Computer Forensics - CSG2305.3

Assignment 2: Forensic Investigation Case Study

Providing Evidence of Identity theft and Fraud

Name: **Marco CAVANI**

Student Number: **10570027**

Email: [**mcavani@our.ecu.edu.au**](mailto:mcavani@our.ecu.edu.au)

Disclaimer

This digital forensic report contains material that serves solely to provide admissible evidence in a case that involves identity fraud and theft. This report is presented by Marco Cavani who was engaged to investigate and analyse the forensic images obtained from Damon Hopkins ‘computer by The Western Australia Police Force (WAPOL). This record contains sensitive data such as personal Identification Documents, Credit Card Credentials, private electronic communications, and private email profiles.

Confidential notice

This document is a strictly confidential communication to The Western Australia Police Force (WAPOL) who requested the material, its use is solely restricted to recipient, and it is not intended to be consumed or used by anyone else.

Contents

[1 Executive Summary 3](#_Toc116250879)

[2 Time comparison details 3](#_Toc116250880)

[3 Issue 1 - Content Related Content relating to the offence 4](#_Toc116250881)

[3.1 Evidence 1 - Jane Citizen Passport - ID: 001 4](#_Toc116250882)

[3.2 Evidence 2 - Izaddin Bin Aris Passport - ID: 002 4](#_Toc116250883)

[3.3 Evidence 3 - Jennifer Barber - ID: 003 5](#_Toc116250884)

[3.4 Evidence 4 - Relaun Tucker - ID: 004 5](#_Toc116250885)

[3.5 Evidence 1.1 - Jane Citizen Credit Card Credential - ID: 011 6](#_Toc116250886)

[3.6 Evidence 2.1- Izaddin Bin Aris Credit Card Credential - ID: 012 6](#_Toc116250887)

[3.7 Evidence 3.1 Barber Credit Card Credential – ID: 013 7](#_Toc116250888)

[3.8 Evidence 4.1 Relaun Credit Card Credential – ID: 014 7](#_Toc116250889)

[4 Issue 2 - Identification 8](#_Toc116250890)

[4.1 Identification Evidence 1 8](#_Toc116250891)

[4.2 Identification Evidence 2 9](#_Toc116250892)

[4.3 Identification Evidence 3 10](#_Toc116250893)

[4 Issue 3 Intent 11](#_Toc116250894)

[4.1 Intent Evidence 1 11](#_Toc116250895)

[4.2 Intent Evidence 2 12](#_Toc116250896)

[4.3 Intent Evidence 3 13](#_Toc116250897)

[5 Issue 4 quantity of File 14](#_Toc116250898)

[6 Issue 5 Installed software 15](#_Toc116250899)

[7 Appendix A Running Sheet 16](#_Toc116250900)

[8 Appendix B Timeline of events 22](#_Toc116250901)

# Executive Summary

This document outlines the findings of the digital forensics investigation conducted by Marco CAVANI on the forensic image provided by The Western Australia Police Force (WAPOL). The findings are presented clearly in a way that can be viewed and evaluated. The aim is to provide proof of identity theft and fraud. The investigation includes evidence related to the case, identification, intent, quantity of files, installed software, a timeline of the events as well as the running sheet. The tools used for the investigation include Autopsy 4.19.1, Registry Viewer 2.0.0.7 (Demo Mode), and FTK Imager 4.5.03. The analysis was performed on the relevant portion of the image using FTK Imager in combination with Registry Viewer to analyse data from the Windows Registry. As a result, the main user, the timestamp, the USB connection, and the email account were identified on the system. After analysing the registry’s hives, the directory tree was inspected using Autopsy. During the static analysis, sensitive data such as personal ID, credit card credentials and potential online blackmail attempts were found and reported. According to Autopsy, 22 out of 77 recently accessed files on Damon’s account were classified as suspicious. Also, the browser history and the web history show suspicious intents. Further, there is evidence of both stenography and cryptography software being installed on the computer.

# Time comparison details

The timestamps used in the Windows Registry hives are based on UTC standard format, whereas the register timestamps in files, folders, and logs are based on W. Australia standard time (WAST), which is UTC +8.

