CSG2305 Computer Forensics

Forensic Investigation Case Study

Glen TEAKLE 10532981

Joondalup – Off Campus

Dr Leslie Sikos

This investigation and report were conducted to find any evidence on the seized device of Damon Hopkins relating to the crime of identity theft.

**Confidentiality Notice**

This report and included documented evidence is to be viewed only by those persons involved directly in the Damon Hopkins identity fraud case. This report is not to be accessed or read by any other individuals without proper authorisation.

No digital or physical copies are to be made of this report unless the proper authorisation has been given.

This report is not to be made available to any individuals other than those with direct involvement in the case, nor is it to be in the possession of any such individuals without proper authorisation.

**Disclaimer**

This report may contain questionable material, including images, videos or text deemed to be offensive, objectionable, shocking or illegal in nature. The evidence contained herein may be in the form of web links which, if clicked on, may connect to the internet. The links may lead to further offensive, objectionable, shocking or illegal content. Viewers are advised to continue at their own discretion, at risk of exposure to such material.

Contents

[Summary and Overview of Tasks 3](#_Toc117607130)

[Background 3](#_Toc117607131)

[Software/Programs Used 3](#_Toc117607132)

[Methods 3](#_Toc117607133)

[Issue 1. Content Relating to Offence. 3](#_Toc117607134)

[Issue 2. Identification. 8](#_Toc117607135)

[User 8](#_Toc117607136)

[Fraud 8](#_Toc117607137)

[Concealment 8](#_Toc117607138)

[Issue 3. Intent. 11](#_Toc117607139)

[Issue 4. Quantity of Files 11](#_Toc117607140)

[Issue 5. Installed Software. 12](#_Toc117607141)

[Appendix A – Running Sheet 12](#_Toc117607142)

[Appendix B – Timeline of Events 24](#_Toc117607143)

# Summary and Overview of Tasks

## Background

Damon Hopkins has been accused of stealing identities online, with the intention of making fake purchases. Damon has no prior convictions and is denying the accusations. Police have obtained a warrant and viewed network traffic at Damon’s workplace where they have determined that the probability of criminal involvement is high. Police have seized Damon’s laptop for inspection by forensics and a digital image has been taken. This report summarises the findings of any evidence relating to the alleged crime, to determine if any crime has taken place.

## Software/Programs Used

Programs used in the investigation were:

* Autopsy version 4.19.1. The time zone setting was automatically configured to show the “Local time zone” when viewing ingested files.
* FTK Imager version 4.5.0.3. A time zone setting option could not be found. This was considered regarding use of other programs (Autopsy) when viewing the disk image file.
* OS Forensics version 8.0.1008 – Trial Version. The time zone was configured upon creation of a new case using GMT + 8.
* Notepad version 1809.

## Methods

The integrity of the disk image was maintained throughout the investigation by initially generating hashes of the case study image files, making copies of the image files and generating hashes of the copies to match the original files. Only the copies of the files were used in the investigation.

The disk image was examined using the above programs to search for any data relevant to the crime of identity theft. Data of interest includes:

* Image files
* Documents
* Emails
* Installed programs that may be relevant to the investigation
* Deleted files
* User accounts and user activity including logins
* Browser history
* Items downloaded/saved from the internet
* Any other data containing names, addresses, user profiles, phone numbers, email addresses, bank/credit card details or social media accounts that could be linked to potential victims of identity theft.

# Issue 1. Content Relating to Offence.

For detailed findings please see Appendix A – Running Sheet.

|  |
| --- |
| Graphical user interface, text, application, chat or text message  Description automatically generated*Figure 1.* |
| File Name – Relaun1.PNG |
| Type – png |
| Size – 76,089 bytes |
| Location - Partition2/root/users/Damon Hopkins/ Desktop/home/SECRET/Facebook |
| Status – Allocated |
| MD5 Hash - ac32854c20cfd6722b69af36a96f7712 |
| Created - 5/4/2021 7:11:42 AM |
| Accessed - 5/12/2021 12:55:06 PM |
| Modified - 5/4/2021 7:11:42 AM |
| Sector Location - 47,896,008 |
| File Description – Screenshot of conversation between “unknown” and “Relaun Tucker”. |
| Likely scam involving Damon and victim. |

|  |
| --- |
| Graphical user interface, text, application, chat or text message  Description automatically generated*Figure 2.* |
| File Name – Relaun2.PNG |
| Type – png |
| Size – 171,936 bytes |
| Location - Partition2/root/users/Damon Hopkins/ Desktop/home/SECRET/Facebook |
| Status - Allocated |
| MD5 Hash - b8952ec09a41fcba867e25d7982fcf41 |
| Created - 5/4/2021 7:12:03 AM |
| Accessed - 5/12/2021 12:55:06 PM |
| Modified - 5/4/2021 7:12:03 AM |
| Sector Location - 3,848,224 |
| File Description – Screenshot of conversation between “unknown” and “Relaun Tucker”. |

|  |
| --- |
| A picture containing text  Description automatically generated*Figure 3.* |
| File Name - $RSQETAE.JPG |
| Type - jpg |
| Size – 46,173 bytes |
| Location - Partition2/NONAME[NTFS]/root/$Recycle.Bin/S-1-5-21-2659424124-211076020-1381419125-1001 |
| Status - Allocated |
| MD5 Hash - 03abb0237daa9f16b54d1f20338becbf |
| Created - 5/12/2021 1:09:22 PM |
| Accessed - 5/12/2021 1:18:52 PM |
| Modified - 5/12/2021 1:09:23 PM |
| Sector Location - 369,396 |
| File Description – Passport photo of Jane Citizen. |
| This picture matches the Google Chrome search of “Jane Citizen”. |

|  |
| --- |
| *Figure 4.* |
| File Name - F963D7BF-2350-4461-A50C-03B21E806637[23].jpg |
| Type - JPG |
| Size – 149,970 bytes |
| Location - Partition2/root/users/Damon Hopkins/ Desktop/home/SECRET/Barber |
| Status - Allocated |
| MD5 Hash - 8f26262efc9ffb3efdbb224fc23f0fa0 |
| Created - 5/11/2021 9:39:41 AM |
| Accessed - 5/12/2021 2:24:35 PM |
| Modified - 5/11/2021 9:39:41 AM |
| Sector Location - 3,181,376 |
| File Description – Lady holding driver’s license to camera. |
| This photo suggests that Damon has coaxed the lady in the photo to show her credentials. |

|  |
| --- |
| Graphical user interface, text, application, chat or text message  Description automatically generated*Figure 5.* |
| File Name – 1.PNG |
| Type - png |
| Size – 22,898 bytes |
| Location - Partition2/root/users/Damon Hopkins/ Desktop/home/SECRET/Facebook |
| Status – Allocated |
| MD5 Hash - 71d27cdef738f7fd1fb5b637c0dab33d |
| Created - 4/19/2021 12:28:51 PM |
| Accessed - 5/6/2021 4:00:57 PM |
| Modified - 4/19/2021 12:28:51 PM |
| Sector Location - 20,846,000 |
| File Description – Screenshot of conversation between Damon (“Ben”) and “Muhammad”. |
| This conversation suggests criminal activity being discussed, specifically involving fraud between Damon and Muhammad. |

|  |
| --- |
| *Figure 6*. |
| File Name – Screenshot of encrypted files.jpg |
| Type - jpg |
| Size – 151006 bytes |
| Location – PC/Case Study/Case\_Study\_Exports |
| Status – Allocated |
| MD5 Hash of screenshot - a0240d5f5a1f2d2dfae8c485879322d3 |
| Created - 2022-10-25 11:43:04 AWST. |
| Accessed - 2022-10-25 11:43:04 AWST. |
| Modified - 2022-10-25 11:43:04 AWST. |
| Sector Location - |
| File Description – Screenshot location of 2 encrypted pdf files from Autopsy 4.19.1. |

