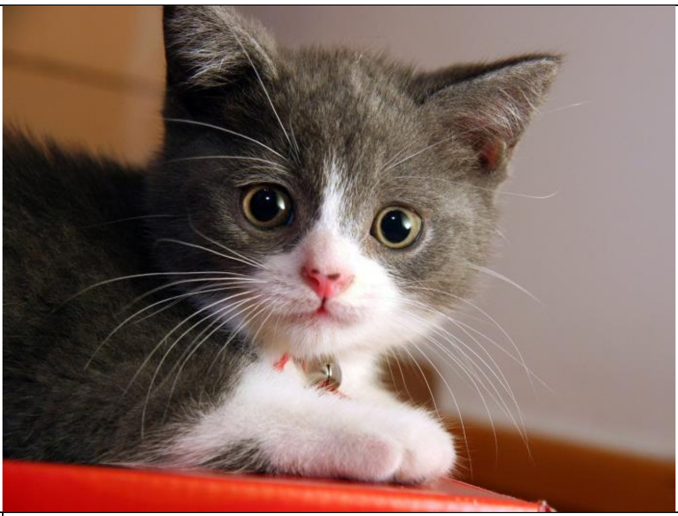
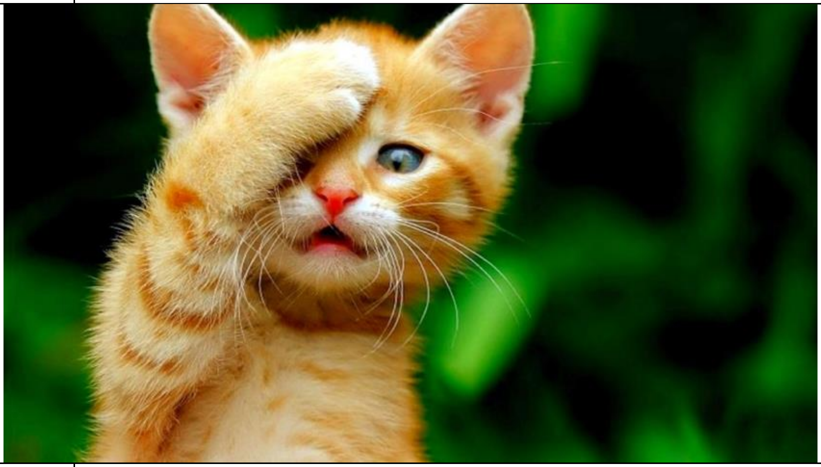
	
File Name	cat_03.jpg
Type	JPEG
Location	/img_2017-B.dd/Users/computer/Pictures/
Status	Allocated
MD5	53f8484efb0fbbeaf6cf0983e0424e07
Accessed	2017-06-12 13:00:06 AWST
Created	2017-06-12 13:00:06 AWST
Changed	2017-06-12 13:00:06 AWST
Sectors	1116110 - 1116260
Analysis	Brown adult cat laying down on a wooden floor

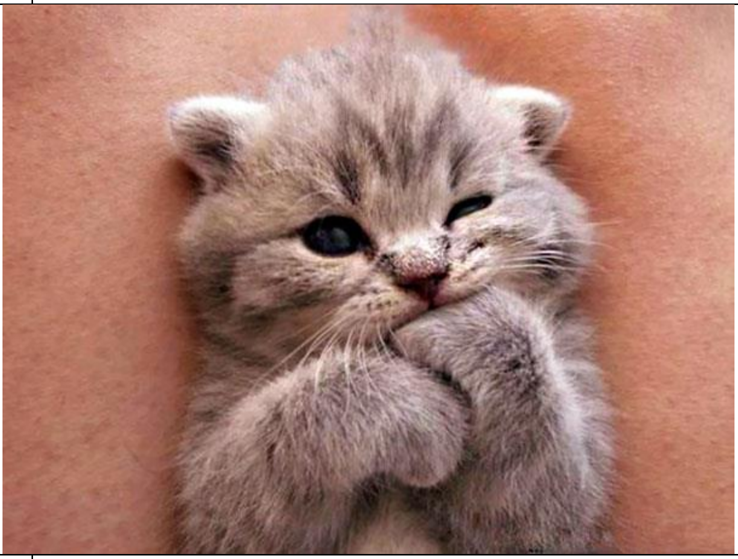
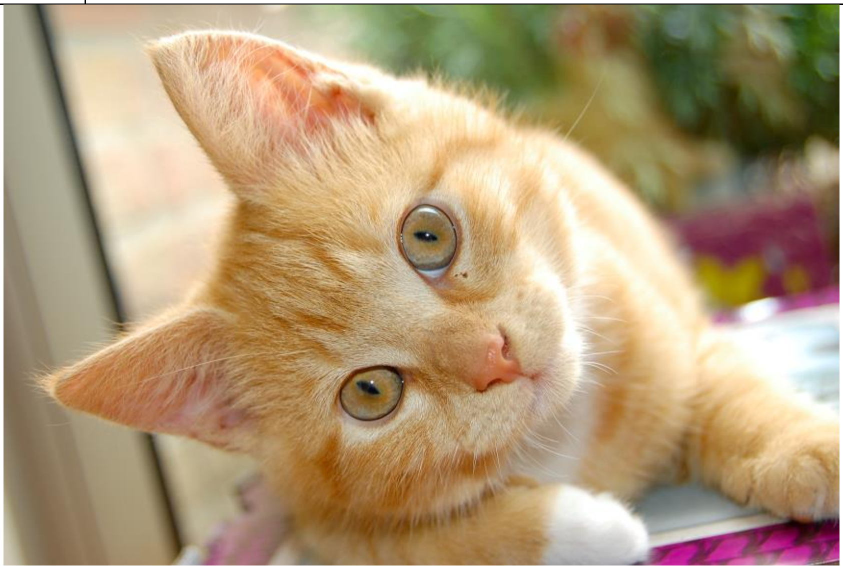
	