# Issue 1 - Content Related Content relating to the offence

## Evidence 1 - Jane Citizen Passport - ID: 001

|  |  |  |
| --- | --- | --- |
| **Evidence 1** | **File Name** | **Status** |
| A picture containing text  Description automatically generated | 247049[23].JPG | Allocated |
| **Created** | **Type** |
| 2021-05-12 21:07:58 AWST | File System image/jpeg |
| **Accessed** | **File Size** |
| 2021-05-12 21:09:17 AWST | 46,173 bytes |
| **Changed** | **MD5** |
| 2021-05-12 21:19:08 AWST | 03abb0237daa9f16b54d1f20338becbf |
| **Modified** | **SHA-256** |
| 2021-05-12 21:07:58 AWST | c04c597cafa8730164ec8be61d030a69c2a4bf0ea443b7c50352215ff07fb3a7 |
| **Location** | |
| /Users/DamonHopkins/AppData/Local/Packages/microsoft.windowscommunicationsapps\_8wekyb3d8bbwe/LocalState/Files/S0/3/Attachments | |
| **Analysis** | | |
| Evidence 1 was classified as relevant as it was associated with her credit card credential found in the form of a text file in the recycle bin directory ([See evidence 011](#_Evidence_5_-)). The Web history shows that Jane citizen has been searched on Facebook by Damon. The file was found in the attachments directory as if it was downloaded from an email address. | | |

## Evidence 2 - Izaddin Bin Aris Passport - ID: 002

|  |  |  |
| --- | --- | --- |
| **Evidence 2** | **File Name** | **Status** |
| Text  Description automatically generated | Passport scan[24].pdf | Allocated |
| **Created** | **Type** |
| 2021-04-22 12:26:51 AWST | Application/pdf |
| **Accessed** | **File Size** |
| 2021-04-22 13:30:19 AWST | 180,764 bytes |
| **Changed** | **MD5** |
| 2021-04-22 12:26:51 AWST | 09417378e9c33cb138f5ef4b6b06bf92 |
| **Modified** | **SHA-256** |
| 2021-04-22 12:26:51 AWST | a74b21b5bb8576c41b5ab220c21fc5fa5a6cbbe9784bb8fb7b653a6b43a22c38 |
| **Location** | |
| /img\_caseStudyFinal.E01/vol\_vol3/Users/Damon Hopkins/Desktop/Home/SECRET/Izaddin | |
| **Analysis** | | |
| Izaddin Bin Aris does not appear in the web history and there is no evidence of communication between Damon and Izaddin. However, a file in the same folder shows his name, credit card credentials and a phone number (See evidence 012). Izaddin might be contacted by phone. Additionally, a folder in the same directory contains the uncropped scanned version of his passport. [(See evidence 012)](#_Evidence_6_-). | | |

## Evidence 3 - Jennifer Barber - ID: 003

|  |  |  |
| --- | --- | --- |
| **Evidence 3** | **File Name** | **Status** |
| A picture containing whiteboard  Description automatically generated | F963D7BF-2350-4461-A50C03B21E806637[23].jpeg | Allocated |
| **Created** | **Type** |
| 2021-05-11 17:39:41 AWST | image/jpeg |
| **Accessed** | **File Size** |
| 2021-05-12 22:24:35 AWST | 14,9970 Bytes |
| **Changed** | **MD5** |
| 2021-05-11 17:40:15 AWST | 8f26262efc9ffb3efdbb224fc23f0fa0 |
| **Modified** | **SHA-256** |
| 2021-05-11 17:39:41 AWST | 012efbd75cf5bb81436d4354f58219df5852bb4ca17b1e3738dd1591ec681216 |
| **Location** | |
| /img\_caseStudyFinal.E01/vol\_vol3/Users/Damon/Hopkins/Desktop/Home/SECRET/ | |
| **Analysis** | | |
| This image was classified as suspicious. However, there is no other evidence linkable to the person except for the file found in the same location called cc.txt that contains credit card credentials [(see evidence 013)](#_Evidence_7_Jennifer). | | |