|  |
| --- |
| *Figure 7.* |
| File Name – SAM |
| Type – File System |
| Size – 131072 bytes |
| Location - img\_caseStudyFinal.E01/vol\_vol3/Windows/System32/config/SAM |
| Status - Allocated |
| MD5 Hash of screenshot - 371bcf361c43a1380b5a8a73897c14f8 |
| Created -  2019-12-07 17:03:44 AWST |
| Accessed -  2021-05-14 13:41:24 AWST |
| Modified -  2021-04-15 20:36:15 AWST |
| Sector Location - Unknown |
| File Description – Creation of user account of Damon Hopkins |

|  |
| --- |
| *Figure 8*.Text  Description automatically generated |
| File Name – image0.jpg |
| Type - jpg |
| Size – 154777 bytes |
| Location - caseStudyFinal.E01/vol\_vol3/Users/Damon Hopkins/AppData/Local/Packages/Microsoft.windowscommunicationsapps\_8wekyb3d8bbwe/LocalState/Files/SO/3/Attachments/passport scan[16].pdf/image0.jpg. |
| Status - Allocated |
| MD5 Hash - f8cea14a090ce700cbe93da22f8dca95 |
| Created – Unknown |
| Accessed – Unknown |
| Modified - Unknown |
| Sector Location - Unknown |
| File Description – Scanned passport of Izaddin Bin Aris. |

# Issue 2. Identification.

## User

* There is a user account called “Damon Hopkins” on the device. User ID S-1-5-21-2659424124-211076020-1381419125-1001 confirmed as a “Normal user account” and the account was created on 2021-04-15 10:42:48 AWST.
* Damon Hopkins is believed to be the user and subsequent individual who obtained the passport images and credit card details, as the secret Facebook account found in the file tree on FTK Imager 5.0.3 Partition2/root/users/Damon Hopkins/ Desktop/home/SECRET/Facebook contains these various images which are described above in “Content relating to offence”.

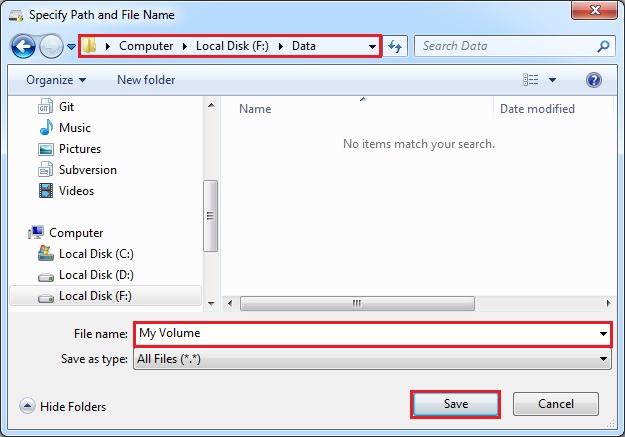
## Fraud

* The message between Damon (“Ben”) and Muhammad (Figure 5) suggests criminal activity being organised, specifically fraud as it is mentioned as “frauding”.
* Figures 1 and 2 containing a conversation between “unknown” and “Relaun Tucker” likely relate to fraud. Firstly because these files originate from a secret folder on Damon’s device; Partition2/root/users/Damon Hopkins/ Desktop/home/SECRET/Facebook. Secondly, the conversation contains elements of a typical scam conversation, where one person tries to convince the other that they are owed a large sum of money after an unknown relative has passed. To gain access to the money, they must provide valid credentials and credit card details to send the money through. The person Relaun is talking to, and friends with on Facebook as shown in the image, is not confirmed to be Damon, however as this file was found in the same SECRET Facebook directory as other suggestive evidence, it is likely to be Damon.
* The “Jane Citizen” passport photo (Figure 3) created 5/12/2021 1:09:22 PM matches with a Google Chrome search for “Jane Citizen” from 2021-05-11 17:44:51 AWST.

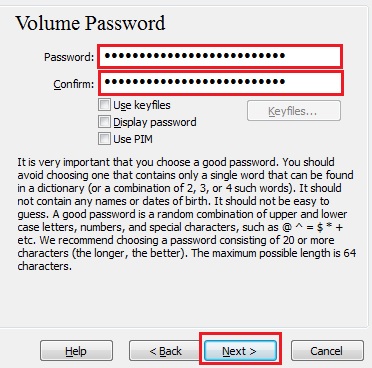
## Concealment

There is evidence of concealment of data likely related to identity theft as indicated by the downloaded programs TrueCrypt and VeryCrypt. Both programs have recently been used, as confirmed in Autopsy 4.19.1.

* TrueCrypt has been used to encrypt at least 2 pdf files.
* Veracrypt was used to password encrypt an entire drive on the device as shown below.

