**Assignment 2**

**Forensic Investigation Case Study**

Family Name: David Selvam

Given Name: Visahl Samson

Student Number: 10498743

Unit code and Title: CSG2308 Computer Forensics

Name of Lecturer: Liau Vui Kie

Campus: PSB Academy, Singapore

Course: Bachelors of Science in Cyber Security (FT)

Due Date: 25th November 2019

Contents

[Restricted document 3](#_Toc25530938)

[Executive summary 4](#_Toc25530939)

[Findings 4](#_Toc25530940)

[Files 4](#_Toc25530941)

[1.1 Image files 4](#_Toc25530942)

[1.2 Zip files 12](#_Toc25530943)

[1.3 Encrypted 13](#_Toc25530944)

[1.4 Recycle bin 13](#_Toc25530945)

[1.5 Web evidence 13](#_Toc25530946)

[1.5.1 Web history 13](#_Toc25530947)

[1.5.2 Web Download 17](#_Toc25530948)

[1.6 Email analysis 19](#_Toc25530949)

[Identification 21](#_Toc25530950)

[Intention 21](#_Toc25530951)

[Quantity 21](#_Toc25530952)

[Software installed 22](#_Toc25530953)

[Timeline of events 22](#_Toc25530954)

[Running sheet 24](#_Toc25530955)

[References 25](#_Toc25530956)

# Restricted document

This document is strictly private, and confidentials. The information in this document cannot be disclosed to public use. Only authorized individuals can access this document.

# Executive summary

A detailed digital forensic investigation requested by Western Australia police in order to conclude a case related with accessing the illegal content Cats which happened inside the organization named Daily planet. As an investigator I have analysed the evidences and prepared this following report. Primary tools used for the analyse process includes Autspy, FTK Manager, OS Forensics, and SIFT workstation. This report begins with findings then moves on to identification, intention, time line of events, running sheet, and ends with conclusion.

# Findings

## Files

### 1.1 Image files

During the investigation I have found following image files which are classified as illegal to access, use, and/or distribute.

