A blue text on a white background

Description automatically generated

Bachelor with Science with Honors in

Cybersecurity

Module Code: **CF ( 501 IT)**

Title: **Clowning About Again**

Module: **Computer Forensics**

Name: **Kaung Myat San**

Student Number: **8580LS1A**

Campus: **Psb Academy(Stem Campus)**

Lecturer: **Zulkifli Jalil**

17th August 2023

Table of Contents

[Summary 3](#_Toc144119532)

[Introduction 4](#_Toc144119533)

[Issue #1- Contents relating to offence. 4](#_Toc144119534)

[Issue #2(a) Identification of Evidence ownership: Defined by Email records. 16](#_Toc144119535)

[Issue #2(b) Identification of Evidence ownership: Defined by analyzed Documents 18](#_Toc144119536)

[Issue #3(a) The accused’s Intent: Defined by Email records 19](#_Toc144119537)

[Issue #3(b) The accused’s Intent: Defined by a photo in Microsoft word hidden inside encrypted virtual disk “usb” 21](#_Toc144119538)

[Issue #3(c) The accused’s Intent: Defined by internet history he explored and downloaded 22](#_Toc144119539)

[Issue #4- Quantity of Files on acquired forensic Image(Percentage of relevant files to case) 26](#_Toc144119540)

[Issue #5- Installed software on system 27](#_Toc144119541)

[Conclusion 28](#_Toc144119542)

[References 28](#_Toc144119543)

[Appendix A - Running Sheet 29](#_Toc144119544)

[Appendix B – Timeline of events 42](#_Toc144119545)

# Summary

This report aims to analyze the forensic image of Clark's computer, as I was tasked with investigating potential evidence of accessing clown-related content. I undertook this task applying the processes of forensic investigation. I began by identifying the seized computer, followed by meticulous data preservation to ensure integrity during analysis. Subsequently, I thoroughly documented the analyzed data for the final presentation phase.

The system under examination operated in the GMT +08:00(Singapore) time zone, within forensic tools like Autopsy same as western Australia time zone. I unzipped the given file and got 202.dd forensic image and created a new case using beautiful forensic tool Autopsy version 4.20.0. Extracted the contents relating to offence and preserved in a specific folder for further steps. I did the extraction easily with the help of autopsy’s functionalities. I employed built-in ‘certUtil’ to compute the hash values for the images, and I utilized the 'john the ripper' tool to decrypt the password-secured images. Subsequently, I located email correspondences involving Clark, Sassy Penguin (Clark 's superior), and Jerry Simpsons using the Thunderbird application, which is employed for email communication. In those email records, it became apparent that Jerry Simpsons was forcing Clark to access the content related to clowns. I found Clark explored clown contents through internet and downloaded by analyzing the internet history. During my analysis through the preserved and extracted data, I found 2 suspicious encrypted virtual disks called “usb” and “system” I tried to open them with every possible way. Then, john the ripper worked on cracking those and got passwords of each file ‘planet’, ‘redballoon’ respectively. I used TrueCrypt tool to check what contains in them, but “system” disk did not contain any files in it while I got 3 evidence Microsoft word files from “usb” disk. Those doc files revealed that Clark Kent was famous “superman” who was hiding from public eyes and a man found out him and blackmailed. I documented every single clown related image, pdfs, videos, log files, internet history, software installed for further presentation phase.

This report analyzed Clark's computer for evidence of accessing clown-related content. The investigation followed forensic processes, revealing coerced actions through email correspondence. Functionalized tools like Autopsy aided analysis. Encrypted disks were decrypted, exposing passwords and significant documents. I analyzed thoroughly from extracted data and found clues. The findings disclosed Clark's dual identity as "superman" and a blackmail situation not because of malware attack. Comprehensive documentation included multimedia, logs, and software records, forming the basis for my presentation.

# Introduction

According to Vacca, J. R. (2005). *Computer Forensics: Computer Crime Scene Investigation* (2nd ed.), “Computer forensics, also referred to as computer forensic analysis, electronic discovery, electronic evidence discovery, digital discovery, data recovery, data discovery, computer analysis, and computer examination, is the process of methodically examining computer media (hard disks, diskettes, tapes, etc.) for evidence. A thorough analysis by a skilled examiner can result in the reconstruction of the activities of a computer user. The selection of technology is often the hardest for any forensic examiner as there are many excellent choices out there. There are some basic rules that can be applied to be able to weed through the variety of materials on each of the tools available to help select the best options.”

