Assignment 2 – Case Study

CSG2305.3 – Computer Forensics

Ky Woodyard - 10632627

2024

Table of Contents

[Summary 2](#_Toc180409637)

[Issue #1 - Can Content Related to the Offence Be Found in the Digital Forensic Image of the Volume of the Drive of the Suspect’s Computer? 2](#_Toc180409638)

[Artifact #1 3](#_Toc180409639)

[Artifact #2 3](#_Toc180409640)

[Artifact #3 3](#_Toc180409641)

[Artifact #4 4](#_Toc180409642)

[Artifact #5 4](#_Toc180409643)

[Artifact #6 4](#_Toc180409644)

[Issue #2 - If Illegal Content Related to the Offence Is Present, Can the Suspect Be Linked to It? 5](#_Toc180409645)

[Issue #3 - Was the Content Accessed/Distributed Intentionally? 5](#_Toc180409646)

[Issue #4 - How Many Files Were Present in the System? 6](#_Toc180409647)

[Issue #5 - Was Any of the Installed or Previously Removed Software Used for the Alleged Crime? 7](#_Toc180409648)

[Running Sheet 0](#_Toc180409649)

[Timeline of Events 6](#_Toc180409650)

# Summary

The focus of this investigation involves John Hopkinson, a senior analyst who complained that his antivirus programme was not updating when he was working remotely. While trying to fix the antivirus issue, an IT specialist came across digital material that made them suspicious of illicit activity. The probe specifically looks on claims of illegal drug and firearm trafficking. The evidence points to internet research on drug kinds, popular substances, and how to acquire and sell them, including attempts to get in touch with a dealer and conduct anonymous transactions using bitcoin.

Here is the specifications of the devices image that was investigated:

|  |  |
| --- | --- |
| Image Name | /img\_drugs.E01 |
| Type | E01 |
| Size | 1000202273280 |
| MD5 | 8542f83945d3a4492a4b0b1cfeba9128 |
| Sector Size | 512 |
| Time Zone | Australia/Perth |
| Device OS | Windows |

On this device image, it was found that of 47,803 files, 670 of them were related to the cases offence. This could have been images of illicit drugs that were downloaded as a result of accessing a webpage, PDF documents downloaded from websites that relate to the growing, selling and general information of illicit substance and the download of programs that could be used for suspicious activity.

|  |  |
| --- | --- |
| **Total files on device image** | **Incriminating content files** |
| 47,807 | 670 |
| 100% | 1.40% |

# Issue #1 - Can Content Related to the Offence Be Found in the Digital Forensic Image of the Volume of the Drive of the Suspect’s Computer?

The artifacts below are only a few examples of a large number of suspicious content found on the device. These artifacts include JPEG files, PNG files and PDF files that all relate to the offence of the case.

## Artifact #1

|  |  |  |
| --- | --- | --- |
| A plant with many leaves  Description automatically generated | Filename | 4.jpg |
| Location | /img\_drugs.E01/Users/shawn/Downloads/ |
| Size | 182071 |
| MIME type | Image/jpeg |
| File type | JPEG |
| Modified | 2021-03-25 09:20:57 AWST |
| Accessed | 2021-05-13 11:12:47 AWST |
| Created | 2021-05-13 11:12:47 AWST |
| MD5 | 4d212ac6538e9821c712fd88767d91d2 |
| Description | Image downloaded from webpage of anatomy of cannabis plant. Cannabis is illegal in Australia except for medical exemptions. |

## Artifact #2

|  |  |  |
| --- | --- | --- |
| A close-up of a white powder  Description automatically generated | Filename | cc2.jpg |
| Location | /img\_drugs.E01/Users/shawn/Downloads/ |
| Size | 9119 |
| MIME type | Image/jpeg |
| File type | JPEG |
| Modified | 2021-04-19 10:01:03 AWST |
| Accessed | 2021-05-13 11:12:47 AWST |
| Created | 2021-05-13 11:12:47 AWST |
| MD5 | Ae6941b2f7aa5cc38b9a15005297762 |
| Description | Image of white substance with items used to ingest the substance. Suspected substance is cocaine which is illegal. |

## Artifact #3

|  |  |  |
| --- | --- | --- |
|  | Filename | 2.jpg |
| Location | /img\_drugs.E01/Users/shawn/Downloads/ |
| Size | 78158 |
| MIME type | Image/jpeg |
| File type | JPEG |
| Modified | 2021-03-25 09:19:25 AWST |
| Accessed | 2021-05-13 11:12:47 AWST |
| Created | 2021-05-13 11:12:47 AWST |
| MD5 | 66bf4cd3df4bbddf1e92478ae0f755eb |
| Description | Disassembled cannabis plants. Cannabis is illegal without medical use. |

## Artifact #4

|  |  |  |
| --- | --- | --- |
| A close up of a cigarette  Description automatically generated | Filename | 5.jpg |
| Location | /img\_drugs.E01/Users/shawn/Downloads/ |
| Size | 107108 |
| MIME type | Image/jpeg |
| File type | JPEG |
| Modified | 2021-03-25 09:25:06 AWST |
| Accessed | 2021-05-13 11:12:47 AWST |
| Created | 2021-05-13 11:12:47 AWST |
| MD5 | 842a442a2f7ffc1ab765fc748053be23 |
| Description | Image of marijuana and its final products such as cookies, rolled up smokes and drinks. These products of cannabis are illegal. |