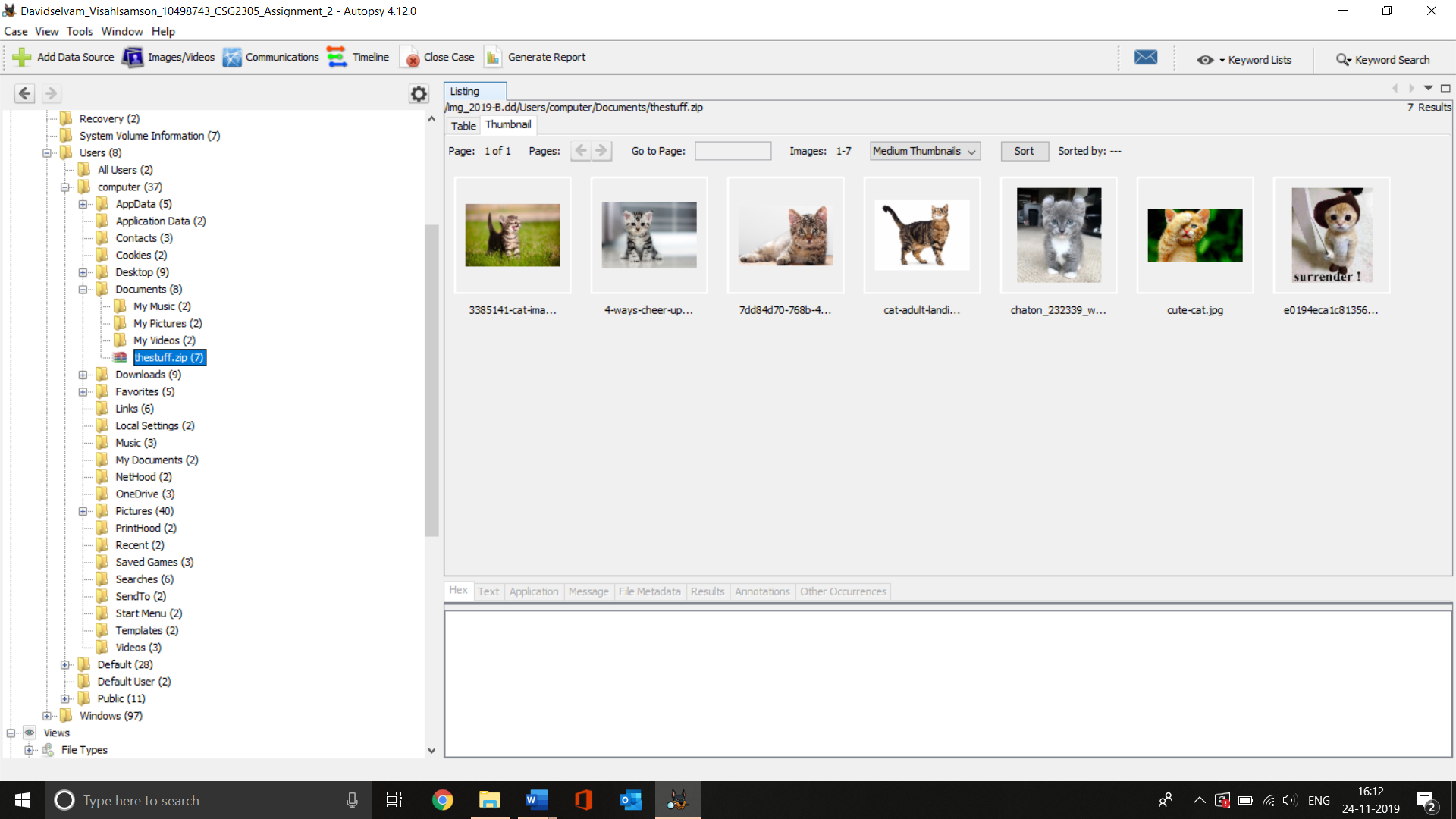
|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **Image No** | **File name and Path** | **MD5 Hash Value** | **File** | **Modified Time** | **Allocation status** | **File Name** |
|  | /img\_2019-B.dd/Users/computer/Pictures/cute-kittens-30-57b30ad41bc90\_\_605.jpg | 3ca727818de66ae034d151a4ae4588ee |  | 2017-05-31 06:39:55 SGT | Allocated | cute-kittens-30-57b30ad41bc90\_\_605.jpg |
|  | /img\_2019-B.dd/Users/computer/Pictures/3385141-cat-images.jpg  /img\_2019-B.dd/Users/computer/AppData/Roaming/Thunderbird/Profiles/k71ku0d7.default/ImapMail/imap.gmail.com/[Gmail].sbd/Sent Mail/thestuff.zip/3385141-cat-images.jpg  /img\_2019-B.dd/Users/computer/Documents/thestuff.zip/3385141-cat-images.jpg | f092a7ed1ab1a9c4c83b2615b0f335a1 | |  | | --- | |  | | 2017-06-12 11:59:48 SGT  2017-06-12 11:59:50 SGT  2017-06-12 11:59:50 SGT | Allocated | 3385141-cat-images.jpg |
|  | /img\_2019-B.dd/Users/computer/Pictures/7dd84d70-768b-492b-88f7-a6c70f2db2e9.jpg  /img\_2019-B.dd/Users/computer/Pictures/cat-03.jpg  /img\_2019-B.dd/Users/computer/Documents/thestuff.zip/7dd84d70-768b-492b-88f7-a6c70f2db2e9.jpg  /img\_2019-B.dd/Users/computer/AppData/Roaming/Thunderbird/Profiles/k71ku0d7.default/ImapMail/imap.gmail.com/[Gmail].sbd/Sent Mail/thestuff.zip/7dd84d70-768b-492b-88f7-a6c70f2db2e9.jpg | 53f8484efb0fbbeaf6cf0983e0424e07 |  | 2017-06-12 11:59:12 SGT  2017-06-12 13:00:07 SGT  2017-06-12 11:59:14 SGT  2017-06-12 11:59:14 SGT | Allocated | 7dd84d70-768b-492b-88f7-a6c70f2db2e9.jpg  cat-03.jpg |
|  | /img\_2019-B.dd/Users/computer/Pictures/cat-adult-landing-hero.jpg  /img\_2019-B.dd/Users/computer/Documents/thestuff.zip/cat-adult-landing-hero.jpg  /img\_2019-B.dd/Users/computer/AppData/Roaming/Thunderbird/Profiles/k71ku0d7.default/ImapMail/imap.gmail.com/[Gmail].sbd/Sent Mail/thestuff.zip/cat-adult-landing-hero.jpg | 2a3c7e0ae9da299dbaee58c80ad992b0 |  | 2017-06-12 12:03:54 SGT  2017-06-12 12:03:56 SGT  2017-06-12 12:03:56 SGT | Allocated | cat-adult-landing-hero.jpg |
|  | /img\_2019-B.dd/Users/computer/Pictures/chaton\_232339\_w620.jpg  /img\_2019-B.dd/Users/computer/Documents/thestuff.zip/chaton\_232339\_w620.jpg  /img\_2019-B.dd/Users/computer/AppData/Roaming/Thunderbird/Profiles/k71ku0d7.default/ImapMail/imap.gmail.com/[Gmail].sbd/Sent Mail/thestuff.zip/chaton\_232339\_w620.jpg | 3fb617f7a7cc758a998410ad4567c126 |  | 2017-06-12 12:03:01 SGT  2017-06-12 12:03:02 SGT    2017-06-12 12:03:02 SGT | Allocated | chaton\_232339\_w620.jpg |
|  | /img\_2019-B.dd/Users/computer/Pictures/cute-cat.jpg  /img\_2019-B.dd/Users/computer/Documents/thestuff.zip/cute-cat.jpg  /img\_2019-B.dd/Users/computer/AppData/Roaming/Thunderbird/Profiles/k71ku0d7.default/ImapMail/imap.gmail.com/[Gmail].sbd/Sent Mail/thestuff.zip/cute-cat.jpg | b4f0a32909d39f9db932efc4487cb635 |  | 2017-06-08 08:58:25 SGT  2017-06-08 08:58:26 SGT    2017-06-08 08:58:26 SGT | Allocated | cute-cat.jpg |
|  | /img\_2019-B.dd/Users/computer/Pictures/cutest-cat-picture-ever.jpg  /img\_2019-B.dd/ProgramData/Microsoft/Windows/AppRepository/Packages/Microsoft.WindowsFeedbackHub\_1.1704.1603.0\_x64\_\_8wekyb3d8bbwe/ | b8ad978bbab094a5c3539a39e5d5e61e |  | 2017-06-08 14:46:37 SGT  2017-06-13 09:05:03  SGT | Allocated | cutest-cat-picture-ever.jpg |
|  | /img\_2019-B.dd/Users/computer/Pictures/czarny-kot-fakt.jpg | 17c9cdaceed06f53aed46f0466df604c |  | 2017-06-14 07:39:22 SGT | Allocated | czarny-kot-fakt.jpg |
|  | /img\_2019-B.dd/Users/computer/Pictures/e0194eca1c8135636ce0e014341548c3.jpg  /img\_2019-B.dd/Users/computer/Documents/thestuff.zip/e0194eca1c8135636ce0e014341548c3.jpg  /img\_2019-B.dd/Users/computer/AppData/Roaming/Thunderbird/Profiles/k71ku0d7.default/ImapMail/imap.gmail.com/[Gmail].sbd/Sent Mail/thestuff.zip/e0194eca1c8135636ce0e014341548c3.jpg | e0194eca1c8135636ce0e014341548c3 |  | 2017-06-12 11:58:02 SGT  2017-06-12 11:58:04 SGT    2017-06-12 11:58:04 SGT | Allocated | e0194eca1c8135636ce0e014341548c3.jpg  e0194eca1c8135636ce0e014341548c3.jpg  e0194eca1c8135636ce0e014341548c3.jpg |
|  | /img\_2019-B.dd/Users/computer/Pictures/HP\_PCC\_md\_0130\_cat53.jpg | 17d9bb1d5b6505e14b24d7b36feed5c4 |  | 2017-06-14 07:40:32 SGT | Allocated | HP\_PCC\_md\_0130\_cat53.jpg |
|  | /img\_2019-B.dd/Users/computer/Pictures/cat2.jpg | 096254b20f79b6728384a54dbba69ea1 |  | 2017-06-14 07:42:18 SGT | Allocated | cat2.jpg |
|  | /img\_2019-B.dd/Users/computer/Pictures/cute-kitten-catcute-little-cat-hd-for-desktop-of-cute-white-kitten.jpg | 67e5e258f7c982e6154271b92aa5a65f |  | 2017-06-14 07:41:03 SGT | Allocated | cute-kitten-catcute-little-cat-hd-for-desktop-of-cute-white-kitten.jpg |
|  | /img\_2019-B.dd/Users/computer/Pictures/f03b7614dfadbbe4c2e8f88b69d12e04.jpg | f03b7614dfadbbe4c2e8f88b69d12e04 |  | 2017-06-14 07:41:26 SGT | Allocated | f03b7614dfadbbe4c2e8f88b69d12e04.jpg |
|  | /img\_2019-B.dd/Users/computer/AppData/Roaming/Thunderbird/Profiles/k71ku0d7.default/ImapMail/imap.gmail.com/[Gmail].sbd/All Mail/maxresdefault.jpg | c6bad95007394210932c27bd61e97a8d |  | 0000-00-00 00:00:00 | Allocated | maxresdefault.jpg |
|  | /img\_2019-B.dd/Users/computer/AppData/Local/Mozilla/Firefox/Profiles/zij1frw0.default/cache2/entries/4C074A918ACE865639183E88679297964650C2DF | da632a0e6a0b6ec1c5066078e74b7c7f | C:\Users\남혜준\Desktop\cat\4C074A918ACE865639183E88679297964650C2DF | 2017-07-27 13:32:44 SGT | Allocated | 4C074A918ACE865639183E88679297964650C2DF |
|  | /img\_2019-B.dd/Users/computer/AppData/Local/Mozilla/Firefox/Profiles/zij1frw0.default/cache2/entries/5F5D6630E8B61138D0BEC8E46ED1D28BDDAD1ECE | 86593c57169b001b908baa4908d05a5a | C:\Users\남혜준\Desktop\cat\5F5D6630E8B61138D0BEC8E46ED1D28BDDAD1ECE | 2017-07-27 13:32:44 SGT | Allocated | 5F5D6630E8B61138D0BEC8E46ED1D28BDDAD1ECE |