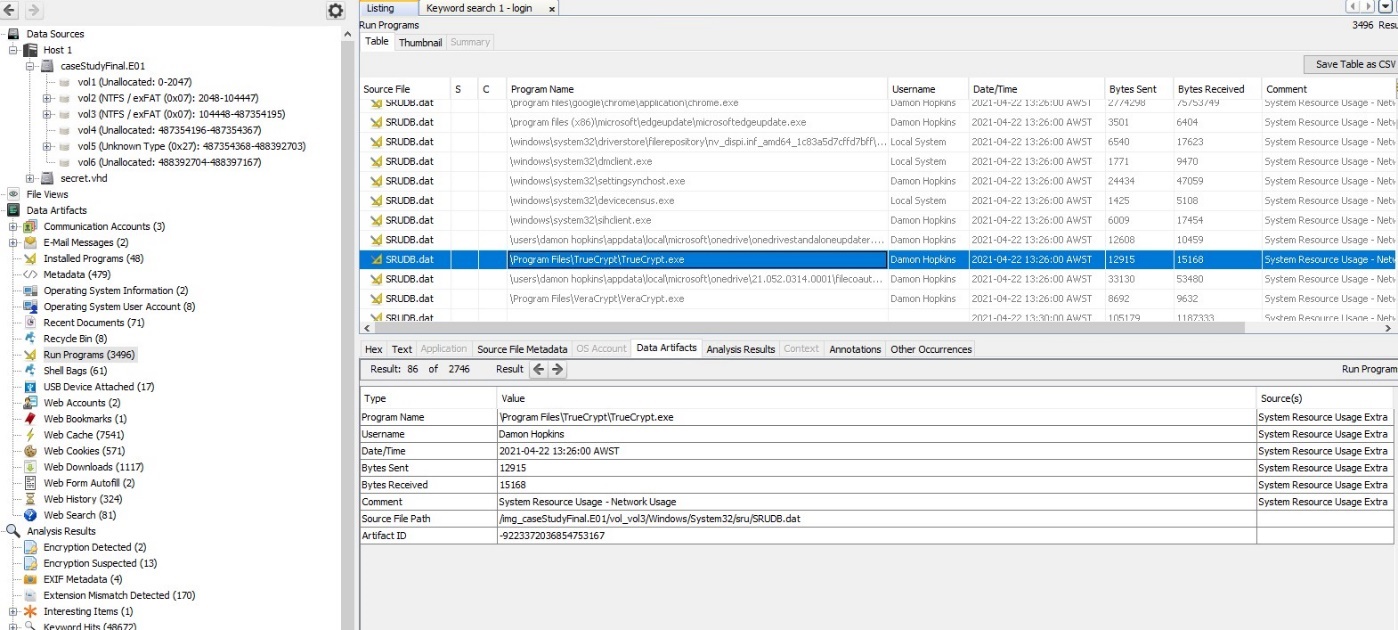
*Figure 9. VeraCrypt Drive Selection.*

*Figures 10 and 11. VeraCrypt Password and Volume Creation.*

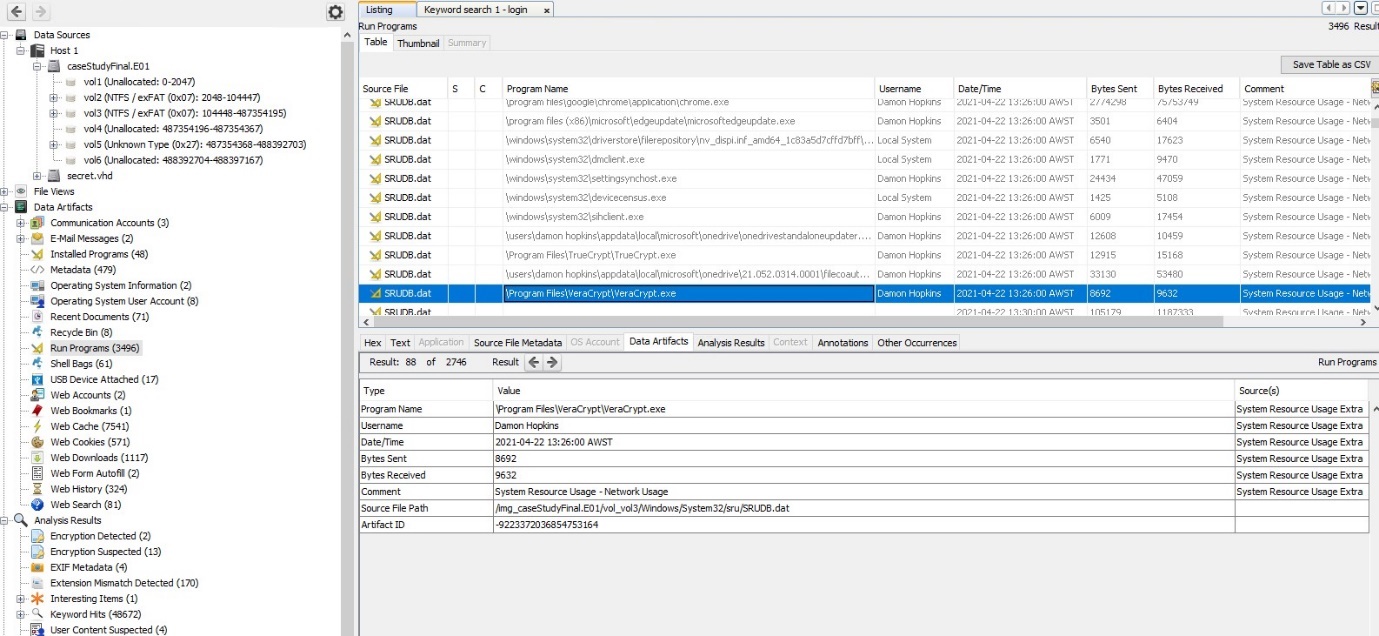
Graphical user interface, text, application

Description automatically generated

TrueCrypt.exe accessed on 2021-04-22 13:26:00 AWST by user “Damon Hopkins”.

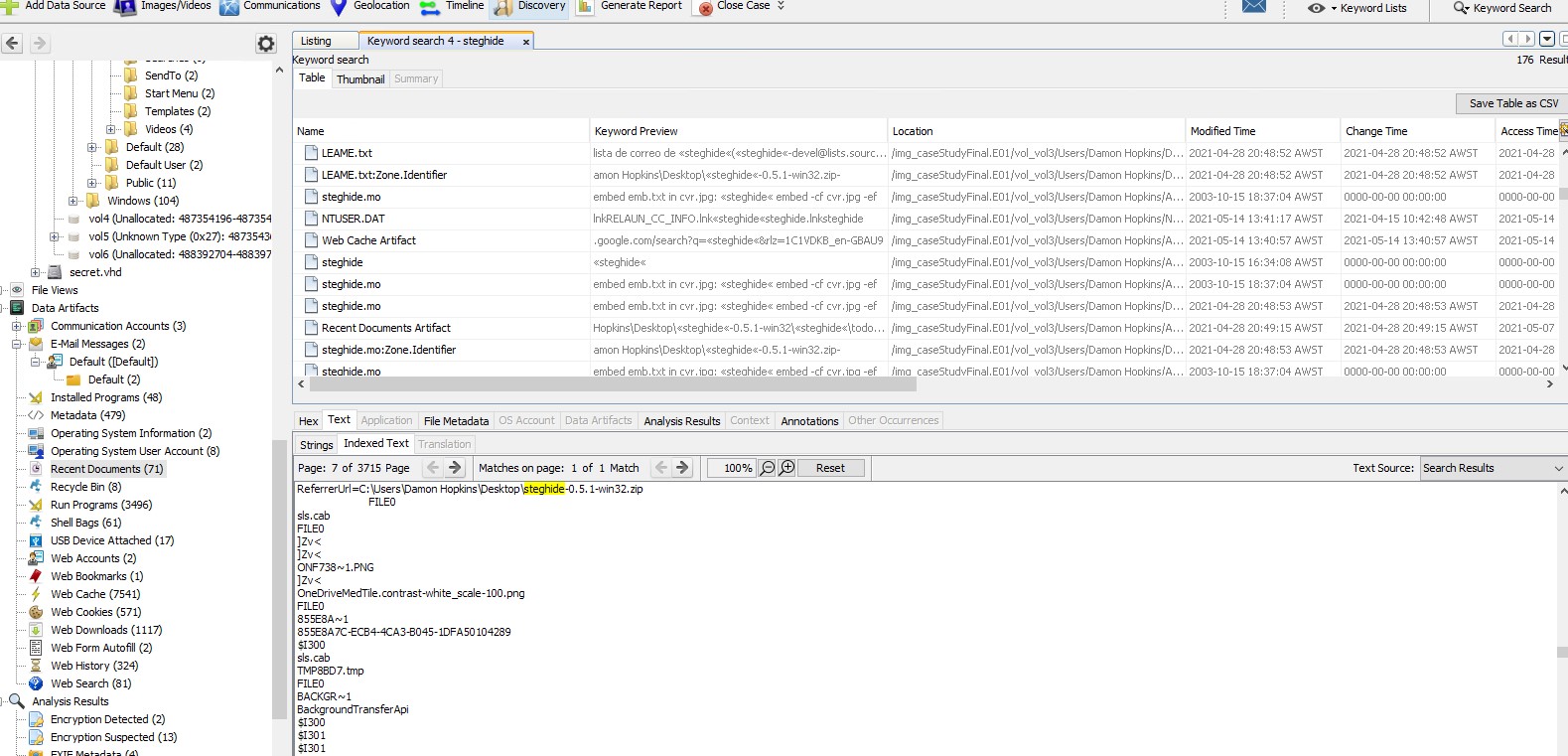
*Figure 12. TrueCrypt Access.*

VeraCrypt.exe accessed on 2021-04-22 13:26:00 AWST by user “Damon Hopkins”.