## Evidence 4 - Relaun Tucker - ID: 004

|  |  |  |
| --- | --- | --- |
| Evidence 4 | **File Name** | **Status** |
| Text  Description automatically generated | RELAUN\_DRIVER\_LICENCE.png | Allocated |
| **Created** | **Type** |
| 2021-04-28 20:46:58 AWST | image/png |
| **Accessed** | **File Size** |
| 2021-04-28 21:06:04 AWST | 67,192 bytes |
| **Changed** | **MD5** |
| 2021-04-28 20:47:53 AWST | 2330a8a8d08568f80bb20ffa080d16b6 |
| **Modified** | **SHA-256** |
| 2021-04-28 20:46:58 AWST | 8b70391253f74b354e5075c49466a689bccc85745382e1e3f7b76de2236d0e06 |
| **Location** | | |
| */img\_caseStudyFinal.E01/vol\_vol3/Users/DamonHopkins/Desktop/Home/SECRET/* | | |
| **Analysis** | | |
| Similarly, to Izaddin and Jane,  Relaun Tucker has a dedicated folder which contains his Driver Licence along with credit card credentials [(see evidence 014).](#_Evidence_8_Relaun) His name has appeared several times in web history. There is evidence of blackmail and  Identity theft that involves Relaun Tucker, which is discussed in Issue 3 intent. | | |

## Evidence 1.1 - Jane Citizen Credit Card Credential - ID: 011

|  |  |  |
| --- | --- | --- |
| **Evidence 5** | **File Name** | **Status** |
| Graphical user interface, text, application, email  Description automatically generated | $RVVLPK8.txt | Allocated |
| **Created** | **Type** |
| 2021-05-12 21:16:57 AWST | Text/plain |
| **Accessed** | **File Size** |
| 2021-05-12 21:18:52 AWST | 90 bytes |
| **Changed** | **MD5** |
| 2021-05-13 11:25:16 AWST | 3be74651f4377d37dd6b8c2bbc167b97 |
| **Modified** | **SHA-256** |
| 2021-05-12 21:17:02 AWST | 8fd755eae82ad68ebd5527344680ef405588ff00c37e02f0eb5abf7f7a285534 |
| **Location** | |
| /img\_caseStudyFinal.E01/vol\_vol3/$Recycle.Bin/S-1-5-21-2659424124-211076020-1381419125-1001/ | |
| **Analysis** | |
| The image refers to a text file found in the recycle bin and contains credit card credential which can be linked with Jane Citizen as the credit card is named after her. | |

## Evidence 2.1- Izaddin Bin Aris Credit Card Credential - ID: 012

|  |  |  |
| --- | --- | --- |
| **Evidence 6** | **File Name** | **Status** |
| Graphical user interface, text, application, email  Description automatically generated | Izzadin Details.odg | Allocated |
| **Created** | **Type** |
| 2021-04-22 12:30:29 AWST | application/vnd.oasis.opendocument.text |
| **Accessed** | **File Size** |
| 2021-04-28 20:47:32 AWST | 10,066 bytes |
| **Changed** | **MD5** |
| 2021-04-22 12:31:08 AWST | 62bd64ed571ced90fe9287fa1d0bbfed |
| **Modified** | **SHA-256** |
| 2021-04-22 12:31:08 AWST | db947ab5a050bf9587564ff92e9933293855571f50fb42785cb77b8f7cbea625 |
| **Location** | |
| /img\_caseStudyFinal.E01/vol\_vol3/Users/Damon Hopkins/Desktop/Home/SECRET/Izaddin/ | |
| **Analysis** | |
| The screenshot refers to a text file located in the Izaddin folder which contains credit card credential that can be linked with Izaddin as suggested from the location folder structure. | |

## Evidence 3.1 Barber Credit Card Credential – ID: 013

|  |  |  |
| --- | --- | --- |
| **Evidence 7** | **File Name** | **Status** |
| Graphical user interface, text, email  Description automatically generated | cc.txt | Allocated |
| **Created** | **Type** |
| 2021-05-11 17:39:50 AWST | Tex t/plain |
| **Accessed** | **File Size** |
| 2021-05-11 17:40:34 AWST | 3 KB |
| **Changed** | **MD5** |
| 2021-05-11 17:40:12 AWST | f29e2c333578982d19d69711c931bc08 |
| **Modified** | **SHA-256** |
| 2021-05-11 17:39:56 AWST | 25e23198861477f47f69b9a00a9a81eb51b7d21ccd0a72f15aa1d26bf3840cf5 |
| **Location** | |
| /img\_caseStudyFinal.E01/vol\_vol3/Users/Damon Hopkins/Desktop/Home/SECRET/Barber/CC.txt | |
| **Analysis** | |
| Barber credit card credentials is inside a subfolder named after her which also contains a picture of a lady showing an ID. | |