|  | /img\_2019-B.dd/Users/computer/AppData/Local/Mozilla/Firefox/Profiles/zij1frw0.default/cache2/entries/44E71A116A8058C725094237E62946F7981F0C3C | 99def09b617f479a7e53cc0291abe56c | C:\Users\남혜준\Desktop\cat\44E71A116A8058C725094237E62946F7981F0C3C | 2017-07-27 13:32:46 SGT | Allocated | 44E71A116A8058C725094237E62946F7981F0C3C |
|  | /img\_2019-B.dd/Users/computer/AppData/Local/Mozilla/Firefox/Profiles/zij1frw0.default/cache2/entries/4B8CFD2C458C97F2023374C8CEDDCE8C18FFE78E | 25319e8ab80dd419dd4a9a3956f4d364 | C:\Users\남혜준\Desktop\cat\4B8CFD2C458C97F2023374C8CEDDCE8C18FFE78E | 2017-06-14 11:15:19 SGT | Allocated | 4B8CFD2C458C97F2023374C8CEDDCE8C18FFE78E |
|  | /img\_2019-B.dd/Users/computer/AppData/Local/Mozilla/Firefox/Profiles/zij1frw0.default/cache2/entries/68690FE1015CF969296B9D2C48106221381209AA | c2639e83139f943ae9f452d1cb7f3457 | C:\Users\남혜준\Desktop\cat\68690FE1015CF969296B9D2C48106221381209AA | 2017-07-27 13:32:46 SGT | Allocated | 68690FE1015CF969296B9D2C48106221381209AA |
|  | /img\_2019-B.dd/Users/computer/AppData/Local/Mozilla/Firefox/Profiles/zij1frw0.default/cache2/entries/5ABEF7C3DB2D79AD5D736A7A6D72C07509E449EC | 394c75f3eb5e4b2fc079774cd70d4762 | C:\Users\남혜준\Desktop\cat\5ABEF7C3DB2D79AD5D736A7A6D72C07509E449EC | 2017-07-27 13:52:47 SGT | Allocated | 5ABEF7C3DB2D79AD5D736A7A6D72C07509E449EC |
|  | /img\_2019-B.dd/Users/computer/Pictures/4-ways-cheer-up-depressed-cat.jpg  /img\_2019-B.dd/Users/computer/Documents/thestuff.zip/4-ways-cheer-up-depressed-cat.jpg  /img\_2019-B.dd/$Recycle.Bin/S-1-5-21-164977783-601896633-895069657-1001/$RXT96AU.jpg  /img\_2019-B.dd/Users/computer/AppData/Roaming/Thunderbird/Profiles/k71ku0d7.default/ImapMail/imap.gmail.com/[Gmail].sbd/Sent Mail/thestuff.zip/4-ways-cheer-up-depressed-cat.jpg | 9a6f4ee0d85fd3fe0b6ce2470cbd1b78 |  | 2017-06-14 08:01:38 SGT  2017-06-12 12:02:26 SGT  2017-06-12 12:02:24 SGT  2017-06-12 12:02:26 SGT | Allocated | 4-ways-cheer-up-depressed-cat.jpg  4-ways-cheer-up-depressed-cat.jpg  4-ways-cheer-up-depressed-cat.jpg  4-ways-cheer-up-depressed-cat.jpg |
|  | /img\_2019-B.dd/Users/computer/Pictures/101438745-cat-conjunctivitis-causes.jpg | 0b057be67f220767dd1075594432e8b8 |  | 2017-06-12 12:01:49 SGT | Allocated | 101438745-cat-conjunctivitis-causes.jpg |
|  | /img\_2019-B.dd/Users/computer/AppData/Local/Mozilla/Firefox/Profiles/zij1frw0.default/cache2/entries/5E822275D63B3969B1B1333DA2097A0B4128A952 | ba6b320eb38bf3c3ae33fcf711b31b33 | C:\Users\남혜준\Desktop\cat\5E822275D63B3969B1B1333DA2097A0B4128A952 | 2017-07-27 13:32:44 SGT | Allocated | 5E822275D63B3969B1B1333DA2097A0B4128A952 |
|  | /img\_2019-B.dd/Users/computer/AppData/Local/Mozilla/Firefox/Profiles/zij1frw0.default/cache2/entries/7475FDC6010B10E9A92F8566A37722CAD23B740A | 25f5057a1e560375320fbf0b1aa08ac5 | C:\Users\남혜준\Desktop\cat\7475FDC6010B10E9A92F8566A37722CAD23B740A | 2017-06-14 11:15:19 SGT | Allocated | 7475FDC6010B10E9A92F8566A37722CAD23B740A |
|  | /img\_2019-B.dd/Users/computer/AppData/Local/Mozilla/Firefox/Profiles/zij1frw0.default/cache2/entries/74EC9D0E06EC8CA48429A71B4F63721B9C46A7BE | aea2b00667c8d2dd131b001448e9e315 | C:\Users\남혜준\Desktop\cat\74EC9D0E06EC8CA48429A71B4F63721B9C46A7BE | 2017-07-27 13:32:46 SGT | Allocated | 74EC9D0E06EC8CA48429A71B4F63721B9C46A7BE |
|  | /img\_2019-B.dd/Users/computer/Pictures/1817db9a2a947adc1d1e2ebbdf8dcafd.jpg | cfc5a8e8a803645232990aaf2ff49fd7 |  | 2017-06-14 07:40:02 SGT | Allocated | 1817db9a2a947adc1d1e2ebbdf8dcafd.jpg |
|  | /img\_2019-B.dd/  Users/computer/AppData/Local/Mozilla/Firefox/Profiles/zij1frw0.default/cache2/entries/0F5FFD50A319226DEC8C39472F3F0E35497A1649 | fb6af646569ecb5e3b8604c741f4d16b |  | 2017-06-21 09:06:23 SGT | Allocated | 0F5FFD50A319226DEC8C39472F3F0E35497A1649 |
|  | /img\_2019-B.dd/Users/computer/AppData/Local/Mozilla/Firefox/Profiles/zij1frw0.default/cache2/entries/E0865112772538A7107E90537AE882A566975C1D | |  |  | | --- | --- | |  | 5af0a4e  35d62733a  29d1fc40d4  9bcea4 | |  | 2017-07-27 13:52:47 SGT | Allocated | E0865112772538A7107E90537AE882A566975C1D |
|  | /img\_2019-B.dd/  Users/computer/AppData/Local/Mozilla/Firefox/Profiles/zij1frw0.default/cache2/entries/CB0FDAAFD566F7970098AF91F1C4922D27625D6E | 8fab13dce26ac2bfb6a7dfe27911d7c6 |  | 2017-07-27 13:32:44 SGT | Allocated | CB0FDAAFD566F7970098AF91F1C4922D27625D6E |
|  | /img\_2019-B.dd/  Users/computer/AppData/Local/Mozilla/Firefox/Profiles/zij1frw0.default/cache2/entries/8F36D78E96FF509F33D9AC6C8055AC15152CAAD6 | 144d7dad4917ce9d7b623283ec6a5e74 |  | 2017-07-27 13:32:45 SGT | Allocated | 8F36D78E96FF509F33D9AC6C8055AC15152CAAD6 |
|  | /img\_2019-B.dd/  Program Files/WindowsApps/Microsoft.SkypeApp\_11.18.614.0\_x64\_\_kzf8qxf38zg5c/SkypeApp/Designs/Emoticons/large/cat.png | d02b21a145574ae692a71f29a242fe9c |  | 2017-03-19 10:32:14 SGT | Allocated | cat.png |
|  | /img\_2019-B.dd/Users/computer/AppData/Local/Mozilla/Firefox/Profiles/zij1frw0.default/cache2/entries/773432A7F9E407F54FB759B177D4E176342DE372 | 213ccef9bd59c0535950a271a3cd34d6 |  | 2017-07-27 13:32:44 SGT | Allocated | 773432A7F9E407F54FB759B177D4E176342DE372 |
|  | /img\_2019-B.dd/  Users/computer/AppData/Local/Mozilla/Firefox/Profiles/zij1frw0.default/cache2/entries/BA23BD7804FA820A4833B07024384DE24FC1BC49 | 82abf4bf7e5b854de2a7ba2e78cf80fc |  | 2017-07-27 13:32:44 SGT | Allocated | BA23BD7804FA820A4833B07024384DE24FC1BC49 |
|  | /img\_2019-B.dd/  Users/computer/AppData/Local/Mozilla/Firefox/Profiles/zij1frw0.default/cache2/entries/E1880A7470573E3128A1C476500E89D3C2235892 | 9d5cbe01f269bbc58096c11243759eac |  | 2017-07-27 13:52:47 SGT | Allocated | E1880A7470573E3128A1C476500E89D3C2235892 |
|  | /img\_2019-B.dd/Users/computer/AppData/Local/Mozilla/Firefox/Profiles/zij1frw0.default/cache2/entries/3D142110BE3848F161556E84F14DB025729E0ED5 | 71a4f8ff43f7fb2dd7c170f45165dde6 |  | 2017-07-27 13:52:47 SGT | Allocated | 3D142110BE3848F161556E84F14DB025729E0ED5 |