# Issue #1- Contents relating to offence.

[To Top of the Document](#_top)

|  |  |  |
| --- | --- | --- |
| A cartoon clown with a hat and a flower in his hair  Description automatically generated | **File Name** | **k7827739.jpg** |
| Type | jpeg |
| Location | /202.dd/Users/computer/Desktop/ |
| Status | Allocated |
| MD5 | 39db918c4014d3a64fabbc17a2fe49a7 |
| Accessed | 2018-07-02 09:22:14 SGT |
| Created | 2018-07-02 09:22:14 SGT |
| Modified | 2018-07-02 09:22:15 SGT |
| Changed | 2018-07-02 09:22:15 SGT |
| Size (bytes) | 41284 |
| **Finding 1** | Cartoon clown  Source : https://fscomps.fotosearch.com/compc/CSP/CSP782/clown-clipart\_\_k7827739.jpg | |

|  |  |  |
| --- | --- | --- |
| A clown with orange hair and a purple collar  Description automatically generated | **File Name** | **k13320412.jpg** |
| Type | jpeg |
| Location | /202.dd/Users/computer/Desktop |
| Status | Allocated |
| MD5 | e5ab36f6264d22714a88d53338469f95 |
| Accessed | 2018-07-02 09:15:08 SGT |
| Created | 2018-07-02 09:15:08 SGT |
| Modified | 2018-07-02 09:15:08 SGT |
| Changed | 2018-07-02 09:15:08 SGT |
| Size (bytes) | 35546 |
| **Finding 2** | Cartoon clown  Source : https://fscomps.fotosearch.com/compc/CSP/CSP992/a-clownwearing-a-green-costume-clipart\_\_k13320412.jpg | |

|  |  |  |
| --- | --- | --- |
| A cartoon clown with a hat  Description automatically generated | **File Name** | **k14032380.jpg** |
| Type | jpeg |
| Location | /202.dd/Users/computer/Desktop/ |
| Status | Allocated |
| MD5 | 913cb94539abfe8de858ce16c0a40e99 |
| Accessed | 2018-07-02 09:21:52 SGT |
| Created | 2018-07-02 09:21:52 SGT |
| Modified | 2018-07-02 09:21:52 SGT |
| Changed | 2018-07-02 09:21:53 SGT |
| Size (bytes) | 31837 |
| **Finding 3** | Cartoon clown  Source : https://fscomps.fotosearch.com/compc/CSP/CSP992/clown-faceclipart\_\_k14032380.jpg | |

|  |  |  |
| --- | --- | --- |
| A cartoon clown holding a banjo  Description automatically generated | **File Name** | **index.jpg** |
| Type | jpeg |
| Location | /202.dd/Users/computer/Desktop/ |
| Status | Allocated |
| MD5 | 64b61cf19e916bc1a40831a17db83b3b |
| Accessed | 2018-07-02 09:12:30 SGT |
| Created | 2018-07-02 09:12:29 SGT |
| Modified | 2018-07-02 09:12:30 SGT |
| Changed | 2018-07-02 09:12:30 SGT |
| Size (bytes) | 15015 |
| **Finding 4** | Cartoon clown  Source : https://www.fotosearch.com/ | |

|  |  |  |
| --- | --- | --- |
|  | **File Name** | **Ronald\_mcdonald-e1476200032847-660x330.jpg** |
| Type | jpeg |
| Location | /202.dd/Users/computer/Pictures/ |
| Status | Allocated |
| MD5 | a3f7eb7ba08cb84137a85bf4683c6bca |
| Accessed | 2018-06-19 07:50:41 SGT |
| Created | 2018-06-19 07:50:41 SGT |
| Modified | 2018-06-19 07:50:42 SGT |
| Changed | 2018-06-19 07:50:42 SGT |
| Size (bytes) | 26494 |
| **Finding 5** | Clown in MacDonald uniform. Source : http://theredshtick.com/wp-content/uploads/2016/10/Ronald\_mcdonalde1476200032847-660x330.jpg | |