*Figure 13. VeraCrypt Access.*

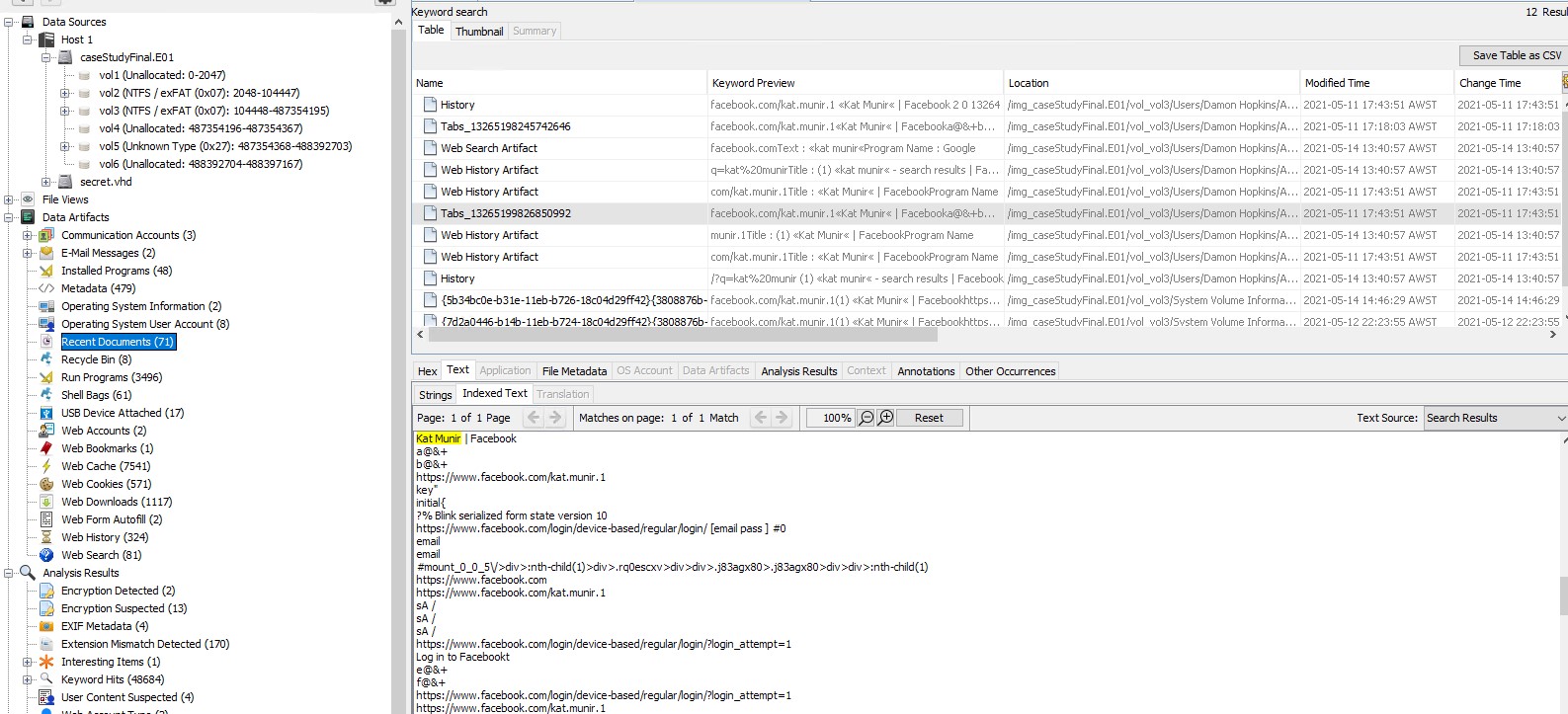
* There are a further 13 files found by Autopsy 4.19.1 with suspected encryption (Figure 14). They are located in: Data Sources/Data Artifacts/Analysis Results/Encryption Suspected. Of the 13 files, “Barber”, “Jane” and “Izaddin” are shown with the comment “suspected encryption due to high entropy”. This suggests that there could be more information on the drive related to the 3 individuals.
* The search in Autopsy 4.19.19 of the keyword “steghide” which resulted in 176 results indicates possible concealment of data in image files. Many of the search results showed the user account/file locations to be “Damon Hopkins”.



*Figure 14. Suspected Encrypted Files.*

# Issue 3. Intent.

There exists several instances of the name “Kat Munir” in Autopsy 4.19.1 relating to Facebook use. These include Facebook attempted logins and searches. These instances could suggest that Damon was attempting to obtain the credentials of “Kat Munir” but was likely stopped when his device was seized.



*Figure 15. Kat Munir keyword search.*

An active file “mpenginedb.db” was discovered using Autopsy 4.19.1 at location: Data Artifacts/Analysis Results/Encryption Suspected. This file was extracted and then an attempt was made at opening it using SQL Lite. However, an error message appeared stating “could not open database file. Reason: file is not a database.” This may suggest a database of stolen credentials was being compiled.

The encryption of the drive and files, and information relating to the user account “Damon Hopkins” indicates that the evidence found was obtained intentionally, and not by a third party.

# Issue 4. Quantity of Files

Total Images – 56271.

Total Videos – 23.

Total Audio – 480.

Total Databases – 75.

Total Archives – 394.

Total Documents (including, HTML, Office, PDF, Plain Text and Rich Text) 10558.

Total Executable (including exe, dll, bat, cmd, com) – 64306.

Total Deleted Files – 7404.

The files that were found and detailed under “Content related to offence” and subsequent files of interest detailed in the Running sheet (Appendix A) in comparison to the total number of undiscovered evidentiary files on the drive is relatively small. However it should be considered that much of the detailed evidence has been shown to originate from the user account “Damon Hopkins”.

# Issue 5. Installed Software.

* Microsoft Edge 2021-05-11 09:18:20 AWST
* Google Chrome v 90.0.4430.212 2021-05-13 03:34:14 AWST
* VeraCrypt v 1.24-Update7 2021-04-22 04:56:13 AWST
* TrueCrypt v 7.2 2021-04-22 04:32:24 AWST
* Steghide 0.5.1 2021-04-28 20:48:52 AWST