Table 1.1 .1 Image files that are classified as illegal

Apart from the image files I have found some other types of files which includes Zip file, encrypted file. The details are given below.

### 1.2 Zip files

Inside the document folder I have found a zip file named thestuff.zip. Before extracting it into my device I have clicked on the zip file inside the Autopsy and got a rough view about it. The evidence before extracting into my device has been given in screenshot 1.



Screenshot 1 Rough view in Autopsy

After that I extracted the zip file and used 7 zip to get the contents inside. I found the 7 same images shown in screenshot 1. The property of the zip file is given in Table 1.2.1

|  |  |
| --- | --- |
| Name | thestuff.zip |
| Location | /img\_2019-B.dd/Users/computer/Documents/thestuff.zip |
| Change Time | 2017-06-14 07:00:50 SGT |
| Access Time | 2017-06-14 07:00:15 SGT |
| Created Time | 2017-06-14 07:00:15 SGT |
| MD5 Hash | 4364f14ecdd1380e8d60c54b92492baa |
| Extension | Zip |
| Flag (Meta) | Allocated |

Table 1.2.1 Zip file properties

### 1.3 Encrypted

I have found 3 encrypted files from the following locations.

* /img\_2019-B.dd/Users/computer/Desktop/encrypted
* /img\_2019-B.dd/Users/computer/Desktop/foryou.txt
* thestuff.txt (from email attachment)

I was able to decrypt the first 2 files with the usage of password “superman” (which obtained from email). I found nothing inside the first file (i.e. encrypted) and from foryou.txt file I found a pdf which is superman.pdf and for the thestuff.txt which obtained from email I was not able to decrypt it.

### 1.4 Recycle bin

Inside the recycle bin I have found a cat image which is listed in Table 1.1.1 as Image No 21.

## 1.5 Web evidence

### 1.5.1 Web history

The web history has been analyzed and found out that the internet has been used to access the illegal contents. The summary of websites/contents accessed by the user are organized in Table 1.5.1.1