|  |  |  |
| --- | --- | --- |
|  | **File Name** | **kikkii\_clown\_party\_pose.jpg** |
| Type | jpeg |
| Location | /202.dd/Users/computer/Pictures/ |
| Status | Allocated |
| MD5 | 76e4975e5efc2a1268584fef7ade5f59 |
| Accessed | 2018-06-19 07:50:06 SGT |
| Created | 2018-06-19 07:50:05 SGT |
| Modified | 2018-06-19 07:50:06 SGT |
| Changed | 2018-06-19 07:50:06 SGT |
| Size (bytes) | 50304 |
| **Finding 6** | Random clown Source : http://www.trickortreatmagic.com.au/img/kikkii\_clown\_party\_pose.jpg | |

|  |  |  |
| --- | --- | --- |
|  | **File Name** | **1492447345937.jpg** |
| Type | Jpeg |
| Location | /202.dd/Users/computer/Pictures/ |
| Status | Allocated |
| MD5 | 3e58af33ebb789d5d81cb4ac613a76c9 |
| Accessed | 2018-06-18 08:22:15 SGT |
| Created | 2018-06-18 08:22:15 SGT |
| Modified | 2018-06-18 08:22:15 SGT |
| Changed | 2018-06-18 08:22:16 SGT |
| Size (bytes) | 17134 |
| **Finding 7** | Donald Trump in clown form  Source : https://static1.squarespace.com/static/530becede4b093256168fba5/t/58f4f06d15d5d b5e25316c1e/1492447345937/ | |

|  |  |  |
| --- | --- | --- |
|  | **File Name** | **s-l640.jpg** |
| Type | Jpeg |
| Location | /202.dd/Users/computer/Pictures/ |
| Status | Allocated |
| MD5 | dd42fe966af825567338e4f873cc2f6a |
| Accessed | 2018-06-19 07:50:17 SGT |
| Created | 2018-06-19 07:50:17 SGT |
| Modified | 2018-06-19 07:50:17 SGT |
| Changed | 2018-06-19 07:50:17 SGT |
| Size (bytes) | 57620 |
| **Finding 8** | Random clown Source : https://ssli.ebayimg.com/images/g/2vUAAOSwxp9W8gwu/s-l640.jpg | |

|  |  |  |
| --- | --- | --- |
|  | **File Name** | **scaryclown.jpg** |
| Type | jpeg |
| Location | /202.dd/Users/computer/Pictures/ |
| Status | Allocated |
| MD5 | ed873fc7b1f226bda891c1780341cdb2 |
| Accessed | 2018-06-18 08:20:05 SGT |
| Created | 2018-06-18 08:20:04 SGT |
| Modified | 2018-06-18 08:20:06 SGT |
| Changed | 2018-06-18 08:20:06 SGT |
| Size (bytes) | 58423 |
| **Finding 9** | Scary clown  Source : http://www.scarymommy.com/wp-  content/uploads/2016/10/scaryclown.jpg?w=697 | |

|  |  |  |
| --- | --- | --- |
|  | **File Name** | **scary-halloween-costumes-ideas-Clown-blood-Halloweenparty-costumes-e1410943909179.jpg** |
| Type | jpeg |
| Location | /202.dd/Users/computer/Pictures/ |
| Status | Allocated |
| MD5 | 51632444d9845cc6686adcf24e536f77 |
| Accessed | 2018-06-18 08:21:54 SGT |
| Created | 2018-06-18 08:21:54SGT |
| Modified | 2018-06-18 08:21:55 SGT |
| Changed | 2018-06-18 08:21:55 SGT |
| Size (bytes) | 59178 |
| **Finding 10** | Scary clown  Source : https://deavita.net/wp-content/uploads/2014/09/scary-halloweencostumes-ideas-Clown-blood-Halloween-party-costumese1410943909179.jpg | |