## Evidence 4.1 Relaun Credit Card Credential – ID: 014

|  |  |  |
| --- | --- | --- |
| **Evidence 8** | **File Name** | **Status** |
| Graphical user interface, text, application, email  Description automatically generated | RELAUN\_CC\_INFO.txt | Allocated |
| **Created** | **Type** |
| 2021-04-28 20:47:25 AWST | Text/plain |
| **Accessed** | **File Size** |
| 2021-04-28 21:06:10 AWST | 4 KB |
| **Changed** | **MD5** |
| 2021-04-28 20:47:53 AWST | 991ea7fa206e3a10e4795724057aba5d |
| **Modified** | **SHA-256** |
| 2021-04-28 20:47:25 AWST | 7df9ef8bcdcfc33074fc22ab94ca2b98da3eb0833570593a2f812d5f0853324a |
| **Location** | |
| /img\_caseStudyFinal.E01/vol\_vol3/Users/Damon Hopkins/Desktop/Home/SECRET/Relaun/RELAUN\_CC\_INFO.txt | |
| **Analysis** | |
| Relaun credit card credentials are located inside the subfolder name after him inside the SECRET folder. The file also contains the pictures of his Driver License and its compressed file which was deleted. | |

**Potential victims:** Jane Citizen, Relaun Tucker, Chung Young, Barber Jennifer, Iziddin Bin Aris

# Issue 2 - Identification

## Identification Evidence 1

Table 1 shows the users in the Security Accounts Management (SAM). The user, Damon Hopkins, was created by a client, and it is the only active profile. The other four accounts were created by the system. Three out of five user profiles have never been used, and one has been used only once but is disabled. The timestamps in table 1 are at UTC whereas the SYSTEM register timestamps for files, folders, and logs are based on W. Australia standard time (WAST) which is UTC +8.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Username | Last Written Time | RID | Account Status | Last Logon Time |
| Administrator | 4/15/2021 2:38:10 UTC | 500 | Disabled | 11/18/2020 |
| Guest | 4/15/2021 2:38:10 UTC | 501 | Disabled | Never |
| DefaultAccount | 4/15/2021 2:38:10 UTC | 503 | Disabled | Never |
| WDAGUtilityAccount | 4/15/2021 2:38:10 UTC | 504 | Disabled | Never |
| Damon Hopkins | 5/142021 4:36:57 UTC | 1001 | Enabled | 5/14/2021 4:36:57 UTC |

Table

Table 2 shows users linked to Damon Hopkins’s account. One account, damon.hopkins11@outlook.com, was used to log in to Facebook.com and the other one, damonhopkins22@outlook.com, was used to login into live.com.

|  |  |  |  |
| --- | --- | --- | --- |
| Username | Domain | Browser | Date of created |
| damon.hopkins11@outlook.com | Facebook.com | Google Chrome | 2021-04-19 20:28:00 AWST |
| damonhopkins22@outlook.com | Live.com | Google Chrome | 2021-04-19 20:34:12 AWST |

Table 2

## Identification Evidence 2

Damon’s email account was used for both work-related and blackmail activities. The conversation to the left of the table below was identified as an attempt to blackmail Chung, as Damon pretended to be a representative from Microsoft claiming that Chung would need to secure his computer. Whereas the conversation to the right of the table was identified, such as work-related communication in which Teri Ferguson asked Damon to work for him on a tax and superannuation program. In conclusion, both the blackmail attempt and his ordinary job-related messages were handled by his personal email (Damonhopkins22@outlook.com).