File Name	cat2.jpg
Type	JPEG
Location	/img_2017-B.dd/Users/computer/Pictures/
Status	Allocated
MD5	096254b20f79b6728384a54dbba69ea1
Accessed	2017-06-14 07:42:17 AWST
Created	2017-06-14 07:42:17 AWST
Changed	2017-06-14 07:42:17 AWST
Sectors	1119625- 1119654
Analysis	Brown kitten inside a box

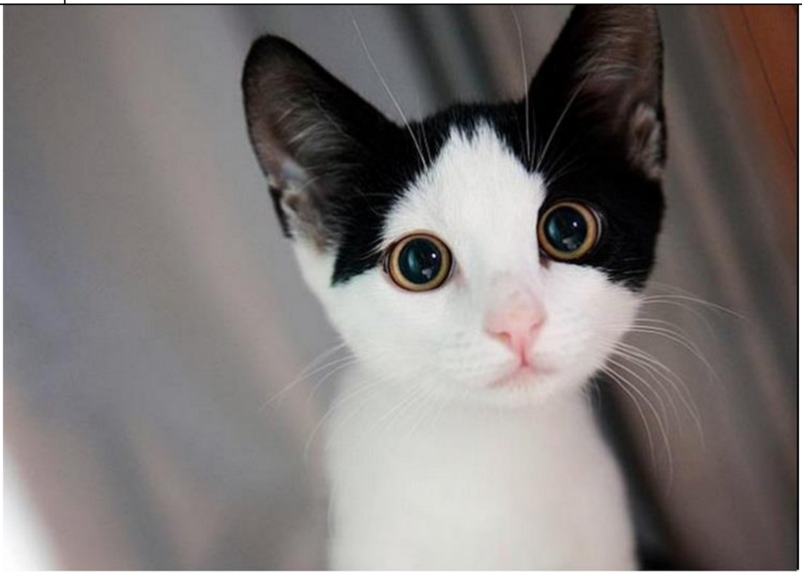
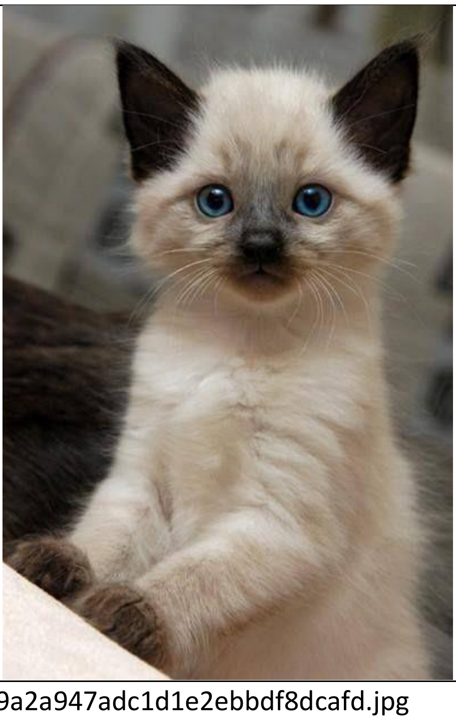
	
File Name	cat-adult-landing-hero.jpg
Type	JPEG
Location	/img_2017-B.dd/Users/computer/Pictures/
Status	Allocated
MD5	2a3c7e0ae9da299dbaee58c80ad992b0
Accessed	2017-06-12 12:03:54 AWST
Created	2017-06-12 12:03:54 AWST
Changed	2017-06-12 12:03:54 AWST
Sectors	3519441- 3519450
Analysis	Brown adult cat walking along a white background

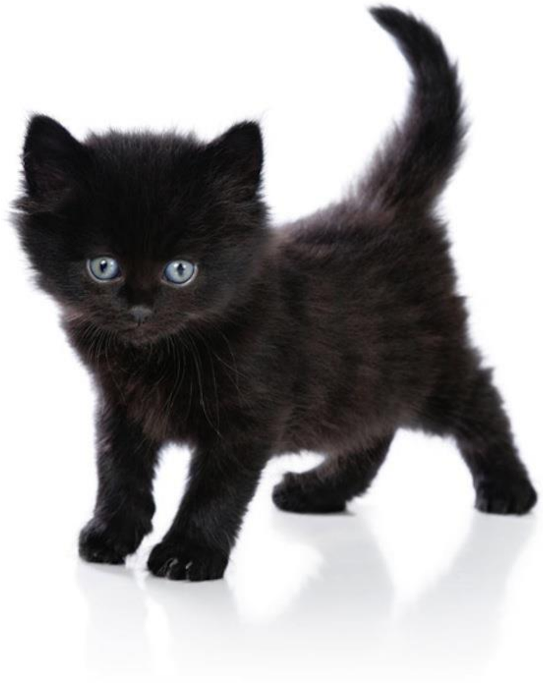
	
File Name	cute-kitten-catcute-little-cat-hd-for-desktop-of-cute-white-kitten.jpg
Type	JPEG
Location	/img_2017-B.dd/Users/computer/Pictures/
Status	Allocated
MD5	67e5e258f7c982e6154271b92aa5a65f
Accessed	2017-06-14 07:41:02 AWST
Created	2017-06-14 07:41:02 AWST
Changed	2017-06-14 07:41:02 AWST
Sectors	390556- 390640
Analysis	White kitten standing on a field of grass
	