|  |  |  |
| --- | --- | --- |
| A clown with a hat and a blue hat  Description automatically generated | **File Name** | **image-20160926-31853-1jvhtv4.jpg** |
| Type | jpeg |
| Location | |  | | --- | | /202.dd/Users/computer/Documents/html/The psychology behind why clowns creep us out\_files/ | |
| Status | Allocated |
| MD5 | 98741fa7cb0b1b74bcc9b7e1d63d2fd0 |
| Accessed | 2018-06-18 10:51:12 SGT |
| Created | 2018-06-18 10:51:12 SGT |
| Modified | 2018-06-18 10:51:12 SGT |
| Changed | 2018-06-18 10:51:12 SGT |
| Size (bytes) | |  | | --- | | 22894 | |
| **Finding 11** | Clown painting  Source : http://theconversation.com/the-psychology-behind-why-clowns-creep-us-out-65936 | |

|  |  |  |
| --- | --- | --- |
|  | **File Name** | **A Little Night Music - Send In The Clowns.pdf** |
| Type | pdf |
| Location | /202.dd/Users/computer/Downloads/ |
| Status | Allocated |
| MD5 | 4f640bc32c0ac35b585a814ee5235df4 |
| Accessed | 2018-06-19 07:44:24 SGT |
| Created | 2018-06-19 07:44:24 SGT |
| Modified | 2018-06-19 07:44:31 SGT |
| Changed | 2018-06-19 07:44:31 SGT |
| Size (bytes) | 3146439 |
| **Finding 12** | Some musical notes with the header relating to clowns  Source : https://www.docdroid.net/bbvy/a-little-night-music-send-in-the-clowns.pdf | |

|  |  |  |
| --- | --- | --- |
|  | **File Name** | **Couto, Mia.pdf** |
| Type | pdf |
| Location | /202.dd/Users/computer/Downloads/ |
| Status | Allocated |
| MD5 | 96ac7e4f3c457773557837a2bf36368c |
| Accessed | 2018-06-19 07:46:29 SGT |
| Created | 2018-06-19 07:46:29 SGT |
| Modified | 2018-06-19 07:46:34 SGT |
| Changed | 2018-06-19 07:46:34 SGT |
| Size (bytes) | 118913 |
| **Finding 13** | A story relating to clowns in pdf format.  Source : https://www.massreview.org/sites/default/files/Couto,%20Mia.pdf | |

|  |  |  |
| --- | --- | --- |
| A picture containing text, outdoor, person  Description automatically generated | **File Name** | **Clowns dancing.mp4** |
| Type | mp4 |
| Location | /202.dd/Users/computer/Downloads/ |
| Status | Allocated |
| MD5 | 071f555cf58073ed4ebfb92915a8491a |
| Accessed | 2018-06-18 10:45:41 SGT |
| Created | 2018-06-18 10:45:41 SGT |
| Modified | 2018-06-18 10:45:47 SGT |
| Changed | 2018-06-18 10:48:12 SGT |
| Size (bytes) | 3324223 |
| **Finding 14** | Two clown dancing video  Source : unknown | |

# Issue #2(a) Identification of Evidence ownership: Defined by Email records.

[To Top of the Document](#_top)

It can be proven that the evidence belonged to Clark through an examination of the email records that indicate his coerced actions in exploring and downloading clown-related content over the internet under the email account [jazzasimpson0000@gmail.com](mailto:jazzasimpson0000@gmail.com) holder’s coercion.

|  |  |  |  |
| --- | --- | --- | --- |
|  | **Email record 1** | | |
| **To** | kcent00@gmail.com | **From** | sassypenguin0@gmail.com |
| **Date/Time** | 3/05/2018 8:12 AM | **Subject** | Recent data breach |
| **Body** | Clark,  As a result of our recent minor security breach I am asking everyone to protect their data, Jimmy here suggested using a tool TrueCrypt. You're a clever boy, I'm sure you can figure out how to use it. Regards,  Chief | | |
| **Analysis** | - Clark’s chief order to Clark.  -This email might be the earliest one in this case as it date mentioned as 3/05/2018 probably 3rd May 2018 Before Clerk went to hang out with his chief | | |

|  |  |  |  |
| --- | --- | --- | --- |
|  | **Email record 2** | | |
| **To** | sassypenguin0@gmail.com | **From** | kcent00@gmail.com |
| **Date/Time** | Wed, 11 Jul 2018 08:11:46 +0800 | **Subject** | Re: Recent data breach |
| **Body** | Hi Chief,  I go to work today, and I think my computer has been hacked. There is all this dodgy content on the computer that I didn't put there. I don't know what to do...I will come by your office in a few minutes! | | |
| **Analysis** | Clerk’s report about his computer got hacked to Chief after he had got no idea what to do then | | |