# Appendix A – Running Sheet

|  |  |  |
| --- | --- | --- |
| **Date/Time** | **Event** | **Duration** |
| 20/09/22 21:00pm | Generated Sha256 hashes for files caseStudyFinal.E01 – caseStudyFinal.E12 using HashCalc.  Output of Sha256:  caseStudyFinal.E01 - **a09854db7b5909440c2c5b1affe780f9d0e94906011803ad406f686daf1e4f13**  caseStudyFinal.E02 – **b628668e9198ba6a6f6e21a0678f99ffabb8c1ac37e19ddb349896924ff49ad5**  caseStudyFinal.E03 – **a40c3ca5d8b78faf399239c75a3eec027fa647f55c9733e274fbfd16bf9d7539**  caseStudyFinal.E04 – **7cdfaedd0721124c9f3c248263a3e23d75c89f4a459a54dbc96a7fb7f9e283f2**  caseStudyFinal.E05 – **9d691b0aaa56dbb767e4e4f22d2c6acfcc932a0ffe848dad108bd72b28878f75**  caseStudyFinal.E06 – **da0fe677e6e7a82ea76a7bb271dbaa20113637e672f242b7589f076a98f38c51**  caseStudyFinal.E07 – **25d3a6c80dd35793474a73d69b27ee77d2a52d820a4a7ddbcfc65650627e4235**  caseStudyFinal.E08 – **5c431d4d16f4605b64d240abfcaa7f90f930b14ba4d9e31603b08e6229d4b4d7**  caseStudyFinal.E09 – **0dcf7e0e404dc6ce610e428180e1b7f916fd1b5a0a2d3f14cdcc6ddf7927ceba**  caseStudyFinal.E10 – **4369d544dc6ad17829ddc29faa5d50c594d3d311c76c04fb471bd88407e740d3**  caseStudyFinal.E11 – **172cfb444b6a489c80e166ef08147c5f77a5a0a003e2b300cce1719f2e82a85c**  caseStudyFinal.E12 - **98f234790e8b28df027c5306aacd483f80a67c66ea441bdf78457f2e6e91b22b** | 12 mins. |
| 20/09/22 21:13pm | Generated copies of caseStudyFinal.E01 - caseStudyFinal.E12 and saved to new directory (Copies of Case Study Files) using Windows File Explorer | 10 mins. |
| 20/09/22 21:24pm | Generated Sha256 hash for copies of caseStudyFinal.E01 – caseStudyFinal.E12 using HashCalc and compared hashes to verify integrity.  Output of Sha256: **a09854db7b5909440c2c5b1affe780f9d0e94906011803ad406f686daf1e4f13**  caseStudyFinal.E02 – **b628668e9198ba6a6f6e21a0678f99ffabb8c1ac37e19ddb349896924ff49ad5**  caseStudyFinal.E03 – **a40c3ca5d8b78faf399239c75a3eec027fa647f55c9733e274fbfd16bf9d7539**  caseStudyFinal.E04 – **7cdfaedd0721124c9f3c248263a3e23d75c89f4a459a54dbc96a7fb7f9e283f2**  caseStudyFinal.E05 – **9d691b0aaa56dbb767e4e4f22d2c6acfcc932a0ffe848dad108bd72b28878f75**  caseStudyFinal.E06 – **da0fe677e6e7a82ea76a7bb271dbaa20113637e672f242b7589f076a98f38c51**  caseStudyFinal.E07 – **25d3a6c80dd35793474a73d69b27ee77d2a52d820a4a7ddbcfc65650627e4235**  caseStudyFinal.E08 – **5c431d4d16f4605b64d240abfcaa7f90f930b14ba4d9e31603b08e6229d4b4d7**  caseStudyFinal.E09 – **0dcf7e0e404dc6ce610e428180e1b7f916fd1b5a0a2d3f14cdcc6ddf7927ceba**  caseStudyFinal.E10 – **4369d544dc6ad17829ddc29faa5d50c594d3d311c76c04fb471bd88407e740d3**  caseStudyFinal.E11 – **172cfb444b6a489c80e166ef08147c5f77a5a0a003e2b300cce1719f2e82a85c**  caseStudyFinal.E12 - **98f234790e8b28df027c5306aacd483f80a67c66ea441bdf78457f2e6e91b22b** | 12 mins. |
| 20/09/22 21:37pm | Opened caseStudyFinal.E01 in FTKImager V4.5.0.3 | 1 min. |
| 20/09/22 21:39pm | Opened the directory tree: caseStudyFinal.E01/Partition2(237914mb)/NONAME[NTFS]/root/Recycle.Bin/S-1-5-21-2659424124-211076020-1381419125-1001/$RB56WVI.zip/VeraCrypt\_1.24/doc/EFI-DCS/ in FTKImager V4.5.0.3.  Discovered 2 active files; disk\_encryption\_v1\_2.pdf (134,972 bytes modified on 10/6/2019 7:14:44 PM)  and dcs\_tpm\_owner\_02.pdf (134,667 bytes modified on 10/6/2019 7:14:44 PM). | 1 min. |
| 20/09/22 21:40pm | [Right click] on file disk\_encryption\_v1\_2.pdf > Export file hash list to Desktop/Case\_Study\_Exports. Saved as disk\_encryption\_v1\_2\_hash.csv | 1 min. |
| 20/09/22 21:40pm | [Right click] on file dcs\_tpm\_owner\_02.pdf > Export file hash list to Desktop/Case\_Study\_Exports. Saved as dcs\_tpm\_owner\_02\_hash.csv | 1 min. |
| 20/09/22 21:40pm | Opened both newly created csv files from Desktop/Case\_Study\_Exports in Notepad v1809. Checked MD5 hashes for both.  disk\_encryption\_v1\_2\_hash.csv MD5 hash – **1d8e803c77fcac87d7a6010cb2ad7b8b**  dcs\_tpm\_owner\_02\_hash.csv MD5 hash - **8a9ca89a9946534eedb2542c198bfc40** |  |
| 20/09/22 21:40pm | [Right click] Exported disk\_encryption\_v12.pdf file from FTKImager V4.5.0.3 to newly created folder on Windows desktop/Case\_Study\_Exports.  Opened disk\_encryption\_v1\_2.pdf in HashCalc and generated MD5 hash.  Result - **1d8e803c77fcac87d7a6010cb2ad7b8b**  Confirmed the 2 hashes match. | 1 min. |
| 20/09/22 21:41pm | Opened disk\_encryption\_v1\_2.pdf from Desktop/Case Study\_Exports. Discovered instructions for VeraCrypt use. | 1 min. |
| 20/09/22 21:42pm | [Right click] Exported dcs\_tpm\_owner\_02.pdf file from FTKImager V4.5.0.3 to newly created folder on Windows desktop/Case\_Study\_Exports.  Opened dcs\_tpm\_owner\_02.pdf in HashCalc and generated MD5 hash.  Result - **8a9ca89a9946534eedb2542c198bfc40**  Confirmed the 2 hashes match. | 1 min. |
| 20/09/22 21:43pm | Opened dcs\_tpm\_owner\_02.pdf file from Desktop/Case\_Study\_Exports. Discovered instructions for VeraCrypt TPM use. | 1 min |
| 20/09/22 21:44pm | Google search in Google Chrome browser for ‘what is TPM’. trustedcomputinggroup.org reports that a TPM (Trusted Platform Module) is a “computer chip that can securely store artifacts used to authenticate the platform (your PC or laptop). | 30 secs |
| 20/09/22 21:44pm | Opened the directory tree: Partition2/root/users in FTKImager V4.5.0.3.  Discovered username “Damon Hopkins” and expanded directory tree. | 1 min |
| 20/09/22 21:45pm | Expanded Desktop/home/SECRET/Barber folder in “Damon Hopkins” directory. | 30 secs |
| 20/09/22 21:47pm | Discovered 2 active files:   * CC.txt (36 bytes) created on 5/11/2021 9:39:50 AM and * F963D7BF-2350-4461-A50C-03B21E806637[23].jpg (149,970 bytes) on starting sector 3,181,376 created on 5/11/2021 9:39:41 AM   The txt file appears to be credit card information.  The jpg file is a photo of a lady holding a driver’s license to the camera. She resembles the photo on the license. The name is “Jennifer Leah Barber”. | 2 mins |
| 20/09/22 21:50pm | [Right click] CC.txt > Export file hash list to Desktop/Case\_Study\_Exports. Saved as CC\_hash.csv  [Right click] F963D7BF-2350-4461-A50C-03B21E806637[23].jpg > Export file hash list to Desktop/Case\_Study\_Exports. Saved as F963D7BF-2350-4461-A50C-03B21E806637[23].csv | 4 mins. |
|  | Opened both newly created csv files from Desktop/Case\_Study\_Exports in Notepad v1809. Checked MD5 hashes for both.  cc\_hash.csv MD5 hash – **f29e2c333578982d19d69711c931bc08**  F963D7BF-2350-4461-A50C-03B21E806637[23]\_hash.csv MD5 hash - **8f26262efc9ffb3efdbb224fc23f0fa0** | 2 mins. |
| 20/09/22 21:56pm | [Right click] Exported cc.txt from FTKImager V4.5.0.3 to newly created folder on Windows desktop/Case\_Study\_Exports.  Opened cc.txt in HashCalc and generated MD5 hash.  Result - **f29e2c333578982d19d69711c931bc08**  Confirmed the 2 hashes match.  [Right click] Exported F963D7BF-2350-4461-A50C-03B21E806637[23].jpg from FTKImager V4.5.0.3 to newly created folder on Windows desktop/Case\_Study\_Exports.  Opened F963D7BF-2350-4461-A50C-03B21E806637[23].jpg in HashCalc and generated MD5 hash.  Result - **8f26262efc9ffb3efdbb224fc23f0fa0**  Confirmed the 2 hashes match. | 4 mins. |