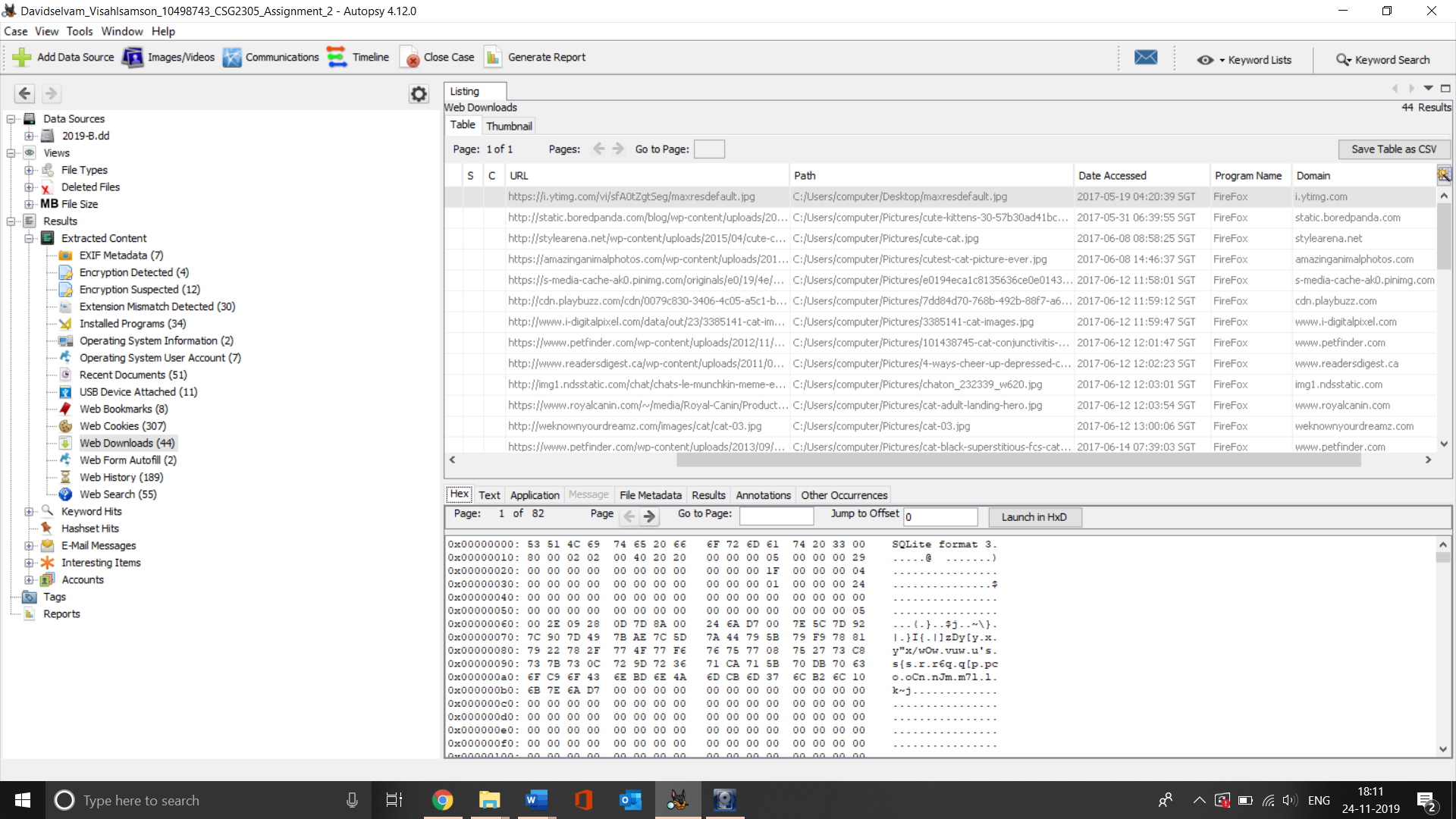
|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Date | Search title | URL | User agent | Search engine |
| 2017-05-19 04:19:21 | cute cat - Google Search | https://www.google.com.au/search?site=&tbm=isch&source=hp&biw=1366&bih=659&q=cute+cat&oq=cute+cat&gs\_l=img.3..0l10.2863.4848.0.6003.8.8.0.0.0.0.520.1309.3-1j1j1.3.0....0...1.1.64.img..5.3.1302.rvKGkgnKmxM | FireFox | Google |
| 2017-05-31 06:37:25 | cat video - YouTube | https://www.youtube.com/results?search\_query=cat+video | FireFox | Google |
| 2017-05-31 06:39:23 | cute kitten - Google Search | https://www.google.com.au/search?site=&tbm=isch&source=hp&biw=1366&bih=659&q=cute+kitten&oq=cute+kitten&gs\_l=img.3...2028.3741.0.3934.11.8.0.0.0.0.0.0..0.0....0...1.1.64.img..11.0.0.ab3NuKnLF5E | FireFox | Google |
| 2017-05-31 06:39:41 | cute-kittens-30-57b30ad41bc90\_\_605.jpg (JPEG Image, 605 × 454 pixels) | https://www.google.com.au/url?sa=i&rct=j&q=&esrc=s&source=images&cd=&ved=0ahUKEwjhzJGe5ZjUAhWIlZQKHSUnBlAQjBwIBA&url=http%3A%2F%2Fstatic.boredpanda.com%2Fblog%2Fwp-content%2Fuploads%2F2016%2F08%2Fcute-kittens-30-57b30ad41bc90\_\_605.jpg&psig=AFQjCNGb3bFgJvqZSsfWi1tpgiYnL1c4og&ust=1496274010257544&cad=rjt | FireFox | Google |
| 2017-06-08 08:57:46 | cute cat pictures - Google Search | https://www.google.com.au/?gfe\_rd=cr&ei=5J04Wc2CCOnDXsmestAN#q=cute+cat+pictures | FireFox | Google |
| 2017-06-08 08:56:53 | Cats Pictures - Cutest Paw | http://www.cutestpaw.com/tag/cats/ | FireFox | Google |
| 2017-06-08 08:57:55 | cute cat pictures - Google Search | https://www.google.com.au/search?q=cute+cat+pictures&tbm=isch&imgil=rqmX7Hwtd64zxM%253A%253BHkACfLrkxSJi-M%253Bhttp%25253A%25252F%25252Fstylearena.net%25252Fcute-cat-pictures%25252F&source=iu&pf=m&fir=rqmX7Hwtd64zxM%253A%252CHkACfLrkxSJi-M%252C\_&usg=\_\_Gd8ItOEk3eS2GvxMpk8d9\_o9UJI%3D&biw=1366&bih=659&ved=0ahUKEwidpIfQha3UAhWIU7wKHRlaAWMQyjcIOg&ei=OKE4WZ2oBIin8QWZtIWYBg | FireFox | Google |
| 2017-06-08 08:58:09 | cute-cat.jpg (JPEG Image, 1600 × 900 pixels) - Scaled (73%) | http://stylearena.net/wp-content/uploads/2015/04/cute-cat.jpg | FireFox | Google |
| 2017-06-08 14:46:11 | cutest-cat-picture-ever.jpg (JPEG Image, 750 × 534 pixels) | https://amazinganimalphotos.com/wp-content/uploads/2013/04/cutest-cat-picture-ever.jpg | FireFox | Google |
| 2017-06-12 11:57:16 | funny cat pictures - Google Search | https://www.google.com.au/?gws\_rd=ssl#q=funny+cat+pictures | FireFox | Google |
| 2017-06-12 11:57:49 | e0194eca1c8135636ce0e014341548c3.jpg (JPEG Image, 564 × 665 pixels) - Scaled (99%) | https://s-media-cache-ak0.pinimg.com/originals/e0/19/4e/e0194eca1c8135636ce0e014341548c3.jpg | FireFox | Google |
| 2017-06-12 11:58:34 | cat pictures - Google Search | https://www.google.com.au/?gws\_rd=ssl#q=funny+cat+pictures | FireFox | Google |
| 2017-06-12 11:58:52 | 7dd84d70-768b-492b-88f7-a6c70f2db2e9.jpg (JPEG Image, 2560 × 1600 pixels) - Scaled (41%) | http://cdn.playbuzz.com/cdn/0079c830-3406-4c05-a5c1-bc43e8f01479/7dd84d70-768b-492b-88f7-a6c70f2db2e9.jpg | FireFox | Google |
| 2017-06-12 11:59:38 | 3385141-cat-images.jpg (JPEG Image, 370 × 245 pixels) | http://www.i-digitalpixel.com/data/out/23/3385141-cat-images.jpg | FireFox | Google |
| 2017-06-12 12:01:21 | 2017-06-12 12:01:21 | https://www.google.com.au/url?sa=i&rct=j&q=&esrc=s&source=images&cd=&ved=0ahUKEwiUwLWItrfUAhVHV7wKHcZqCu8QjBwIBA&url=https%3A%2F%2Fwww.petfinder.com%2Fwp-content%2Fuploads%2F2012%2F11%2F101438745-cat-conjunctivitis-causes.jpg&psig=AFQjCNH8UeLAwpy9ErBTNodpUAP5rbDicA&ust=1497326411405752&cad=rjt | FireFox | Google |
| 2017-06-12 12:01:28 | 101438745-cat-conjunctivitis-causes.jpg (JPEG Image, 2673 × 1797 pixels) - Scaled (36%) | https://www.google.com.au/url?sa=i&rct=j&q=&esrc=s&source=images&cd=&ved=0ahUKEwiUwLWItrfUAhVHV7wKHcZqCu8QjBwIBA&url=https%3A%2F%2Fwww.petfinder.com%2Fwp-content%2Fuploads%2F2012%2F11%2F101438745-cat-conjunctivitis-causes.jpg&psig=AFQjCNH8UeLAwpy9ErBTNodpUAP5rbDicA&ust=1497326411405752&cad=rjt | FireFox | Google |
| 2017-06-12 12:02:13 | 4-ways-cheer-up-depressed-cat.jpg (JPEG Image, 1000 × 700 pixels) - Scaled (94%) | https://www.google.com.au/url?sa=i&rct=j&q=&esrc=s&source=images&cd=&ved=0ahUKEwj9mOihtrfUAhUJXrwKHYpyBqkQjBwIBA&url=http%3A%2F%2Fwww.readersdigest.ca%2Fwp-content%2Fuploads%2F2011%2F01%2F4-ways-cheer-up-depressed-cat.jpg&psig=AFQjCNH8UeLAwpy9ErBTNodpUAP5rbDicA&ust=1497326411405752&cad=rjt | FireFox | Google |
| 2017-06-12 12:02:38 | chats-le-munchkin-meme-en-grandissant-il-garde-son-adorable-taille-de-chaton\_232339\_w620.jpg (JPEG Image, 620 × 700 pixels) - Scaled (94%) | https://www.google.com.au/url?sa=i&rct=j&q=&esrc=s&source=images&cd=&ved=0ahUKEwieufiutrfUAhWLu7wKHbN7CbQQjBwIBA&url=http%3A%2F%2Fimg1.ndsstatic.com%2Fchat%2Fchats-le-munchkin-meme-en-grandissant-il-garde-son-adorable-taille-de-chaton\_232339\_w620.jpg&psig=AFQjCNH8UeLAwpy9ErBTNodpUAP5rbDicA&ust=1497326411405752&cad=rjt | FireFox | Google |
| 2017-06-12 12:03:46 | cat-adult-landing-hero.jpg (JPEG Image, 470 × 350 pixels) | https://www.royalcanin.com/~/media/Royal-Canin/Product-Categories/cat-adult-landing-hero.ashx | FireFox | Google |
| 2017-06-14 07:39:15 | czarny-kot-fakt.jpg (JPEG Image, 600 × 773 pixels) - Scaled (85%) | http://zalajkowane.pl/wp-content/uploads/2014/05/czarny-kot-fakt.jpg | FireFox | Google |
| 2017-06-14 07:39:55 | 1817db9a2a947adc1d1e2ebbdf8dcafd.jpg (JPEG Image, 399 × 600 pixels) | https://s-media-cache-ak0.pinimg.com/736x/18/17/db/1817db9a2a947adc1d1e2ebbdf8dcafd.jpg | FireFox | Google |
| 2017-06-14 07:41:20 | f03b7614dfadbbe4c2e8f88b69d12e04.jpg (JPEG Image, 1600 × 1200 pixels) - Scaled (54%) | https://s-media-cache-ak0.pinimg.com/originals/f0/3b/76/f03b7614dfadbbe4c2e8f88b69d12e04.jpg | FireFox | Google |
| 2017-06-14 07:52:00 | 4426323.jpg (JPEG Image, 340 × 255 pixels) | http://luniktyen.weebly.com/uploads/5/6/9/8/5698387/4426323.jpg?342 | FireFox | Google |
| 2017-06-14 08:00:52 | CATS will make you LAUGH YOUR HEAD OFF - Funny CAT compilation - YouTube | https://www.youtube.com/watch?v=hY7m5jjJ9mM | FireFox | Google |
| 2017-07-27 13:26:56 | Cat Haven where Every Cat Matters - Kittens & Cats for adoption & sale | http://www.cathaven.com.au/ | FireFox | Google |