|  |  |  |  |
| --- | --- | --- | --- |
|  | **Email record 3** | | |
| **To** | kcent00@gmail.com | **From** | jazzasimpson0000@gmail.com |
| **Date/Time** | clowning about | **Subject** | 18/06/2018 11:11 AM |
| **Body** | stop clowning about and start working like a superman :) | | |
| **Analysis** | Forcing clerk to access more clown contents like superman | | |

|  |  |  |  |
| --- | --- | --- | --- |
|  | **Email record 4** | | |
| **To** | jazzasimpson0000@gmail.com | **From** | kcent00@gmail.com |
| **Date/Time** | Mon, 2 Jul 2018 10:20:09 +0800 | **Subject** | Re: clowning about |
| **Body** | How many am I send you and how do I get it to you? | | |
| **Analysis** | Clerk asking how to send contents to Jerry Simpson and quantity | | |

|  |  |  |  |
| --- | --- | --- | --- |
|  | **Email record 5** | | |
| **To** | kcent00@gmail.com | **From** | jazzasimpson0000@gmail.com |
| **Date/Time** | 3/07/2018 7:00 AM | **Subject** |  |
| **Body** | The quantity here is relevant, just keep accessing/downloading the content and I will be in touch! | | |
| **Analysis** | Jerry Simpson replied clerk to just keep accessing clown contents and did not mentioned how much | | |

|  |  |  |  |
| --- | --- | --- | --- |
|  | **Email record 6** | | |
| **To** | jazzasimpson0000@gmail.com | **From** | kcent00@gmail.com |
| **Date/Time** | Mon, Jul 9, 2018, at 11:24 AM | **Subject** | Re: clowning about |
| **Body** | I am done with this game. This is what I got, now leave me alone!!!!!(With attachment – zip file) | | |
| **Analysis** | Clerk sent contents with zip file and told to stop blackmailing | | |

|  |  |  |  |
| --- | --- | --- | --- |
|  | **Email record 7** | | |
| **To** | jazzasimpson0000@gmail.com | **From** | kcent00@gmail.com |
| **Date/Time** | Mon, Jul 10, 2018, at 09:41  AM | **Subject** | Re: clowning about |
| **Body** | No, no, you are not done, I want more, more clown content! | | |
| **Analysis** | As usual way blackmailer do, he did not stop and kept coercing | | |

# Issue #2(b) Identification of Evidence ownership: Defined by analyzed Documents

[To Top of the Document](#_top)

As well as by reviewing the Microsoft Word documents, it is his diary and in it he opened the ‘usb’ file and read the documents, wrote note about illegality of clowns.

|  |  |
| --- | --- |
| File Name | **Journal.doc** |
| Type | Microsoft word |
| Location | /202.dd/Users/computer/Documents/ |
| Status | Allocated |
| MD5 | c53b7d63c8a0787b897584819a4f8d0f |
| Accessed | 2018-05-02 12:23:52 SGT |
| Created | 2018-05-02 12:23:52 SGT |

Screens screenshot of a screenshot of a screenshot of a screenshot of a screenshot of a screenshot of a screenshot of a screenshot of a screenshot of a screenshot

Description automatically generated

# Issue #3(a) The accused’s Intent: Defined by Email records

[To Top of the Document](#_top)

|  |  |  |  |
| --- | --- | --- | --- |
|  | **Email record 1(Intent)** | | |
| **To** | kcent00@gmail.com | **From** | jazzasimpson0000@gmail.com |
| **Date/Time** | clowning about | **Subject** | 18/06/2018 11:11 AM |
| **Body** | stop clowning about and start working like a super man :) | | |
| **Analysis** | First mail after the date of Clerk opening usb drive by Jerry Simpson. | | |