File Name	cat-black-superstitious-fcs-cat-myths-162286659.jpg
Type	JPEG
Location	/img_2017-B.dd/Users/computer/Pictures/
Status	Allocated
MD5	7e9be033a955f18f777a87d28f93be3e
Accessed	2017-06-14 07:39:03 AWST
Created	2017-06-14 07:39:03 AWST
Changed	2017-06-14 07:39:03 AWST
Sectors	305997- 306024
Analysis	Black cat laying down witha white background

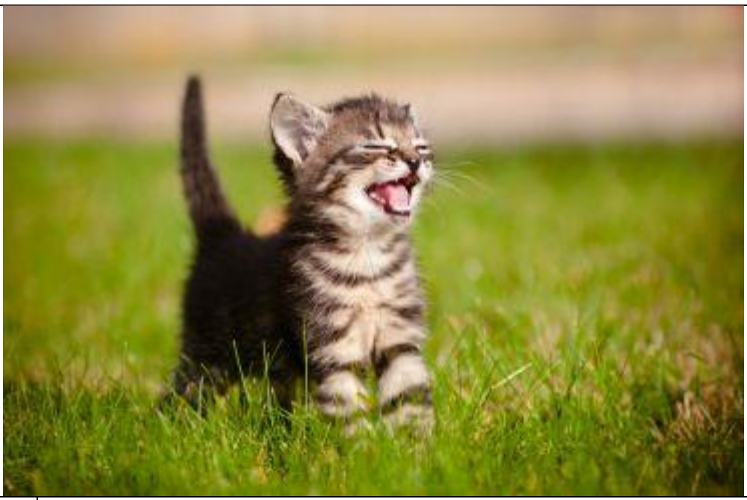
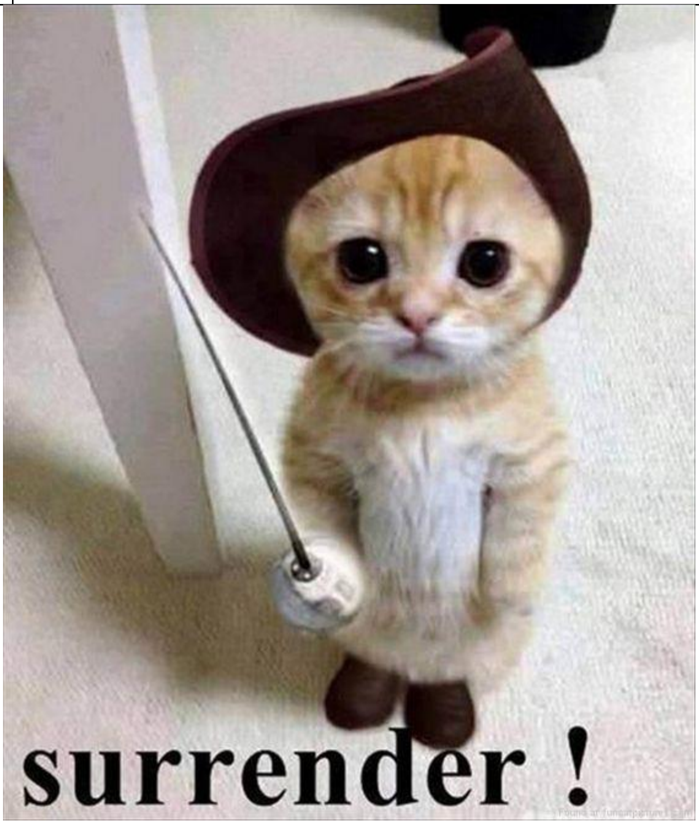
	
File Name	chaton_232339_w620.jpg
Type	JPEG
Location	/img_2017-B.dd/Users/computer/Pictures/
Status	Allocated
MD5	3fb617f7a7cc758a998410ad4567c126
Accessed	2017-06-12 12:03:01 AWST
Created	2017-06-12 12:03:01 AWST
Changed	2017-06-12 12:03:01 AWST
Sectors	344761- 344774
Analysis	Grey Kitten standing on a beige carpet

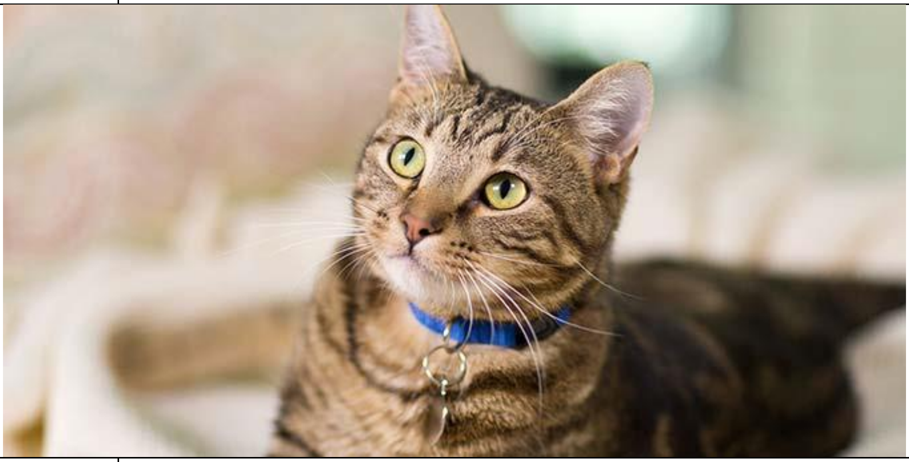
	
File Name	f03b7614dfadbbe4c2e8f88b69d12e04.jpg
Type	JPEG
Location	/img_2017-B.dd/Users/computer/Pictures/
Status	Allocated
MD5	f03b7614dfadbbe4c2e8f88b69d12e04
Accessed	2017-06-14 07:41:25 AWST
Created	2017-06-14 07:41:25 AWST
Changed	2017-06-14 07:41:25 AWST
Sectors	486441- 486560
Camera	Cannon Eos 20d
Analysis	Grey Kitten laying down on a red surface
	