| 21/09/22 06:18am | Expanded Desktop/home/SECRET/Facebook folder in “Damon Hopkins” directory using FTKImager V4.5.0.3.  Discovered 3 active files;   * 1.PNG (22,898 bytes on starting sector 20,846,000 created on 4/19/2021 12:28:51 PM). A screenshot of a conversation between Damon (“Ben”) and “Muhammad” talking about recent activities, exchange of email addresses and fraud. * Relaun1.PNG (76,089 bytes starting on sector 47,896,008 created on 5/4/2021 7:11:42 AM). Screenshot of a Facebook message conversation between “Relaun Tucker” who is friends on Facebook with “unknown”. The unknown informs Relaun he has money owed to him from a deceased Aunt’s estate, totalling 26.7 million US dollars. Unknown also claims to be the Aunt’s attorney. * Relaun2.PNG (171,936 bytes starting on sector 3,848,224 created on 5/4/2021 7:12:03 AM). Screenshot of the continued conversation; the unknown asks Relaun for photo identification and credit card details to “wire funds” from the deceased estate. Relaun sends a photo of his drivers license with all valid credentials visible, followed by credit card details. | 5 mins. |
| 21/09/22 06:24am | [Right click] on file 1.PNG > Export file hash list to Desktop/Case\_Study\_Exports. Saved as 1\_hash.csv  [Right click] on file Relaun1.PNG > Export file hash list to Desktop/Case\_Study\_Exports. Saved as Relaun1\_hash.csv  [Right click] on file Relaun2.PNG > Export file hash list to Desktop/Case\_Study\_Exports. Saved as Relaun2\_hash.csv | 2 mins. |
| 21/09/22 06:26am | Opened newly created csv files from Desktop/Case\_Study\_Exports in Notepad v1809. Checked MD5 hashes for all 3.  1\_hash.csv MD5 hash – **71d27cdef738f7fd1fb5b637c0dab33d**  Relaun1\_hash.csv MD5 hash - **ac32854c20cfd6722b69af36a96f7712**  Relaun2\_hash.csv MD5 hash - **b8952ec09a41fcba867e25d7982fcf41** | 2 mins. |
| 21/09/22  06:28am | [Right click] Exported 1.PNG from FTKImager V4.5.0.3 to newly created folder on Windows desktop/Case\_Study\_Exports.  Opened 1.PNG in HashCalc and generated MD5 hash.  Result - **71d27cdef738f7fd1fb5b637c0dab33d**  Confirmed the 2 hashes match.  [Right click] Exported Relaun1.PNG from FTKImager V4.5.0.3 to newly created folder on Windows desktop/Case\_Study\_Exports.  Opened Relaun2.PNG in HashCalc and generated MD5 hash.  Result - **ac32854c20cfd6722b69af36a96f7712**  Confirmed the 2 hashes match.  [Right click] Exported Relaun2.PNG from FTKImager V4.5.0.3 to newly created folder on Windows desktop/Case\_Study\_Exports.  Opened Relaun2.PNG in HashCalc and generated MD5 hash.  Result - **b8952ec09a41fcba867e25d7982fcf41**  Confirmed the 2 hashes match. | 5 mins. |
| 22/09/22  06:20am | Expanded directory tree Data Artifacts/E-Mail Messages/Default/([Default])/Default(2) using Autopsy 4.19.1.  Discovered 2 active files:   1. Tech Support[19].eml. Contains an email sent from [damonhopkins22@outlook.com](mailto:damonhopkins22@outlook.com) to [chungtujyoung@keenmail.com](mailto:chungtujyoung@keenmail.com) on 2021-05-04 15:14:25 AWST. Subject: Tech Support. Damon claims to be a representative from Microsoft who can help with abnormal activity that has been seen on Chung’s device. 2. msg\_43.txt Contains an email sent from ; >; to [webmaster@python.org](mailto:webmaster@python.org) on 2004/11/27 11:41:44 AWST. Subject: Banned file: auto\_mail.python.bat in mail from you. Email body contains numerous email addresses from @dot.ca.gov where the mail was not delivered due to an attachment being blocked by the spam firewall. The subject is: Delivery\_failure\_notice. | 10 mins |
| 22/09/22  06:55am | Expanded the directory tree Partition2/NONAME[NTFS]/root/$Recycle.Bin/S-1-5-21-2659424124-211076020-1381419125-1001 in FTK Imager 4.5.0.3. Discovered 18 active files of various extensions (zip, jpg, txt, ink, ini).  jpg file $RSQETAE.JPG (46,173 bytes) on starting cluster 369,396. Date created 5/12/2021 1:09:22 PM, is a passport photo of “Jane Citizen” with all relevant details visible. | 10 mins |
| 22/09/22  06:55am | [Right click] on file $RSQETAE.JPG > Export file hash list to Desktop/Case\_Study\_Exports. Saved as $RSQETAE.JPG\_hash.csv | 30 secs. |
| 22/09/22  06:55am | Opened $RSQETAE.\_hash.csv file from Desktop/Case\_Study\_Exports in Notepad v1809. Checked MD5 hash.  $RSQETAE.JPG\_hash.csv MD5 hash – **03abb0237daa9f16b54d1f20338becbf** | 3 mins. |
|  | [Right click] Exported $RSQETAE.JPG from FTKImager V4.5.0.3 to newly created folder on Windows desktop/Case\_Study\_Exports.  Opened $RSQETAE.JPG in HashCalc and generated MD5 hash.  Result - **03abb0237daa9f16b54d1f20338becbf**  Confirmed the 2 hashes match. |  |
| 22/09/22  07:05am | Keyword search for “Jane Citizen” using Autopsy 4.19.1 revealed 16 results including:   1. Facebook search for “Jane Citizen” using Google Chrome.   URL : https://www.facebook.com/search/top/?q=jane%20citizen  Date Accessed : 2021-05-11 17:44:51 AWST  Referrer URL : https://www.facebook.com/search/top/?q=jane%20citizen  Title : jane citizen - search results | Facebook  Program Name : Google Chrome  Domain : facebook.com   1. $RVVLPK8.txt file (active) containing credit card details.   Name on card : Jane Citizen  Card number : 89876454346698675  Expr : nov 2024  cvs : 745 | 2 mins. |
| 28/09/22  10:35am | Opened Case\_Study in Autopsy 4.19.1. Navigated to Data Sources/Data Artifacts/Installed Programs. Discovered 48 installed programs. | 2 mins |
| 28/09/22  10:37am | Searched through list of 48 installed programs to determine any that may be of interest to the case. Discovered “Microsoft Edge 90.0.818.56, Python 3.9.4, Address Book, Google Chrome 90.0.4430.212, VeraCrypt 1.24 and TrueCrypt 7.2” | 12 mins |
| 28/09/22  10:55am | Navigated to Data Sources/Data Artifacts/Web Accounts and discovered 2 accounts:   1. Facebook, Date Created 2021-04-19 20:28:00 AWST. Username: [damon.hopkins11@outlook.com](mailto:damon.hopkins11@outlook.com) using Google Chrome. 2. Live.com Date Created 2021-04-19 20:34:12 AWST. Username damonhopkins22@outlook.com using Google Chrome. | 7 mins |
| 28/09/22  11:05am | Navigated to Data Sources/Data Artifacts/Operating System Information to determine OS and file system in use on laptop. Determined Windows 10 Home dated 2021-04-15 02:39:01 AWST. Owner: Damon Hopkins. Product ID: 00326-10000-00000-AA341. | 3 mins |
| 28/09/22  11:10am | Navigated to Data Sources/Data Artifacts/Operating System User Account to determine number of user accounts on the laptop. Discovered 8 username entries; 1 belonging to Damon Hopkins. | 2 mins |
| 28/09/22  11:15am | 1. Navigated to Data Sources/Data Artifacts/Shellbags. Discovered 61 entries with 13 of interest. 2. My Computer\CLSID\_Desktop\Home\SECRET\Izaddin 3. My Computer\CLSID\_Desktop\Home\SECRET\Relaun 4. My Computer\CLSID\_Desktop\Home\SECRET\Barber 5. My Computer\CLSID\_Desktop\Home\SECRET\Facebook 6. My Computer\CLSID\_Desktop\VeraCrypt\_1.24 7. My Computer\CLSID\_Desktop\Work 8. My Computer\CLSID\_Desktop\steghide-0.5.1-win32\steghide 9. My Computer\CLSID\_Desktop\s-tools4 10. My Computer\Z:\ 11. My Computer\T:\ 12. My Computer\E:\\Users 13. Users\AppData\Local\Programs\Python | 10 mins |