Table 1.5.1.1 Web history

(Note : all the details are sorted on date basis in ascending order)

### 1.5.2 Web Download

While analyzing the web I have discovered the downloads in the form of sql lite data databases. Below given screenshot shows the list of sql lites in autopsy. The file path for the sqllite is img\_2019-B.dd/Users/computer/AppData/Roaming/Mozilla/Firefox/Profiles/zij1frw0.default/places.sqlite The extended details are given in the following table 1.5.2.1



Screenshot 2 Downloads in SQL Lite format

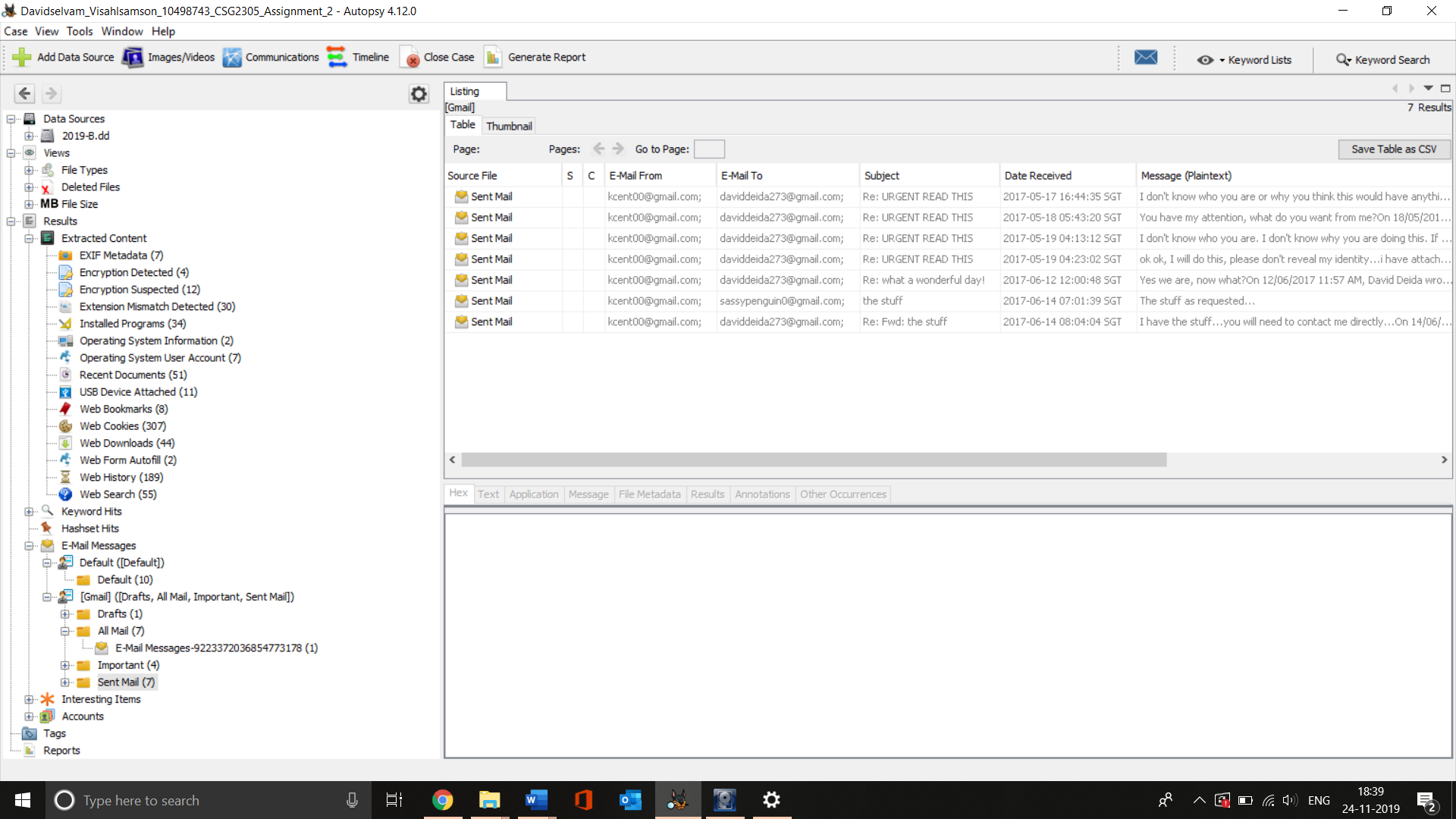
|  |  |  |  |
| --- | --- | --- | --- |
| **Dat** | **URL domain** | **File** | **Path** |
| 2017-05-19 04:20:39 | https://i.ytimg.com/vi/sfA0tZgtSeg/  maxresdefault.jpg | maxresdefault.jpg | C:/Users/computer/Desktop/  maxresdefault.jpg |
| 2017-05-31 06:39:55 | http://static.boredpanda.com/blog/wp-content/uploads/2016/08/cute-kittens-30-57b30ad41bc90\_\_605.jpg | -kittens-30-57b30ad41bc90\_\_605  .jpg | C:/Users/computer/Pictures/  cute-kittens-30-57b30ad41bc90\_\_605.jpg |
| 2017-06-08 08:58:25 | http://stylearena.net/wp-content/uploads/2015/04/cute-cat.jpg | cute-cat.jpg | C:/Users/computer/Pictures/  cute-cat.jpg |
| 2017-06-08 14:46:37 | https://amazinganimalphotos.com/wp-content/uploads/2013/04/cutest-cat-picture-ever.jpg | cutest-cat-picture-ever.jpg | C:/Users/computer/Pictures/  cutest-cat-picture-ever.jpg |
| 2017-06-12 11:58:01 | https://s-media-cache-ak0.pinimg.com/originals/e0/19/4e/  e0194eca1c8135636ce0e014341548c3  .jpg | e0194eca1c8135636ce0e  014341548c3.jpg | C:/Users/computer/Pictures/  e0194eca1c8135636ce0e014  341548c3.jpg |

Table 1.5.2.1 Download history

(Note : Only few downloads are given in table 1.5.2.1)

## 1.6 Email analysis

In this case, I believe that the email conversation I found would play an important role. Because while going through the conversation I have found that the story going to change its direction. The email conversation happened between Clark and person identify himself as Daviddeida273@gmail.com. The below given screenshot 3 is an evidence of conversation and detailed conversation in given in table 1.6.1