File Name	cute-cat.jpg
Type	JPEG
Location	/img_2017-B.dd/Users/computer/Pictures/
Status	Allocated
MD5	b4f0a32909d39f9db932efc4487cb635
Accessed	2017-06-08 08:58:24 AWST
Created	2017-06-08 08:58:24 AWST
Changed	2017-06-08 08:58:24 AWST
Sectors	1359841- 1359878

Analysis	Yellow kitten with right paw covering right eye
	
File Name	cute-kittens-30-57b30ad41bc90__605.jpg
Type	JPEG
Location	/img_2017-B.dd/Users/computer/Pictures/
Status	Allocated
MD5	3ca727818de66ae034d151a4ae4588ee
Accessed	2017-05-31 06:39:54 AWST
Created	2017-05-31 06:39:54 AWST
Changed	2017-05-31 06:39:54 AWST
Sectors	1519407- 1519420
Analysis	Grey Kitten laying down on lap
	
File Name	101438745-cat-conjunctivitis-causes.jpg.jpg
Type	JPEG
Location	/img_2017-B.dd/Users/computer/Pictures/
Status	Allocated
MD5	f03b7614dfadbbe4c2e8f88b69d12e04
Accessed	2017-06-12 12:01:49 AWST
Created	2017-06-12 12:01:49 AWST

Changed	2017-06-12 12:01:49 AWST
Sectors	1251854- 1252471
Analysis	Grey Kitten laying down on a purple surface
	
File Name	cutest-cat-picture-ever.jpg
Type	JPEG
Location	/img_2017-B.dd/Users/computer/Pictures/
Status	Allocated
MD5	b8ad978bbab094a5c3539a39e5d5e61e
Accessed	2017-06-08 14:46:37 AWST
Created	2017-06-08 14:46:37 AWST
Changed	2017-06-08 14:46:37 AWST
Sectors	226317- 226334
Analysis	Black and white kitten standing with pink nose and mouth
	
File Name	1817db9a2a947adc1d1e2ebbdf8dcafd.jpg
Type	JPEG

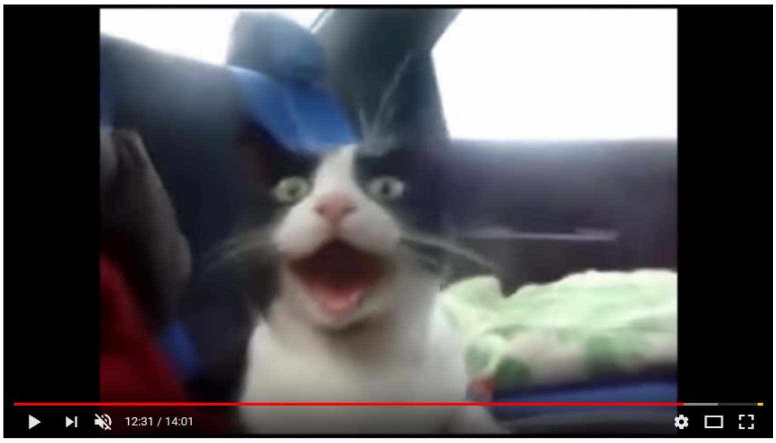
Location	/img_2017-B.dd/Users/computer/Pictures/
Status	Allocated
MD5	cfc5a8e8a803645232990aaf2ff49fd7
Accessed	2017-06-14 07:40:01 AWST
Created	2017-06-14 07:40:01 AWST
Changed	2017-06-14 07:40:02 AWST
Sectors	2185963- 2185969
Analysis	Light brown kitten standing with black and blue eyes
	
File Name	czarny-kot-fakt.jpg
Type	JPEG
Location	/img_2017-B.dd/Users/computer/Pictures/
Status	Allocated
MD5	17c9cdaceed06f53aed46f0466df604c
Accessed	2017-06-14 07:39:22 AWST
Created	2017-06-14 07:39:22 AWST
Changed	2017-06-14 07:39:22 AWST
Sectors	926272- 926286
Analysis	Black kitten standing on a white background

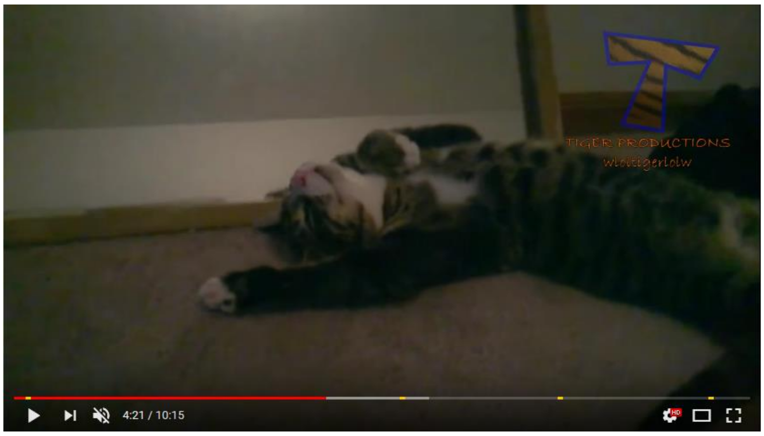
	
File Name	3385141-cat-images.jpg
Type	JPEG
Location	/img_2017-B.dd/Users/computer/Pictures/
Status	Allocated
MD5	f092a7ed1ab1a9c4c83b2615b0f335a1
Accessed	2017-06-12 11:59:48 AWST
Created	2017-06-12 11:59:48 AWST
Changed	2017-06-12 11:59:48 AWST
Sectors	3497627- 3497630
Analysis	Brown kitten meowing on a field of grass
	