|  |  |
| --- | --- |
| **Blackmail attempt Chung** | **Damon Hopkins’ work-related activity** |
| Hi Chung,  My name is Damon, and I am a representative from Micr= osoft. We have been seeing abnormal activity occurring from your device, th= is seems to indicate either a hacking attack or malware, in our terms of se= rvice this is a violation, however we are able to help. Without help your device will be rendered useless. Ho= w do you wish to proceed.  Regards,  Damon  From: [Damonhopkins22@outlook.com](mailto:Damonhopkins22@outlook.com)  2021-05-14 13:08:44 AWST | Hi Damon,  Nice to hear from you. I do have one task for you. We need a tax and  superannuation prog  Sent from Mail for Windows 10 From: teriferguson Sent: Friday, 14 May 2021 12:36 PM To: damonhopkins22@outlook.com Subject: Tax |

Table 3

## Identification Evidence 3

The user, Damon Hopkins, accessed a folder which contains normal job-related activities at the same time as the folder called SECRET in which the majority of the evidence was found [(see Issue 1 - Content relating to the offence)](#_Issue_1_-).

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| File Name | File Path | File Content | Data Sources | Accessed |
| Work.lnk | C:\Users\Damon Hopkins\Desktop\Work | Work Journal.odt | caseStudyFinal.E01 | 2021-04-19 20:25:57 AWST |
| Home.lnk | C:\Users\Damon Hopkins\Desktop\Home | SECRET.lnk | caseStudyFinal.E01 | 2021-04-19 20:26:56 AWST |
| SECRET.lnk | C:\Users\Damon Hopkins\Desktop\Home | Barber  Izaddin  Relaun | caseStudyFinal.E01 | 2021-04-19 20:26:56 AWST |

Table 4

The screenshot in table 4 proves the work-related nature of the content in the following directory : C:\Users\Damon Hopkins\Desktop\Work

|  |
| --- |
| **Damon Hopkins’ work related activities** |
| Graphical user interface, text, application  Description automatically generated |

Table 5

# Issue 3 Intent

## Intent Evidence 1

Table 6 shows a conversation between two users who seem to share an interest in making frauds. The name Ben is associated with Damon, as if he was using a different name on social media. Further, Ben shared Damon Hopkins’s email as it was his. The same email account was used to connect with potential victims [(see Identification Evidence 2)](#_Identification_Evidence_2).

|  |
| --- |
| **Evidence of Shared interested in making fraud** |
| Graphical user interface, text, application, chat or text message  Description automatically generated |
| Hello  Elliot,  ll get started first thing tomorrow. RThe password was a little trickt vby but I finally got it! FI work as a freelance software engineer, b but could do with a little extra cash artt the moment.Thanks,  Damon |

Table 6

## Intent Evidence 2

The first conversation is about Damon being ghosted by Chung, while the second message is about a credit card credential obtained and encrypted. The third conversation is once again about an acquired target and a file being encrypted by Damon.

|  |
| --- |
| **Evidence of blackmail Attempt** |
| Hey  Elliot, I think Chung has ghosted me, I emailed two days ago and still have no response, I will move onto |
| Hey  Elliot, I found a guy on book and was able to vince him 0senhis CC info4 "drivers license, I have attached an encrypted fil# think you ll know what the pass(O is.  Regards;  \_Damonc |
| Hi Elliot,  Target acquired, the password for the file is encryptedRegards,  Damoin |

Table 7

## Intent Evidence 3

The images below refer to a conversation between two Facebook users, where one user reached out to Relaun Tucker telling him about the possibility of receiving assets from a Great Aunt who was unknown by the potential victim. Furthermore, the two images on the left of the table below show the conversation in which Relaun Tucker was convinced to provide his own ID and credit card details; the same ID and credential related to [Evidence 004](#_Evidence_4_-). Whereas the image on the right might indicate that Damon’s email account was used to subscribe on eBay using Relaun Tucker Identity.