|  |  |  |  |
| --- | --- | --- | --- |
|  | **Email record 2(Intent)** | | |
| **To** | jazzasimpson0000@gmail.com | **From** | kcent00@gmail.com |
| **Date/Time** | Mon, 2 Jul 2018 10:20:09 +0800 | **Subject** | Re: clowning about |
| **Body** | How many am I send you and how do I get it to you? | | |
| **Analysis** | Clerk asking how to send contents to Jerry Simpson and quantity | | |

|  |  |  |  |
| --- | --- | --- | --- |
|  | **Email record 3(Intent)** | | |
| **To** | kcent00@gmail.com | **From** | jazzasimpson0000@gmail.com |
| **Date/Time** | 3/07/2018 7:00 AM | **Subject** |  |
| **Body** | The quantity here is relevant, just keep accessing/downloading the content and I will be in touch! | | |
| **Analysis** | Forcing clerk to keep accessing clown contents no matter how much | | |

|  |  |  |  |
| --- | --- | --- | --- |
|  | **Email record 4(Intent)** | | |
| **To** | jazzasimpson0000@gmail.com | **From** | kcent00@gmail.com |
| **Date/Time** | Mon, Jul 9, 2018 at 11:24 AM | **Subject** | Re: clowning about |
| **Body** | I am done with this game. This is what I got, now leave me alone!!!!!(With attachment – zip file) | | |
| **Analysis** | Clerk replied with clown contents in zip file and told to stop coercing | | |

|  |  |  |  |
| --- | --- | --- | --- |
|  | **Email record 5(Intent)** | | |
| **To** | jazzasimpson0000@gmail.com | **From** | kcent00@gmail.com |
| **Date/Time** | Mon, Jul 10, 2018 at 09:41 AM | **Subject** | Re: clowning about |
| **Body** | No, no, you are not done, I want more, more clown content! | | |
| **Analysis** | Jerry replied and did not stop | | |

# Issue #3(b) The accused’s Intent: Defined by a photo in Microsoft word hidden inside encrypted virtual disk “usb”

[To Top of the Document](#_top)

|  |  |  |  |
| --- | --- | --- | --- |
| A screenshot of a video game  Description automatically generated | | File Name | **open-me-third.doc** |
| Type | doc |
| Location | Encrypted virtual disk “usb” |
| Status | Allocated |
| MD5 | a77ee19d8c6264e88098bafc0b36805e |
| Accessed | 2018-06-18 |
| Created | 6/7/2018 8:56:26 AM |
| Modified | 6/7/2018 7:37:44 AM |
| Changed | 6/7/2018 7:37:44 AM |
| Size  (bytes) | 197,120 |
| Sectors | 1,608 |
| **Analysis** | This evidence shows Clerk intent clearly that he afraid of revealing his true identity “superman”, so he chose to explore and downloaded the clown contents as Simpson said | | |

# Issue #3(c) The accused’s Intent: Defined by internet history he explored and downloaded

I put every Description, Search engine used, downloaded file, time, URL of Clark’s internet history in table in image form.

A screenshot of a black table with white text

Description automatically generated

A black screen with white text

Description automatically generated

A screenshot of a black and white list

Description automatically generated

A screenshot of a black and white list

Description automatically generated

A screenshot of a black and white screen

Description automatically generated

# Issue #4- Quantity of Files on acquired forensic Image(Percentage of relevant files to case)

[To Top of the Document](#_top)

|  |  |  |
| --- | --- | --- |
| **Types** | **Number of offence files** | **Files in System** |
| **Images** | 9(excluding redundant images) | 51334 |
| **Videos** | 1 | 434 |
| **Audio** | 0 | 380 |
| **Database** | 1 | 115 |
| **HTML** | 1 | 905 |
| **Office** | 1 | 27 |
| **Pdfs** | 4 | 13 |
| **Plain Texts** | 0 | 311 |
| **Archives** | 1 | 669 |
| **Executable File - exe** | 0 | 3098 |
| **Executable File - bat** | 0 | 20 |
| **Executable File - com** | 0 | 23 |
| **Executable File - dll** | 0 | 21550 |
| **Executable File - cmd** | 0 | 10 |

Among all files in disk, 0.0224% relevant to the offence case.