File Name	e0194eca1c8135636ce0e014341548c3.jpg
Type	JPEG
Location	/img_2017-B.dd/Users/computer/Pictures/

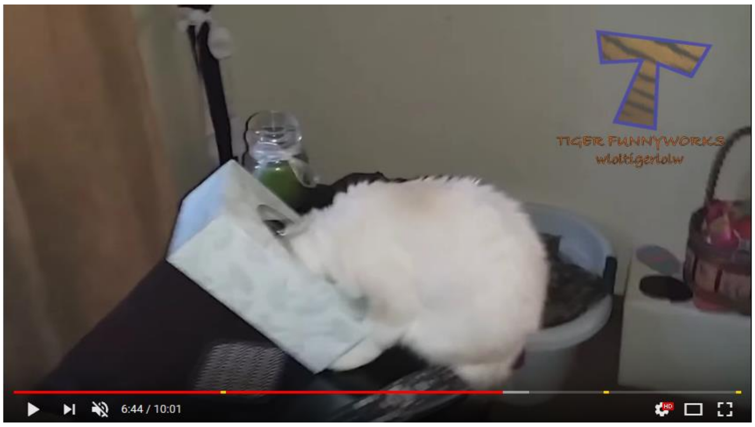
Status	Allocated
MD5	e0194eca1c8135636ce0e014341548c3
Accessed	2017-06-12 11:58:02 AWST
Created	2017-06-12 11:58:02 AWST
Changed	2017-06-12 11:58:02 AWST
Sectors	1039560- 1039572
Analysis	Yellow kitten holding and wearing musketeer outfit with the word “Surrender”.
	
File Name	HP_PCC_md_0130_cat53.jpg
Type	JPEG
Location	/img_2017-B.dd/Users/computer/Pictures/
Status	Allocated
MD5	17d9bb1d5b6505e14b24d7b36feed5c4
Accessed	2017-06-14 07:40:31 AWST
Created	2017-06-14 07:40:31 AWST
Changed	2017-06-14 07:40:31 AWST
Sectors	1108953- 1108958
Analysis	Brown cat wearing a blue collar

Video Links

On the same directory as the document folder /users/computer/documents/, there is also a docx file named “*links*” containing 3 different links to videos on a website called “*youtube*”.The 3 links found in the documents file are “ *https://www.youtube.com/watch?v=tntOCGkgt98*” , “ *https://www.youtube.com/watch?v=XyNlqQId-nk*” and *https://www.youtube.com/watch?v=hY7m5jjJ9mM* .The docx file was created , last accessed and modified on 14 June 2017 at 8:01 am , has a size of 11 megabytes ,allocated dir/meta flags and has a md5 hash of “*4e0af85db16d3ba53a221363346a3d8e*”.The first video is titled “*Funny Cats Compilation [Most See] Funny Cat Videos Ever Part 1”,* the video is a 14 minute compilation of kitten and cats that includes kittens playing in boxes , cats playing with other animals , cats getting angry at humans , cats struggling to not take a shower etc. The second video is titled *“The funniest and most humorous cat videos ever! - Funny cat compilation”* which is also a 10-minute compilation video of cats doing amusing stuff such as facing a mirror for the first time, playing with a shoe and cats sleeping a dreaming. The last video is named “CATS *will make you LAUGH YOUR HEAD OFF - Funny CAT compilation*” which contain material similar to the other two videos.