Screenshot 3 Quick view of email conversation

|  |  |  |  |
| --- | --- | --- | --- |
| **Date and Time** | **From** | **To** | **Text** |
| 17/05/2017  5:55 PM | Daviddeida273  @gmail.com | Kcent00@gmail.com  (Clark) | Hello Clark or should I call you S....wait wait that would be to easy...I prepared a headline for a future news story...it would be in your best interest to check out the attached file...I've encrypted it using a standard truecrypt file container...the password is how about we use the password superman. I'll be in touch! |
| 17/05/2017  4:44 PM | Kcent00@gmail.com  (Clark) | Daviddeida273@gmail.com  (Blackmailer) | I don't know who you are or why you think this would have anything to do with me, but you have the wrong person. |
| 18/05/2017 10:32 AM | Daviddeida273@gmail.com  (Blackmailer) | Kcent00@gmail.com  (Clark) | You will do precisely as I say or the whole world will know your little secret, superman! |
| 18/05/2017 5:44 AM | Kcent00@gmail.com  (Clark) | Daviddeida273@gmail.com  (Blackmailer) | You have my attention, what do you want from me? |
| 19/05/2017 8:53 AM | Daviddeida273@gmail.com  (Blackmailer) | Kcent00@gmail.com  (Clark) | You are going to locate, download and distribute a minimum of 20 cute cat pictures. Oh and while you are at it, find and throw in a video and some kind of book about cats also! |
| 19/5/2017  4:13 AM | Kcent00@gmail.com  (Clark) | Daviddeida273@gmail.com  (Blackmailer) | I don't know who you are. I don't know why you are doing this. If you are looking for a ransom, I can tell you I don't have any money. But what I do have are a very particular set of skills, skills I have acquired over a very long career. Skills that make me a nightmare for people like you. If you stop this now, that'll be the end of it. I will not look for you, I will not pursue you. But if you don't, I will look for you, I will find you, and I will hurt you. |
| 19/5/2017  7:12 AM | Daviddeida273@gmail.com  (Blackmailer) | Kcent00@gmail.com  (Clark) | 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!  tick tock, tick tock, tick tock |
| 19/5/2017  4:23 AM | Kcent00@gmail.com  (Clark) | Daviddeida273@gmail.com  (Blackmailer) | ok ok, I will do this, please don't reveal my identity...i have attached the first picture |
| 19/5/2017  7:20 AM | Daviddeida273@gmail.com  (Blackmailer) | Kcent00@gmail.com  (Clark) | Good work, keep at it, I’ll be in touch |
| 12/6/2017  11:57 AM | Daviddeida273@gmail.com  (Blackmailer) | Kcent00@gmail.com  (Clark) | How is the task coming along, are we making progress? |
| 12/6/2017  12:00 PM | Kcent00@gmail.com  (Clark) | Blackmailer | Yes we are, now what? |
| 12/6/2017  13:06:59 | Daviddeida273@gmail.com  (Blackmailer) | Kcent00@gmail.com  (Clark) | 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! |
| 14/6/2017  7:01 AM | Kcent00@gmail.com  (Clark) | acquaintance -sassypenguin0@gmail.com | The stuff as requested... |
| 14/6/2017  7:04 AM | acquaintance -  sassypenguin0@gmail.com | Daviddeida273@gmail.com  (Blackmailer) | He has delivered the good! |
| 14/6/2017  7:15:12 | Daviddeida273@gmail.com  (Blackmailer) | Kcent00@gmail.com  (Clark) | Well done Clark...looks like your secret might be safe after all...  I went 20 pictures delivered to me...and then your secret shall remain quiet... |
| 14/6/2017  8:04:04 | Kcent00@gmail.com  (Clark) | Daviddeida273@gmail.com  (Blackmailer) | I have the stuff...you will need to contact me directly... |

Table 1.6.1 Email conversation between clark and david

While going through the conversation I found out that someone identifying themselves as David Deida threatening Clark for some unknown reasons. Also, he demanding Clark to send cats.

# Identification

After analyzing the image files I have found 35 pictures, 29 web history results, 1 encrypted file which comes under illegal category to access, and distribute. Also, I have an email conversation that evidences the transmission of illegal materials. So, it becomes clear that the respective device has been used to store, access, and transmit the illegal materials. When going through the timeline we can see that the case lasts for 70 days.

Also, if the computer has been used by someone other than Clark to access the illegal material in workplace should have reported it immediately.

## Intention

While seeing the evidences found it becomes clear that Clark has purposely accessed, stored, transmitted the illegal files. Along with it we can see that some files include the usage of “Truecrypt” which is basically a utility used to encrypt the data inside a drive/computer which makes the statement stronger.

Also, if malware is claimed for this case it would be false. Because in general malware will access, download, and install random websites, softwares, and files. Whereas in this case all the actions are seems to be done purposely.

# Quantity

|  |  |  |  |
| --- | --- | --- | --- |
| **Type** | **Total files** | **Illegal contents** | **Illegal contents (%)** |
| Photos | 22344 | 35 | 0.15734580111491 |
| Videos | 404 | 0 | 0% |
| Audio | 392 | 0 | 0% |
| Archives | 435 | 1 | 0.22988505747126% |
| Databases | 108 | 1 | 0% |
| Plain Text | 246 | 1 | 0.4065% |
| HTML | 832 | 31 | 3.7259615384615% |
| PDF | 2 | 1 | 50% |
| Office | 65 | 1 | 1.5384% |
| Total | 244828 | 71 | 0.028999950985998% |

Table 2.1

# Software installed

Apart from pre-installed/default softwares that comes with device I have found 4 softwares that are installed. All these 4 softwares are used in this case.

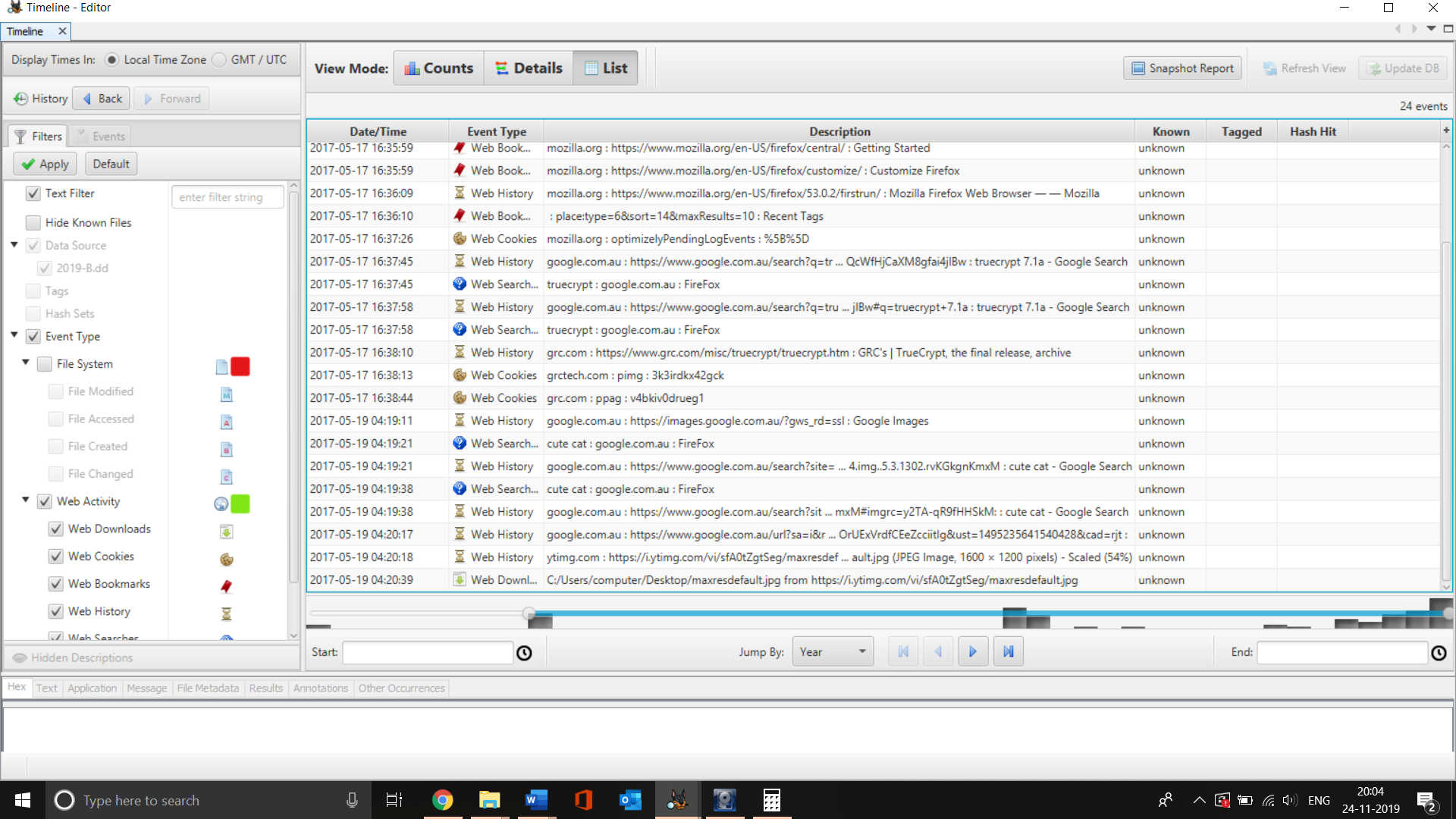
1. 7Zip – This is basically a file achiever. The zip file (thestuff.zip) listed previously created with the use of 7Zip.