# Issue #5- Installed software on system

[To Top of the Document](#_top)

|  |  |  |  |
| --- | --- | --- | --- |
| **Date** | **Time** | **Program Name** | **Analysis** |
| 2018-06-07 | 08:53:48  SGT | TrueCrypt.exe | Software used to create encrypted virtual disks and securing data with: encryption and password protection. |
| 2018-07-03 | 09:12:10  SGT | mirc752.exe | IRC software |
| 2018-06-18 | 13:22:40  SGT | bfgminer | Potential Malware verified by virustotal.  https://www.virustotal.com/gui/file/df3a7bcb  cbca64bb750b9e82fa00685a91846aa6b05e876dbf887eb 16c74ca07 |
| 201805-03 | 07:57:41  SGT | Microsoft Thunder Bird | Email software |
| 2018-07-02 | 09:03:02  SGT | Steghide | Steganographic software |

# Conclusion

In this investigation, I applied 5 phases of computer forensic. I first make sure the integrity of evidence and materials by saving the MD5 hash values, identified suspect’s information, extracted data, and filtered offended data, analyzed, documented and prepared for presentation. The knowledge I gained from doing this report “What digital forensic is”, “password cracking techniques”, “leant to use forensic tools well”, “understood deeper to phases of digital forensic”, “learnt integrity of every single file is important” and “evidence should not be on logical assumptions”.

# References

Vacca, J. R. (2005). *Computer Forensics: Computer Crime Scene Investigation* (2nd ed.). Cengage Learning.

Maras, M.-H. (2014). *Computer Forensics: Cybercriminals, Laws, and Evidence* (2nd ed.). Jones & Bartlett Learning.

# Appendix A - Running Sheet

[To Top of the Document](#_top)

|  |  |  |
| --- | --- | --- |
| **Date/Time** | **Duration** | **Justification of my work** |
| **18thAugust**  **2023**  **13:21:00 SGT** | 43 mins | First of all, I downloaded all fragmentation of 202.7z.001 to 202.7z.008 file to my computer and combined all fragments, unzipped and I got 202.dd file  I duplicated the file and renamed one as 202\_original.dd and left that alone and changed permission of both to read-only mode.  I used the copied version “202.dd” for next steps and disconnect my window from internet for forensic safety practice(I used window in virtual machine) |

|  |  |  |
| --- | --- | --- |
| **18thAugust**  **2023**  **14:05:00 SGT** | 10 mins | I used built in hash generator called certUtil to generate hash value of 202.dd file and stored hash in a safe text file for further integrity check  A screenshot of a computer  Description automatically generated |
| **18thAugust**  **2023**  **14:15:00 SGT** | 1 mins | Right click the original\_hash.txt and click read-only in properties of file  To keep all metadata unchanged |
| **18thAugust**  **2023**  **14:10:00 SGT** | 4 hours | And then I installed the autopsy 4.20.0 and started to open case with the name “Clerk”  Ingesting of all files took 4hours to complete.  While ingesting I exported some available files appeared |
| **18thAugust**  **2023**  **18:10:00 SGT** | 7mins | I checked the NTUSER.dat and found the computer name and also time zone of the computer the last time use  A screenshot of a computer  Description automatically generatedA screenshot of a computer  Description automatically generated |
| **18thAugust**  **2023**  **18:20:00 SGT** | 3mins | Subsequently, I searched for potentially concerning files within the \202.dd\Users\computer directory, Clerk Kent's default directory. Within Autopsy, I analyzed the contents of the Desktop folder, where I encountered four cartoon clown images, a compressed zip file, and an encrypted image of a USB drive. |

|  |  |  |
| --- | --- | --- |
|  |  |  |
| **18thAugust**  **2023**  **18:30:00 SGT** | 3 mins | I exported the k13320412.zip and extracted the zip file and analyzed  I found 2 pdf files and 1 video file, 9 clown relating jpeg files. |
|  |  | A screenshot of a computer  Description automatically generated |