|  |  |
| --- | --- |
| **Evidence of black mail attempt** | **Evidence of Identity Theft** |
| **Graphical user interface, text, application, chat or text message  Description automatically generated** Graphical user interface, text, application, chat or text message  Description automatically generated | © 1995-2021 eBay Inc. **eBay sent this message to Relaun Tucker (damonho-13).** Your registered name is included to show this message originated from eBay. [Learn more](https://rover.ebay.com/rover/2/0/8?bu=45208349751&segname=TE76007_T_ALL&crd=20210512170000&mpre=https%3A%2F%2Fwww.ebay.com.au%2Fhelp%2Faccount%2Fprotecting-account%2Frecognising-spoof-emails%3Fid%3D4195%26campaign-id%3D90001%26run-date%3D20210512170000%26TemplateId%3D1cb7b781-f129-4982-b289-8bd0204d9101%26TemplateVersion%3D621%26co%3D0%26placement-type%3DfooterLearn%26user-id%3D45208349751%26instance%3D1620864000%26site-id%3D15%26TrackingCode%3DTE76007_T_ALL%26placement-type-name%3DfooterLearn&ch=osgood&url=%24%7BlocationUrl%7D%26campaign-id%3D%24%7BcampaignId%7D%26run-date%3D%24%7BRUN_DT%7D%26TemplateId%3D%24%7BtemplateId%7D%26TemplateVersion%3D%24%7BtemplateVersion%7D%26co%3D%24%7BlinkOrder%7D%26placement-type%3D%24%7BplacementType%7D%26user-id%3D%24%7BENCRYPTED_USER_ID%7D%26instance%3D%24%7BINSTANCE_ID%7D%26site-id%3D%24%7BSITE_ID%7D%26TrackingCode%3D%24%7BTrackingCode%7D%26placement-type-name%3D%24%7BplacementType%7D&osub=b4aa0796697a1f593a9821ba2734be69%7ETE76007_T_ALL&sojTags=emid%3Dbu%2Cut%3Dut%2Csegname%3Dsegname%2Ccrd%3Dcrd%2Curl%3Durl%2Cch%3Dch%2Cosub%3Dosub).  You are subscribed as [damonhopkins22@outlook.com](mailto:damonhopkins22@outlook.com) registered on eBay. If you do not wish to receive General Email Promotions, please [click here to unsubscribe](https://marketing.ebay.com.au/unsubscribe/home?token=AQAGAAAAgEHmFPYhgEpIcCXTvlNb4pEPnq6K_0-wMFAT0jcNEnOLwthm3Ex_CbfX5GbCryWkRpcnLpWFQULuZq25LK8Sm0IKaK93UFpK2jacw4VDwqDjYprirB_o0MZsTMx7yJ0_1eTs49q1kfqF0W9r_XAR19sdLBen_NZ_T8PksXzfsgbE). |

Table 8

# Issue 4 quantity of File

|  |  |  |
| --- | --- | --- |
| **Usage: OS Drive (Windows 10)** | **OS: Windows 10 Home** | **Size: 250 GB** |

The bar chart shows the total number of files sorted by type. Audio and video represent less than 1% while 1% is represented by not analysed files. The majority of the files at 36% are unknown, followed by documents at 28% and other documents at 23% respectively. The bar chart shows the exact quantity of the files sorted by type.

# Issue 5 Installed software

**VeraCrypt:** VeraCrypt is a free source encryption software used for establishing and maintaining on the fly encrypted volume in which the data is automatically encrypted after it is saved and decrypted once it is loaded. In saying that, no data stored in an encrypted block can be decrypted without using the right password. Further, VeraCrypt always saves decrypted files temporarily in the RAM.

**TrueCrypt:** TrueCrypt is an open-source encryption software which is no longer supported and used for on-the-fly encryption. It can be used for encrypting a partition or the whole storage device.

**S-tools4:** S-tools4 is a stenography tool that can be used to hide text messages inside of an image. S-Tools is a program composed by Andy Brown. It is a steganography instrument accessible online. It allows to hide a text file into an image simply dragging the txt file on the image.