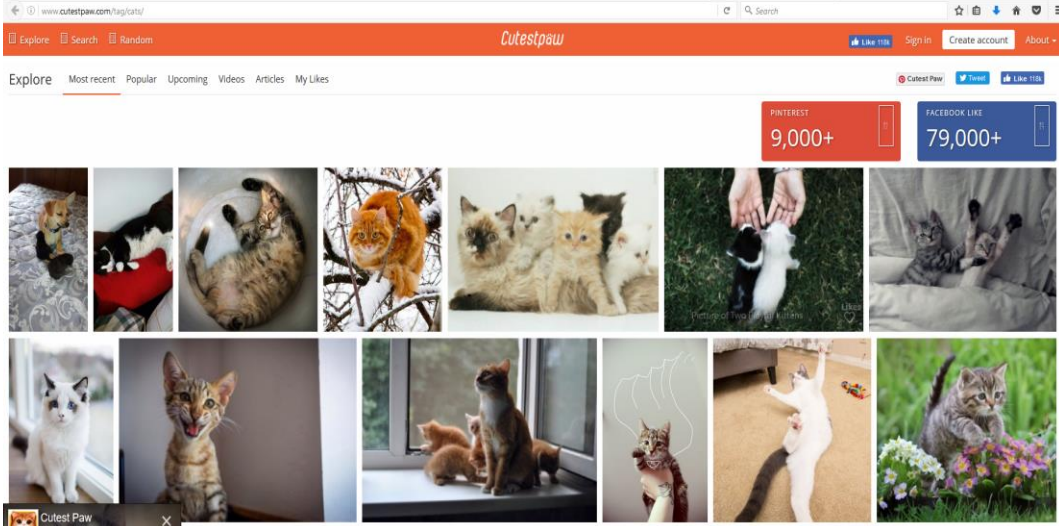




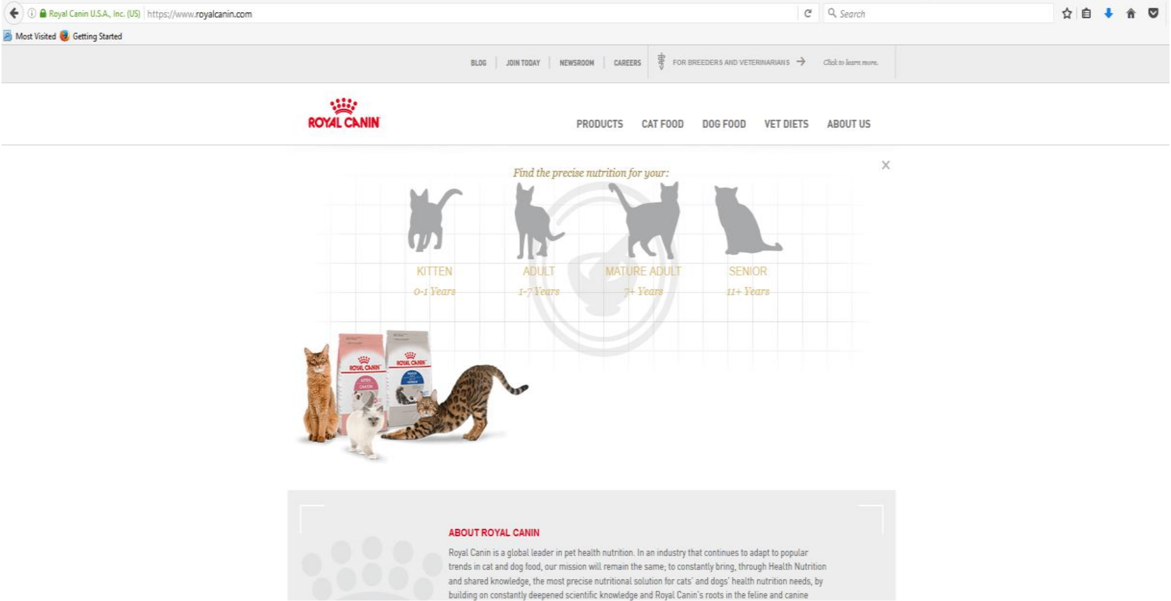
This shows that the owner of the content not only wants materials in JPEG format but they also want to access material with in other form such as suspicious web links and this shows that the owner could potentially have materials in other format like movies. This also shows that the user has knowledge on how to search for materials on the internet.

Web Data

Using the tool Internet Evidence Finder as well as autopsy web tools, I was able to find evidence of Clark’s machine browser accessing links that is related to the material of illegal content.Other than that , I was also able to recover google searches for material relating to cats with the key term be “*cute cat pictures* “ , “*cute kittens* “ , “*funny cat pictures*” , “ *cat pictures* “ , “*cat adoption perth*” as well as google searches for concealment method and other way of accessing the materials “*truecrypt*” , “*Tor browser*”, “ *bit shifting encryption software* “ , “*veracrypt*” and “ccleaner”. The user also google and access a webpage called “*savedeo*” which is a video downloading tool.



Web Link	http://www.cutestpaw.com/tag/cats/
Date Accessed	2017-06-08 08:56:53
Title	Cats Pictures - Cutest Paw
Domain	www.cutestpaw.com
Browser	FireFox

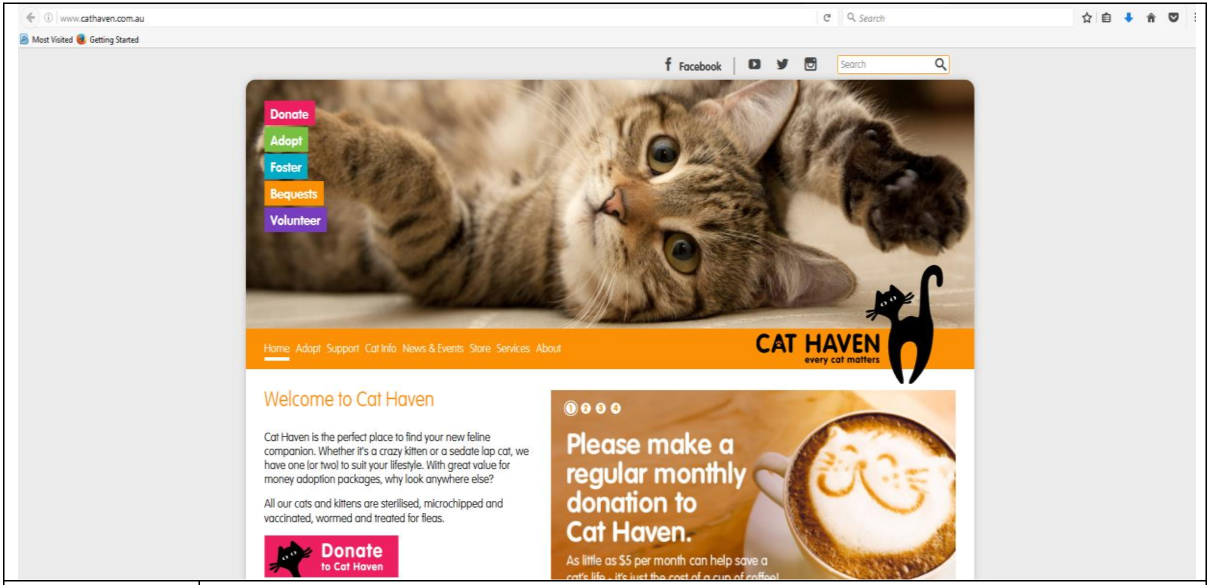


ABOUT ROYAL CANIN

Royal Canin is a global leader in pet health nutrition. In an industry that continues to adapt to popular trends in cat and dog food, our mission will remain the same; to constantly bring, through Health Nutrition and shared knowledge, the most precise nutritional solution for cats’ and dogs’ health nutrition needs, by building on constantly deepened scientific knowledge and Royal Canin’s roots in the feline and canine