| 28/09/22  11:26am | Performed a search for “Izaddin” in Case\_Study using Autopsy 4.19.1.  Returned 60 results.  Results of interest:   1. Recycle Bin Artifact.   Path : C:\Users\Damon Hopkins\Desktop\Home\SECRET\Izaddin\izaddin  Time Deleted : 2021-04-22 13:28:53 AWST  Username : Damon Hopkins   1. Web History Artifact.   URL : file:///C:/Users/Damon%20Hopkins/Desktop/Home/SECRET/  Izaddin/Passport%20scan[16].pdf  Date Accessed : 2021-04-22 04:26:51 AWST  Referrer URL :  Title :  Program Name : Microsoft Edge  Domain :  Username : Damon Hopkins   1. Web History Artifact.   URL : file:///C:/Users/Damon%20Hopkins/Desktop/Home/SECRET/  Izaddin/Izaddin%20Details.odt  Date Accessed : 2021-04-22 04:30:35 AWST  Referrer URL :  Title :  Program Name : Microsoft Edge  Domain :  Username : Damon Hopkins   1. Web History Artifact.   URL : file:///C:/Users/Damon%20Hopkins/Desktop/Home/SECRET/  Izaddin/secret.vhd  Date Accessed : 2021-04-22 04:47:02 AWST  Referrer URL :  Title :  Program Name : Microsoft Edge  Domain :  Username : Damon Hopkins   1. Izaddin Details.odt   Full name : Izaddin Bin Aris  DOB : 10/11/1951  Maiden Name : Arouja  CCN: 67655208265  CC Ex : 08/2023  Csv : 895  Phone Number : 987254267  Contains credit card details.   1. Metadata from Izaddin Details.odt file:   Author: Damon Hopkins  Character Count: 129  Content-Type: application/vnd.oasis.opendocument.text  Creation-Date: 2009-04-16T11:32:02.64  Edit-Time: PT53S  Image-Count: 0  Last-Modified: 2021-04-22T12:31:08.06  Last-Save-Date: 2021-04-22T12:31:08.06 | 10 mins. |
| 28/09/22  2:45pm | Navigated to Host 1/caseStudyFinal.E01/vol3 (NTFS /exFAT (0x07): 104448-487354195)/Users/Damon Hopkins/Desktop/Home/SECRET/Izaddin.  Discovered active file “Izaddin Bin Aris.odt”  Contents - Full name : Izaddin Bin Aris  DOB : 10/11/1951  Maiden Name : Arouja  CCN: 67655208265  CC Ex : 08/2023  Csv : 895  Phone Number : 987254267  Discovered active file “Passport scan [16].pdf. Contains a scanned picture (image0.jpg) of a passport belonging to Izaddin Bin Aris with all personal details shown.  [Right click] extract file to Dekstop/Case\_Study\_Exports/image0.jpg  Opened image0.jpg file in HashCalc and checked MD5 hash.  MD5 - **f8cea14a090ce700cbe93da22f8dca95** | 10 mins |
| 28/09/22  2:57pm | Navigated to Data Artifacts/Recycle Bin. Discovered file “$RVVLPK8.txt” which contains credit card details for “Jane Citizen”.  Name on card : Jane Citizen  Card number : 89876454346698675  Expr : nov 2024  cvs : 745 | 4 mins. |
| 28/09/22  3:15pm | Navigated to /Data Artifacts/Analysis Results/Encryption Suspected. Discovered active file “mpenginedb.db”  [Right click] extract file to Desktop/Case\_Study\_Exports.  Attempted to open file in DB Browser for SQLite but received an error: “Could not open database file. Reason: file is not a database.” | 4 mins. |
| 04/10/22  5:30am | Opened OSForensics 8.0.1008 – Trial Version and created a new case called “Case Study”.  Clicked on “Add to Case – Device – Image File – caseStudyfinal.E01  Selected Partition 1 – 232.gb (NTFS). Created new index.  Clicked on Program Artifacts and then TRUECRYPT.EXE-CD68308F.pf  Last Run Time 4/22/2021 12:45:12 | 15mins. |
| 04/10/22  5:45am | Opened Case\_Study in Autopsy 4.19.1.  Searched for “truecrypt” Returned 24 results.  Result located at:   |  |  | | --- | --- | |  | /img\_caseStudyFinal.E01/vol\_vol3/Users/Damon Hopkins/AppData/Local/Google/Chrome/User Data/Default/Cache/f\_000174/VeraCrypt\_1.24/src/License.html  Modified Time 2019-10-07 01:14:45 AWST  MD5 Hash 71b08138acbbc3b87c387d51c3edfab3 | | 5mins. |
| 04/10/22  10:15pm | Opened Case\_Study in Autopsy 4.19.1.  Navigated to File Views/File Types/By Extension/Images/  Opened “Beginner’s Tutorial\_Image\_001.jpg - Beginner’s Tutorial\_Image\_014.jpg”.  All the included jpg files are screenshots of the encryption of a drive at each step of the process using VeryCrypt.  “Beginner’s Tutorial\_Image\_006.jpg” is not present.  Beginner’s Tutorial\_Image\_001.jpg. Date Created 2019-10-06 19:14:44 AWST. Date Modified 2021-04-22 12:56:17 AWST. Size 72868 bytes. Unallocated. Image shows VeraCrypt drive selection screen with “Create Volume” button highlighted.  Beginner’s Tutorial\_Image\_002.jpg. Date Created 2019-10-06 19:14:44 AWST. Date Modified  2021-04-22 12:56:17 AWST. Size 97433 bytes. Unallocated. Image shows “VeraCrypt Volume Creation Wizard” screen with “Create an Encrypted File Container” button highlighted.  Beginner’s Tutorial\_Image\_003.jpg. Date Created 2019-10-06 19:14:44 AWST. Date Modified 2021-04-22 12:56:17 AWST. Size 45726 bytes. Unallocated. Image shows “ Volume type” screen with “Standard VeraCrypt volume” button highlighted.  Beginner’s Tutorial\_Image\_004.jpg. Date Created 2019-10-06 19:14:44 AWST. Date Modified 2021-04-22 12:56:17 AWST. Size 60635 bytes. Unallocated. Image shows “ Volume Location” screen with “Select file” button highlighted and “Never save history” box checked.  Beginner’s Tutorial\_Image\_005.jpg. Date Created 2019-10-06 19:14:44 AWST. Date Modified 2021-04-22 12:56:17 AWST. Size 67538 bytes. Unallocated. Image shows “Specify path and file name” screen.” Computer > Local Disk (F:) > Data is highlighted at the top of the selection window. File name – “My Volume” is highlighted at the bottom of screen. “Save” button is highlighted.  Beginner’s Tutorial\_Image\_007.jpg. Date Created 2019-10-06 19:14:44 AWST. Date Modified 2019-10-07 01:14:45 AWST. Size 60251 bytes. Unallocated. Image shows “Volume Location” screen with “F:\Data/My Volume” selected and the “Next” button highlighted.  Beginner’s Tutorial\_Image\_008.jpg. Date Created 2019-10-06 19:14:44 AWST. Date Modified 2021-04-22 12:56:17 AWST. Size 44347 bytes. Unallocated. Image shoes “Encryption Options” with 2 drop boxes. First one has “AES” selected. The second has “SHA-512’ selected. The “next” button is highlighted.  Beginner’s Tutorial\_Image\_009.jpg. Date Created 2019-10-06 19:14:44 AWST. Date Modified 2021-04-22 12:56:17 AWST. Size 36014 bytes. Unallocated. Image shoes “Volume Size” selection screen with 250 mb selected. Free space on drive F:\ is 27.87 GB. “Next” button is highlighted.  Beginner’s Tutorial\_Image\_010.jpg. Date Created 2019-10-06 19:14:44 AWST. Date Modified 2021-04-22 12:56:17 AWST. Size 65196 bytes. Unallocated. Image shows “Volume Password” screen with a 26-character password having been entered and confirmed in the box below. “Next” button is highlighted.  Beginner’s Tutorial\_Image\_011.jpg. Date Created 2019-10-06 19:14:44 AWST. Date Modified 2021-04-22 12:56:17 AWST. Size 58346 bytes. Unallocated. Image shows “Volume Format” screen with “Filesystem FAT” selected and “cluster default” selected. “Random collected from mouse movements is shown as a horizontal green progress bar roughly ¾ the total length of the bar. “Next” button is highlighted.  