|  |  |  |
| --- | --- | --- |
| **18thAugust**  **2023**  **18:33:00 SGT** | 3 mins | I first exported “usb” from disk using autopsy  And generated the md5 hash of the “usb” before I handle to ensure the integrity of the evidence |
| **18thAugust**  **2023**  **18:36:00 SGT** | 20 mins | I generated ‘usb’ file’s hash value with truecrypt2john.py to write into clerkusb.txt    Then I cracked that hash using john the ripper dictionary attack using popular rockyou.txt and got the password (planet)  A screenshot of a computer program  Description automatically generated |
| **18thAugust**  **2023**  **19:00:00 SGT** | 12mins | I downloaded TrueCrypt software and selected the usb file and mounted using the cracked password “planet”  Then I found 3 interesting Microsoft document and found the key useful evidence |

|  |  |  |
| --- | --- | --- |
| **18thAugust**  **2023**  **19:13:00 SGT** | 6mins | After that, found some html files inside the Documents Folder and saw it was about a psychology page of some knowledge byFrank T. McAndrew and Cornelia H. Dudley Professor of Psychology, Knox College  A screenshot of a computer  Description automatically generated |

|  |  |  |
| --- | --- | --- |
| **18thAugust**  **2023**  **19:20:00 SGT** | 4mins | Then again I found 6 clown images in Pictures folder |

|  |  |  |
| --- | --- | --- |
| **18thAugust**  **2023**  **19:24:00 SGT** | 3mins | It’s convenient to find records like emails using autopsy as it categorized thoroughly |
| **18thAugust**  **2023**  **19:30:00 SGT** | 10mins | It took me some minutes to read all the mails and figured out that emails records are relevant to offence of accessing clowns in respective ways |
| **18thAugust**  **2023**  **19:40:00 SGT** | 6mins | Then I analyzed Web related contents using autopsy functionality the left side just like the way I had done with emails.  And I saw evidence Clerk searching for clown contents and downloaded the clown relating contents,  Also, some clues like the download of some software and browsing about erasing his disk |
|  |  |  |

|  |  |  |
| --- | --- | --- |
| **18thAugust**  **2023**  **19:46:00 SGT** | 6mins | Then I checked every single folders in his home directory (computer) and found an software called bfgminer.exe  Potential bitcoin mining trojan and also journel.doc |
| **18thAugust**  **2023**  **19:52:00 SGT** | 4 mins | I exported the bgfminer.exe the place I found and drop it in website malware analysis tool called HYBRID ANALYSIS and it showed malicious  Maybe Clark tried of convincing others that he was infected with some kind of malware like trojan, and clown contents were coming from that trojan along with bitcoin mining software  A screenshot of a computer  Description automatically generated |
| **18thAugust**  **2023**  **19:56:00 SGT** | 7 mins | I read that document and found that he read the contents in ‘usb’ and started accessing to clown contents  Also wrote about illegality of clowns Screens screenshot of a screenshot of a screenshot of a screenshot of a screenshot of a screenshot of a screenshot of a screenshot of a screenshot of a screenshot  Description automatically generated |

# Appendix B – Timeline of events

[To Top of the Document](#_top)

|  |  |  |
| --- | --- | --- |
| Time | Event | Source |
| 2018-06-05 | Someone called Clark on phone and told he would get a ‘usb’ stick dropped on his desk | From journel.doc |
| 2018-06-07 08:55:35  SGT | Clerk took a usb and looked into it.  He found three Microsoft word documents that coercing about his truth identity. | From decrypted usb |
| 2018-06-18 08:19:33  SGT | He was afraid of appealing his identity and started accessing clown contents. | From internet histories |
| 2018-06-18 11:11:00 SGT | He got “stop clowning about and start working like a superman :)” email from the blackmailer. | From email records |
| 2018-06-18 10:49:48  SGT to 2018-07-02  09:21:52 SGT | Clark kept accessing and downloading for clown contents from websites | From internet histories |
| 2018-07-02  10:20:09 SGT | Clark asked Simpson how to send the accessed contents. | From email records |
|  |  |  |
| 2018-07-09  11:24 SGT | Clerk send clown contents achieved with .zip to Simpson along with  lines of sentences to let him go. | From email records |
| 2018-07-10  09:41 SGT | Simpson replied “No” to let him go and to keep accessing clowns. | From email records |
| 2018-07-10 10:28:47  SGT | Clerk searched YouTube videos to erase his computer data | From internet histories |
| 2018-07-11  08:11:46 SGT | Clerk send email to his Chief(Sassy Penguin) that he has been hacked | From email records |