Web Link	https://www.royalcanin.com
Date Accessed	2017-06-12 12:03:46

Title	Royal Canin
Browser	FireFox



Welcome to Cat Haven

Cat Haven is the perfect place to find your new feline companion. Whether it's a crazy kitten or a sedate lap cat, we have one (or two) to suit your lifestyle. With great value for money adoption packages, why look anywhere else?

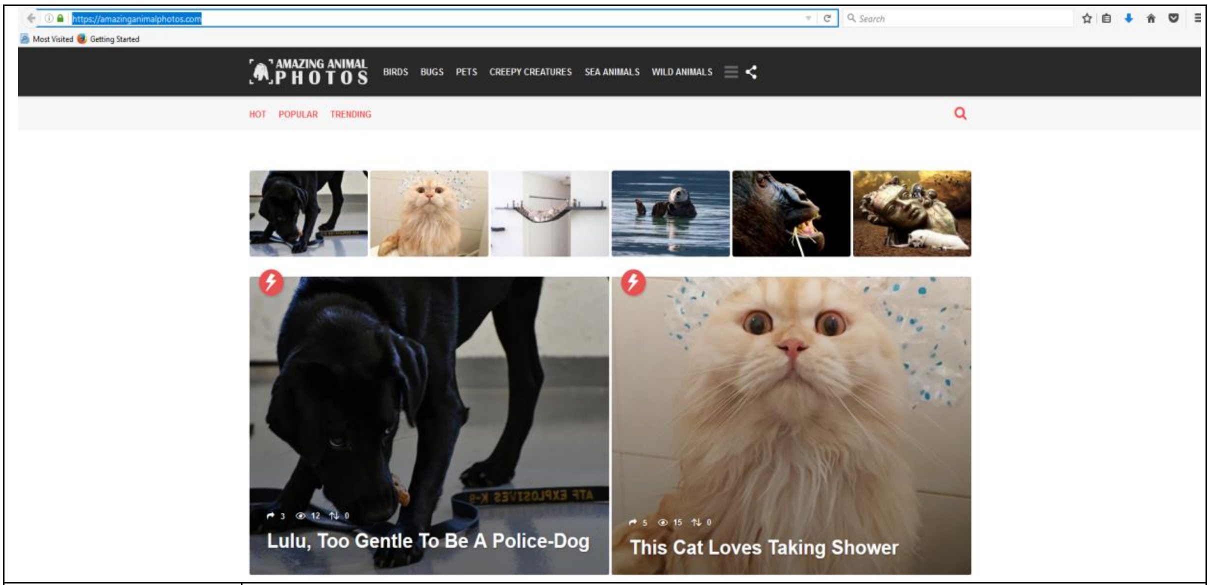
All our cats and kittens are sterilised, microchipped and vaccinated, wormed and treated for fleas.

Donate to Cat Haven

Please make a regular monthly donation to Cat Haven.

As little as $5 per month can help save a cat's life - it's just the cost of a cup of coffee!

Web Link	http://www.cathaven.com.au/
Date Accessed	2017-07-27 13:52:44
Title	Cat Haven where Every Cat Matters - Kittens & Cats for adoption & sale
Browser	FireFox



Web Link	https://amazinganimalphotos.com/
Date Accessed	2017-06-08 14:46:11
Title	Amazing Animal Photos
Browser	FireFox

This shows that the owner of the content has knowledge on how to accessing material relating to cats, furthermore having the knowledge of concealment as well as downloading the content. Another value that the evidence hold is based on the google search, the owner possibly has downloaded videos off webpage and perhaps own video content related to cat on the machine. Lastly, this also shows that there may be more content on the system that was wipe out with tool like ccleaner or encrypted with tools like Vera crypt and true crypt

Identification

The owner of the computer for the investigation that took place belongs to Clark Kent and based on a few evidence given from the computer, the owner of the content belongs to the owner of the computer which is Clark Kent. The first prove that links the material to Clark is the **software installed** on the computer such as “True crypt” which is a data/volume encryption software, this shows that he is trying to conceal the material that he obtained, for instance If the computer was getting manipulated by another entity then they would most likely take the time to setup the encryption of the illegal files. Another software that was on the system was “mIRC” private chat program, similar logic as the encryption if the computer was getting accessed by another individual they will not use a highly secured program for social interaction. There is also anti - malware software correctly installed on the system such as “Windows Defender” and “Windows Security”, while it is not the most effective at defending against unauthorised access, it will still work well guarding the computer.

Another evidence that shows Clark was the owner of the content is the amount of people that accessed the machine, based on the **user profile** of the computer it only shows 2 active accounts on the system, the first account is named “computer”. This is the account where the materials are located in, it also contains files titled “News stories “and contain documentation of the latest news which is the job of Clark Kent. The other profile contains minimal items and only a few update logs which is usually used by the administration.