# Appendix A Running Sheet

|  |  |  |
| --- | --- | --- |
| Date/Time | Event | Duration |
| 1/10/2022 – 8:30 am | Verify the integrity of the working copy of image (caseStudyFinal.E01 MD5) using terminal comment md5sum on SIFT:  md5sum output 7f693d101bd91a1c5911624a5d62b674  Integrity Verified using SIFT (md5sum) | 2 Minutes |
| 1/10/2022 – 8:32 am | Gather information about user and system profiles  Extract SAM and SYSTEM using FTK Imager 4. 5.0.3  Save the files to be loaded into Access Data Registry Viewer 2.0.0.7 | 5 Minutes |
| 1/10/2022 – 8:45 am | Load and Analyse data from the Windows registry:  Security Account Manager (SAM) analysis using Access Data Registry Viewer 2.0.0.7 (Demo Mode)  5 users found  4 were created by the system  1 was created by the user Damon Hopkins  SYSTEM registry analysed using Access Data Registry Viewer 2.0.0.7 (Demo Mode)  Output:  The Time zone of files, folders and logs are defined (in UTC +8 WAST)  Computer name, identified  Output:  DESKTOP-6NIJ9S9  USBs Connected to the computer when identified  Output:  17 USBs connected since Windows was installed | 60 Minutes |
|  | Open Autopsy 4.19.1  Open existing case - caseStudyFinal.E01  Create a folder for collecting evidence  Name the folder with the case ID  Folder created in the desktop CASE-E01  Inside CASE-E01  Create folders to collect different file type as following:  Case  Report  Images  Documents  temp  Create a txt file inside case folder to registering the steps and actions in a time frame  Case-E01.txt created |  |
| 1/10/2022 – 9:45 am | Browse the copy of image (caseStudyFinal.E01) volume 3, using Autopsy 4.19.1  navigate through vol3(NTFS / exFAT (0x7): 104448-487354195.  Open Users >> Damon Hopkins and start looking for evidence by browsing through the folders.  5 pieces of evidence found  **Barber’ ID:**  F963D7BF-2350-4461-A50C03B21E806637[23].jpeg  **Izaddin Bin Aris’ Passport:**  Passport scan[24].pdf  **Relaun Tucker Driver License:**  RELAUN\_DRIVER\_LICENCE.png  **Location**  vol3(NTFS / exFAT (0x7): 104448-487354195/Users/Damon Hopkins/Desktop/Home/SECRET | 45 minutes |
| 1/10/2022 – 10:30 am | Tag and extract suspicious file(s)/Folder(s)  5 pieces of evidence collected | 15 minutes |
| 1/10/2022 - 10:45 am | Analyse and extrapolate information from the tagged file such as file name, size, hash values(sha256 & MD5), Type, Location and data about file(s) creation, modification, change and access  Tables were created to showcase the information | 45 minutes |
| 1/10/2022 – 11:00 am | Perform In-dept searching through the New Technology File System (NTFS) using Autopsy 4.19.1  Searching for images and text files: Mime type (jpeg, jpg, PNG, GIF, txt, pdf)  Relaun1.PNG  Relaun2.PNG  1.PNG  **Jane’ passport** :  247049[23].JPG  VeraCrypt screenshot of 28 items  e.g.,  857642-Beginner's Tutorial\_Image\_001.jpg  The user might undertake VeraCrypt  Tutorial to encrypt file on the fly  Keyword search:  The word Jane produced 85 results 8 (9%)  files contained suspicious contents  $rvvpk8.txt  History  History Provider Cache History.hxd  Recycle Bin Artefact  Tabs-13265440774939687  Web History artefacts  Famale\_names.txt  The word Elliot produced 20 results 4 (25%)  files contained suspicious contents  Hxstore.hxd  Veracrypt28x128.png-slack  {5b34bc0e-b31e-11eb-b726-18c04d29ff42}{3808876b-c176-4e48-b7ae-04046e6cc752}-slack    The word izaddin produced 60 results  Notable file(s)  Izaddin.details.odt  The word Leah produced 45 results  Notable fille(s): none  The word Relaun produced 39 results  Notable fille(s):  31.dat  38.dat  41.dat  3 files were Extracted and analysed x  31.dat  38.dat  41.dat  **Installed Program**  48 installed programs  Noted:  VeraCrypt  TrueCrypt  **Operating System information**  Produced 2 results:  damon.hopkins11@outlook.com was used to log in to Facebook.com  [damonhopkins22@outlook.com](mailto:damonhopkins22@outlook.com) was used to log in to Live.com  **Web Accounts**  Account identified  1 is used to log in to Facebook  1 account is used to log in to live  **Web Download**  Stenography tools were downloaded.  **Web History**  Web history search to define user interested topics.  Researched topic of interested:   * Learning cryptography and stenography * Tax calculator * MEME card * Jane Citizen FB page * Renaul Tucker FB page   **Encryption detected**  1 file found  Tips[4].txt  Attempt to open the file using the terminal failed as the password is unknown.  **Encryption Suspected**  According with Autopsy 12 files have might been encrypted.  **Unlocated folder**  2 pieces of evidence were found  [(Evidence ID: 001 and 011](#_Evidence_1_-)) along with  28 jpg – VeraCrypt tutorial images unlocated . | 240 minutes |
| 1/10/2022 – 16:00 pm | Extract a copy of Damon Hopkins user account folder.  Navigate the folder Damon Hopkins >> Desktop.  3 encryption tools in for of exe files found. | 15 minutes |
| 1/10/2022 – 16:15 pm | Navigate to Damon Hopkins >> Desktop >> Home >> Facebook to gather additional information  1 Screenshot of a suspicious conversation between two user that seem to share interest in making fraud.  Evidence collected and analysed, [see intent section](#_Issue_3_Intent).  Name Elliot noted on the conversation | 5 minutes |
| 1/10/2022 – 17:00 pm | Performed Keyword search using Autopsy to check if the name Elliot appear in the results.  22 files analysed.  Noted 4 conversation between Damon and Elliot talking about suspicious activity that can be related to the offence.  [Evidence analysis can be seen here](#_Issue_3_Intent). | 60 minutes |
| 1/11/2022 – 8:00 am | Performed Keyword search using autopsy to check if Damon’s email accounts appear in the results.  56 results analysed, 3 file obtained  1 message to Chung  2 Messages received from Teri Ferguson  [See here](#_Identification_Evidence_2) | 60 minutes |
| 1/11/2022 – 9:00 am | Analyse recent activities using Autopsy to check and correlate last actions on Damon Computer.  3 activities noted [(see identification section)](#_Issue_2_-)  Damon accessed his regular job files at the same time as the suspicious folder where the majority of the evidence were found. | 60 minutes |
| 1/11/2022 – 10:00 am | Check web history for the second time, to triangulate information  No results | 30 minutes |
| 1/11/2022 – 10:30 am | Check downloaded file to see what software have been downloaded from internet using Autopsy 4.19.1  3 encryption tools fond | 60 minuts |
| 1/11/2022 – 11:30 am | Research about installed software  TruCrypt.com  VeraCrypt.com  s-tool4.com  tools review [(here)](#_Issue_5_Installed) | 30 minutes |
| 1/11/2022 – 12:00 pm | Check the quantity of files using Autopsy 4.19.1  The total number of files is 365,533 | 30 minutes |