Beginner’s Tutorial\_Image\_012.jpg. Date Created 2019-10-06 19:14:44 AWST. Date Modified 2021-04-22 12:56:17 AWST. Size 18934 bytes. Unallocated. Image shows “VeraCrypt Volume Creation Wizard ” screen with the message “The VeryCrypt volume has been successfully created.  Beginner’s Tutorial\_Image\_013.jpg. Date Created 2019-10-06 19:14:44 AWST. Date Modified 2021-04-22 12:56:17 AWST. Size 21278 bytes. Unallocated. Image shows “Volume Created” screen and confirmation the Veracrypt volume has been created and is ready for use. The “Exit” button is highlighted.  Beginner’s Tutorial\_Image\_014.jpg. Date Created 2019-10-06 19:14:44 AWST. Date Modified 2021-04-22 12:56:17 AWST. Size 76689 bytes. Unallocated. Image shows drive selection screen with “M:” highlighted.  Beginner’s Tutorial\_Image\_015.jpg. Date Created 2019-10-06 19:14:44 AWST. Date Modified 2021-04-22 12:56:17 AWST. Size 76354 bytes. Unallocated. Image shows “M:” and “Select File” highlighted.  Beginner’s Tutorial\_Image\_016.jpg. Date Created 2019-10-06 19:14:44 AWST. Date Modified 2021-04-22 12:56:17 AWST. Size 69892 bytes. Unallocated. Image shows “Select a Verycrypt Volume” screen with File Explorer screen > Computer > Local Disk (F:) > Data location selected. “My Volume, Date Modified 12/30/2014 11:28” and “Open” highlighted.  Beginner’s Tutorial\_Image\_017.jpg. Date Created 2019-10-06 19:14:44 AWST. Date Modified 2021-04-22 12:56:17 AWST. Size 77042 bytes. Unallocated. Image shows drive selection screen with “M:” highlighted and the “Mount” option highlighted.  Beginner’s Tutorial\_Image\_018.jpg. Date Created 2019-10-06 19:14:44 AWST. Date Modified 2021-04-22 12:56:17 AWST. Size 34325 bytes. Unallocated. Image shows “Enter Password for F:\Data\My Volume”. “Password” field is highlighted.  Beginner’s Tutorial\_Image\_019.jpg. Date Created 2019-10-06 19:14:44 AWST. Date Modified 2021-04-22 12:56:17 AWST. Size 36310 bytes. Unallocated. Image shows 26- character password entered and “PKCS-5 PRF” highlighted with “HMAC-SHA-512” selected. “OK” button is highlighted.  Beginner’s Tutorial\_Image\_020.jpg. Date Created 2019-10-06 19:14:44 AWST. Date Modified 2021-04-22 12:56:17 AWST. Size 79449 bytes. Unallocated. Image shows VeryCrypt drive selection screen with “M: F:\Data\My Volume, Size 249 MB, Encryption Algorithm AES and Type Normal” highlighted.  Beginner’s Tutorial\_Image\_021.jpg. Date Created 2019-10-06 19:14:44 AWST. Date Modified 2021-04-22 12:56:17 AWST. Size 45484 bytes. Unallocated. Image shows Windows Explorer screen with “Computer” selected and “Local Disk (M:) selected.  Beginner’s Tutorial\_Image\_022.jpg. Date Created 2019-10-06 19:14:44 AWST. Date Modified 2021-04-22 12:56:17 AWST. Size 79812 bytes. Unallocated. Image shows VeryCrypt drive selection screen with “M: F:\Data\My Volume, Size 249 MB, Encryption Algorithm AES and Type Normal” highlighted. The “Dismount” button is selected.  Beginner’s Tutorial\_Image\_034.png. Date Created 2019-10-06 19:14:44 AWST. Date Modified 2021-04-22 12:56:17 AWST. Size 17113 bytes. Unallocated. Image shows “Partition 1” labelled as “Decoy Operating System” with a pink background colour and “Partition 2” labelled “Outer Volume” with a cream/yellow background colour. A separate box containing “Hidden Volume” and “Hidden Operating System” placed together with a pink and green striped background. | 10 mins. |
| 25/10/22  09:40am | Opened Case\_Study in Autopsy 4.19.1. Navigated to Data Artifacts/Web Search. Discovered a Google search history file for “identity fraud statistics” using Google Chrome on 2021-04-19 20:23:00 AWST.  Discovered a Google search history file for “truecrypt” using Google Chrome on 2021-04-22 12:29:38 AWST.  Discovered a Google search history file for “encryption software” using Google Chrome on 2021-04-22 12:40:11 AWST.  Discovered a Google search history file for “veracrypt” using Google Chrome on 2021-04-22 12:40:47 AWST.  Discovered a Google search history file for “facebook” using Google Chrome on 2021-04-27 22:15:36 AWST.  Discovered a Google search history file for “relaun tucker” using Google Chrome on 2021-04-27 22:16:55 AWST.  Discovered a Google search history file for “barber leah” using Google Chrome on 2021-05-06 23:47:00 AWST.  Discovered a Google search history file for “jane citizen” using Google Chrome on 2021-05-11 17:44:51 AWST. | 5 mins. |
| 25/10/22  11:40am | Opened file tree Analysis Results/Encryption Detected. Discovered 2 files with locations containing encrypted files.   1. caseStudyFinal.E01/vol\_vol3/Users/Damon Hopkins/AppData/Local/Packages/Microsoft.windowscommunicationsapps\_8wekyb3d8bbwe/LocalState/Files/SO/3/Attachments/tips[4].pdf 2. caseStudyFinal.E01/vol\_vol3/Users/Damon. Hopkins/Downloads/tips[4].pdf. Created 2021-04-20 19:49:56 AWST.   Navigated to location 1. Discovered caseStudyFinal.E01/vol\_vol3/Users/Damon Hopkins/AppData/Local/Packages/Microsoft.windowscommunicationsapps\_8wekyb3d8bbwe/LocalState/Files/SO/3/Attachments/passport scan[16].pdf/image0.jpg. Size 154777 bytes.  Navigated to location 2. Discovered encrypted pdf file. When clicked on, access was not allowed without correct password. Screenshot created of file location in Autopsy 4.19.1 and saved on Desktop/Case Study/Case\_Study\_Exports as Screenshot of encrypted pdf files.jpg. Date Created 2022-10-25 11:43:04 AWST. | 20 mins. |
| 25/10/22  1:10pm | Navigated to Data Sources/Data Artifacts/Operating System User Account. Discovered 8 accounts. One of these is named “Damon Hopkins” Date Created 2021-04-15 10:42:48 AWST and flagged as “Normal user account”. | 5 mins. |
| 25/10/22 1:50 pm | Performed keyword search for “Kat Munir” using Autopsy 4.19.1 after noticing the name appear several times while looking through other evidence. Several entries were discovered relating to Facebook searches. | 5 mins. |
| 25/10/22  2:45 pm | Navigated to caseStudyFinal.E01/vol\_vol3/Users/Damon Hopkins/Desktop/steghide-0.5.1-win32 in Autopsy 4.19.1.  Files were seen in “Recent Documents” that contained the term “steghide”.  Steghide is a tool used to hide data inside image files.  Performed a keyword search in Autopsy “steghide” which returned 176 results. | 10 mins. |

# Appendix B – Timeline of Events

|  |  |  |
| --- | --- | --- |
| **DATE** | **TIME** | **EVENT** |
| 2019-10-06 | 19:14:44 AWST | VeraCrypt program used to encrypt drive |
| 2019-12-07 | 17:03:44 AWST | Damon Hopkins account created |
| 2021-04-19 | 12:28:51 PM | Fraud conversation between Damon and Muhammad |
| 2021-05-04 | 7:11:42 AM | Conversation with “Relaun Tucker” |
| 2021-05-11 | 17:44:51 | Google search for “Jane Citizen” |
| 2021-05-11 | 9:39:41 AM | Photo of “Barber” |
| 2021-05-12 | 1:09:22 PM | Passport photo of Jane Citizen |
| Unknown | Unknown | Passport of Izaddin Bin Aris |