Lastly, the **timeline** shows that the download of cat materials was not a single time but it was multiple times sporadically between the month of May through the month of June. This poses the question of how and why did Clark Kent failed to report to the administration if it was unauthorised during the month. The materials were openly placed on his recent visit directories that includes desktop, documents and downloads which he most likely visits daily.

Intent

In my opinion, Clark Kent has accessed and retained the materials **not on purpose** . Clark was forced to obtain these material in exchange for not revealing compromising information to the public based on the retrieved email messages. Clark did used google to search for cat pictures with harmful terms such as “*cute cat pictures* “ , “*cute kittens* “ , “*funny cat pictures*” and internet history shows that he visits the unhealthy webpages such as "*cathaven.com" and " cutestpaw.com*" . I believe this is because he is trying to find materials for the individuals that demanded them.

Exculpatory email evidence

During the investigation , i was able to recover parts of the email conversation with another individial named *David deida* and *Sassy penguin* with the email *daviddeida273@gmail.com* and sassypenguin0@gmail.com via mozilla thunderbird and gmail . The messages show that Clark Kent was forced to accessed, download and send materials relating to cats back to the individual in exchange for sensitive information not being revealed. Some emails suggesting include

On 18/05/2017 10:32 AM, David Deida wrote:
"*You will do precisely as I say or the whole world will know your little secret* “,

On 19/05/2017 8:53 AM, David Deida wrote:

“You are going to locate, download and distribute a minimum of 20 cute cat pictures. Oh and while y ou are at it, find and throw in a video and some kind of book about cats also!”

On Fri, May 19, 2017 at 4:13 AM, Clark <kcent00@gmail.com> wrote:

“Clark you are not Bryan Mills, stop the hero act, get to work, time is ticking...ohh and you have 30 minutes to send me the first picture...just so I know you''ve started your assignment!”.

On 12/06/2017 13:06 PM, Dacid Deida wrote:

“When you are ready, I want you to to send some images to an acquaintance - email is sassypenguin0@gmail.com. Then bundle the lot up and send them to me!”

The chat logs show David deida is trying to reveal some sort of secret that Clark has and he wants him to find, download and distribute 20 cute cat pictures, video and a book about cats to sassy penguin and himself David Deida.

Quantity of file

How many files of interest were discovered on the device(s) in question?

Desktop – foryou.txt , encrypted , stuff .txt

Foryou.txt – contain sensitive material

Stuff.txt -

Documents – Links.docx , thestuff.zip

Pictures – 17 pictures

How many ‘other’ non evidentiary files were on the computer?

Putting evidence into context is important…

Proportionality – evidence vs. non-evidence

% of incriminating files vs. normal files

Accidental vs. intentional possession of content!!

Running Sheet

Actions Conducted	Method of Action	Outcome
String search for material relating to cat	Select Tools , File search by attributes and Type in “Cat” , “ cats “ , “kittens” on the name field on autopsy	Found 28337 Results with mostly system folder And 4 Cat pictures
Analysed JPG ,PNG material on the system	Select Tools and View Images/Videos on menu bar in Autopsy	Found 18 Different Cat pictures
Analysed System for Video file such as wmv,mp4 , avi , mpg	On Selection tab , go to directory users/videos/ on autopsy	-
Search for Common Files Accessed	On the selection tab , accessed and searched files in Desktop , Favourites ,Documents and Downloads on Autopsy	Found a document with web links to cats , Concealment program and Encrypted text files
Search for hardware attached to the machine	On the selection tab , go to the directory results/device attached on Autopsy	Found 11 Results which includes a webcam , wheel mouse , two different usb storage device and a Bluetooth device
Analysed software installed on the system	Go to Installed program directory on the tab , check program files and program files x86 on Autopsy	Found 34 different software installed
Analyse web history and web cache	On the result tab , Select web bookmarks , web cookies , web search and web history on Autopsy	Found Web links related to cats
Find video content on the system	Load image and go thorugh videos on the files and stream section of Defraser	Found over 100 video files available on the system, all non- relating to cats
In Depth analysis of user Internet activity	Select Facebook IEF Refined Results , Chat , media , web related and encryption section of the tab on Internet Evidence Finder	Found Facebook Links, Twitter Links 2.Found evidence of using mIRC and QQ private chat 3.Found Webpage Links relating to “Cats” 4.Found 20 Encrpyed Files unrelating to cats
Email messages investigation	Select E-mail messages on the tab to use Autopsy ingestion module	Found back and forth conversation between kcent00@gmail.com , Daviddeida273@gmail.com , sassypenguin@gmail.com and encryption password
In - Depth Email analysis/ recovery	Install Mozilla Thunderbird , extract thunderbird profiles	Found 3 attachment that includes , 2 text file

	from AppData and replace the profile for the local machines thunderbird profiles.	“ foryou.txt” & “stuff.txt” , 1 unknown attachment “thestuff and a cat picture “maxdefault.jpg” as well as a distinct conversation between another individual.
Email attachment download attempt	Approve to reveal content of the message and right click to download the content	Downloaded foryou.txt , stuff.txt and “maxdefault.jpg”, could not manage to download the “thestuff” as it prompts for password.
Decryption attempt Foryou.txt	Open Truecrypt , Select File foryou.txt , Mount file in to volume , put in password found in email and right click open	Found sensitive information relating to the secret
Decryption attempt “encrypted“ file	Open TrueCrypt ,Select File encrypted , Mount file in to volume , put in password found in email and right click open	-
Decryption attempt stuff.txt	Open TrueCrypt , Select File stuff.txt , Mount file in to volume , put in password found in email and right click open	Found cat pictures

Timeline of events