# Appendix B Timeline of events

|  |  |
| --- | --- |
|  | Email from Demon to Elliot |
|  |  |
|  | Relaun Tucker |
|  |  |
|  | Jane Citizen |
|  |  |
|  | Jennifer Barber |
|  |  |
|  | Izaddin Bin Aris |

|  |  |  |
| --- | --- | --- |
| **Subject** | **Date and Time** | **Description** |
| Damon email | |  |  | | --- | --- | |  | 2021-05-12 22:23:53 AWST | | Damon and Elliot communication about a new target being acquired |
| Evidence 1.1 | 2021-05-12 21:16:57 AWST | A file containing Jane Citizen’ credit card credential was created |
| Evidence 1 | 2021-05-12 21:07:58 AWST | Jane’s passport was created |
| Evidence 3.1 | 2021-05-11 17:39:50 AWST | Barber credit card credential file was created |
| Evidence 3 | 2021-05-11 17:39:41 AWST | Barber passport was created |
| Jane | 2021-05-11 17:44:51 AWST | Jane was search on Facebook |
| Evidence 4.1 | 2021-04-28 20:47:25 AWST | Renaul credit card credential file was created |
| Evidence 4 | 2021-04-28 20:46:58 AWST | Relaun passport was created |
| Relaun | 2021-04-27 22:16:55 AWST | Relaun was search on Facebook |
| Evidence 2 | 2021-04-22 12:26:51 AWST | Izaddin passport was created |
| Evidence 2.1 | 2021-04-22 12:30:29 AWST | Izaddin credit card credential file was created |
| Conversation between Damon and Elliot | 2021-04-19 20:19:03 AWST | Damon advised Elliot of a new person’s information acquired |
| Conversation between Damon and Elliot | |  | | --- | | 2019-10-06 19:14:44 AWST | | I will start tomorrow… |