2. Mozilla Firefox – It’s a web browser. All the actions/evidences mentioned previously in web evidence accessed through this software.

3. Mozilla thunderbird – It’s an email client. The entire email conversation listed previously was carried-on in this software.

4. Truecrypt – Utility software to encrypt the data/drive in a system. This has been used while sending the illegal contents to David. Also, the license file inside the truecrypt folder confirms the usage of it.

## Timeline of events



Screenshot 4 Timeline Autopsy

Screenshot 4 shows the timeline of event map generated in Autopsy after Clark received the email. The detailed timeline of events listed in following table 2.2

|  |  |  |  |
| --- | --- | --- | --- |
| **Date and Time** | **Time** | **Incident** | **Evidence (Can be found under)** |
| 17 May | 5:55 PM | Clark receiving first email from David which has encrypted file attached with it. Also, usage of the file through Truecrypt | Email, Encrypted File |
| 18 May | 10:32 AM | Clark getting threaten by David | Email |
| 19 May | 4:19 AM | Clark refusing to listen David | Email |
| 8:53 AM | Clark asksed by David to distribute 20 illegal contents | Email |
| 9:12 AM | Clark used Firefox and searched cute cat then sent that to David | Email, Web History |
| 31 May | 6:37 AM | Clark used firefox and searched cat video in Youtube | Web History |
| 6:39 AM | Clark used firefox to searched cute kitten and downloaded image | Web History, Picture |
| 8 June | 8:56 AM | Clark used firefox and accessed www.cutestpaw.com/tag/cats/ | Web History |
| 8:57 AM | Clark used firefox and google searched cute cat pictures | Web History |
| 8:58 AM –  2:46 PM | Clark used firefox and downloaded a cat picture then stored into picture folder | Picture |
| 12 June | 11:57 AM | Clark asked by David regarding the progress. Then Clark used firefox and google searched funny cat pictures  David said clark to send few illegal contents to sassypenguin0@gmail.com. | Email, Web History |
| 11:58 AM –  12:03 PM | Clark used firefox and google searched cat pictures via then downloaded several pictures into pictures folder | Web History, Picture |
| 14 June | 7:01 AM | Clark compressed the pictures into thestuff.zip using 7 Zip and mailed it to | Compressed File, Email |
| 7:04 AM | Sassy Penguin has forwarded Clark’s mail thestuff.zip to David. | Email |
| 7:15 AM | Clark asked by David to contact him directly | Email |
| 7:39 AM –  8:00 AM | Clark used firefox then accesses and downloaded more pictures on pictures folder | Web History,  Picture |
| 7:56 AM –  8:01 AM | Clark used firefox searched funny cat videos in YouTube and saved the Video link in link.txt file. | Website |
| 9:10 AM | Clark used firefox and searched cat adoption perth | Web Form Autofill |
| 11:15 AM | Clark accessed used Firefox to access cat image. | Picture |
| 27 July | 1:25 PM –  1:32 PM | Clark used Firefox and accessed www.cathaven.com.au. | Web History, Picture |

Table 2.2 Time line event

# Running sheet

The running sheet provided in table 1.6.3 consists the activities I have done from the beginning.

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Date** | **Time** | **Action** | **Motive** | **Tools utilized** | **Time Taken** |
| 31/10/2019 | 18:00 | Downloaded the following image files from ECU Blackboard.  2019-B.7z.002 (1,000 MB)   2019-B.7z.005 (1,000 MB)   2019-B.7z.001 (1,000 MB)   2019-B.7z.003 (1,000 MB)   2019-B.7z.007 (656.284 MB)   2019-B.7z.004 (1,000 MB)   2019-B.7z.006 (1,000 MB) | To start the forensics analysis process | Google Chrome | 1 hour |
| 19:00 | Extracted the files | To get final image file to analyze | 7 ZIP | 15 Minutes |
| 19:20 | Checked the Hash Value | To ensure the integrity is mainteined | 7 ZIP SHA | 15 Minutes |
| 19:45 | Created copy of the file and check the hash value | To ensure the the copy has not corrupted | 7 ZIP | 30 Minutes |
| 01/11/2019 | 08:00 | Installed Autopsy, OS forensics | To investigate the image file | Downloaded using google chrome | 2.15 hours |
| 03/11/2019 | 11:15 | Started Autopsy and created project with the image file | To start the analysis | Autopsy | 20 Minutes |
|  | 11:40 | Searched “Cat” in autopsy search | To search all the files relevant to Cat | Autopsy | 10 Minutes |
|  | 11:50 | Documented the image file findings | To submit the evidence | Microsoft office word | 2 Hours |
|  | 14:00 | Searched “Kitten” in autopsy search | To get all the images relevant to kitten | autopsy | 10 Minutes |
|  | 14:10 | Documented the image file findings | To submit the evidence | Microsoft office word | 10 Minutes |
| 04/11/2019 | 10:00 | Started OS forensics and created new project using the image file | To start the analysis | OS Forensics | 10 Minutes |
|  | 10:15 | Analysed the results in OS forensics | To ensure two softwares showing same evidences | OS Forensics | 1 Hour |
| 14/11/2019 | 08:15 | Gone through the image file to get web evidences | To get all the web evidences | autopsy | 2 Hours |
|  | 11:40 | Documented all the web evidences | To submit the evidence | Microsoft office word | 2 Hours |
| 16/11/2019 | 15:00 | Investigate the encrypted files, software used in the computer, email evidence | To find the evidences inside the encrypted file, email and from the software | Autopsy | 3 hours |
| 17/11/2019 | 20:00 | Documenting the findings | To submit the evidence | Microsoft office word |  |

Table 2.3 Running sheet

# References

Sammons, J. (2015). The basics of digital forensics. Amsterdam: Syngress Media.

Carrier, B. (2005). File system forensic analysis. Boston, Mass.: Addison-Wesley.

Martin, B. (2011). OSForensics, System Information Gathering Software - gHacks Tech News. Retrieved from <https://www.ghacks.net/2011/06/28/os-forensics-system-information-gathering-software/>

Gerard Johansen. (2017). Digital Forensics and Incident Response. Packt Publishing.