## Artifact #5

|  |  |  |
| --- | --- | --- |
|  | Filename | BC\_Logo\_30x30.png |
| Location | /img\_drugs.E01/Program Files/VeraCrypt/docs/html/en/ |
| Size | 4097 |
| MIME type | Image/png |
| File type | PNG |
| Modified | 2021-04-15 09:32:13 AWST |
| Accessed | 2021-05-13 13:12:08 AWST |
| Created | 2021-05-13 13:12:08 AWST |
| MD5 | 382eb591ff877480deade16f9abcf879 |
| Description | Image of bitcoin symbol downloaded from the VeraCrypt program. Shows intention of using cryptocurrency which relates to the case. |

## Artifact #6

|  |  |  |
| --- | --- | --- |
|  | Filename | Marijuana Grow Bible.pdf |
| Location | /img\_drugs.E01/Users/shawn/Downloads/ |
| Size | 1721732 |
| MIME type | Application/pdf |
| File type | PDF |
| Modified | 2021-03-25 09:40:18 AWST |
| Accessed | 2021-05-13 11:12:51 AWST |
| Created | 2021-05-13 11:12:51 AWST |
| MD5 | a780f8c9b2ee5415995546ea48006fbf |
| Description | PDF document describing the growth of marijuana. The growing of marijuana is illegal. |

Artefacts 1, 3, 4 and 6 all show a depiction of cannabis or marijuana. This links with the offence of the case as the suspect was found to have intentions that are related to drug use. Artefact 2 shows a depiction of cocaine which is another illicit drug that relates to the offence of the case. Meanwhile artefact 5 depicts bitcoin which was downloaded from VeraCrypt in order to manage and transfer cryptocurrency which also relates to the offence of the case.

# Issue #2 - If Illegal Content Related to the Offence Is Present, Can the Suspect Be Linked to It?

Here is a breakdown of what is known with regards to the relationship between the owner of the material and the material itself.

* It is John Hopkinson’s laptop that was seized and investigated
  + There are multiple resume’s from candidates applying for a financial position that the user owns on the laptop
  + There are also web searches with regards to financial positions and high paying jobs in the financial sector
  + John does work as a Senior Analyst at his company

However, the user that is used on the device image is known as Shawn. It is known that:

* Shawn has an email address of [skemp19951@gmail.com](mailto:skemp19951@gmail.com)
  + This email address is linked to his google account
    - This google account is linked with accessing this incriminating evidence.

# Issue #3 - Was the Content Accessed/Distributed Intentionally?

The intention of the user accessing the content that was accessed on the device image is listed below. The first table shows the bookmarks on the users web browser. This is often used in order to remember a web page for a later date or to potentially access it quicker than if the user was to type in the websites domain. As shown in this table, these bookmarks are related to the offence and the content that was found. Bookmarks are manually made by the user.

|  |  |  |
| --- | --- | --- |
| **Date/Time** | **Bookmarked Website** | **Domain** |
| 2021-03-24 07:47:04 AWST | What is the tor browser? | csoonline.com |
| 2021-03-24 09:16:37 AWST | Illicit drug prices and quantity discounts | sciencedirect.com |
| 2021-03-25 09:20:26 AWST | How to Grow Cannabis (Easy 10-Step Guide) | growweedeasy.com |
| 2021-03-25 09:21:04 AWST | The Different Parts Of A Marijuana & Cannabis Plant | weedmaps.com |
| 2021-03-25 09:23:06 AWST | Why Buy at the Dispensary When You Can Grow Cannabis at Home for Cheaper | leafly.com |
| 2021-03-25 09:23:55 AWST | How much does it cost to grow cannabis indoor for business use? | cannabusinessplans.com |
| 2021-03-25 09:27:16 AWST | Aussie Weed Prices | ponderingpot.com.au |

In this table is a few examples of search queries that the user made on Google Chrome.

|  |  |  |
| --- | --- | --- |
| **Date/Time** | **Search** | **Program Name** |
| 2021-03-22 09:16:46 AWST | “drugs” | Google Chrome |
| 2021-03-22 09:18:21 AWST | “popular drugs among youth” |
| 2021-03-22 09:20:21 AWST | “most common drugs among youth in australia” |
| 2021-03-22 09:26:12 AWST | “most expensive drugs” |
| 2021-03-22 09:27:26 AWST | “marijuana” |
| 2021-03-22 09:34:02 AWST | “cannabis benefits” |
| 2021-03-31 05:54:31 AWST | “How to Grow Cannabis” |
| 2021-04-08 08:11:20 AWST | “bitcoin price” |
| 2021-04-08 09:52:54 AWST | “lsd” |
| 2021-04-19 10:00:26 AWST | “cocaine” |

From these tables there is a clear similarity, which is that the majority of the content that was accessed above was done so between the 22nd of March 2021 and the 25th of March 2021.

# Issue #4 - How Many Files Were Present in the System?

The entirety of the device image had 47,803 files which includes images, videos, databases, html files, plain text, rich text and other executables. Of these 47,803 files 670 were found to have some sort of evidence that related to the offence of this case. Therefore, 1.40% of the device image contained incriminating evidence. Here is the breakdown of the 670 files that were suspected of having content related to the offence of the case.

The investigation found the following:

670 files of content related to cannabis, cocaine and cryptocurrency was found.

|  |  |  |
| --- | --- | --- |
| **File Type** | **Number of Files** | **% of files related to crime** |
| PNG | 39 | 5.82 |
| JPG | 618 | 92.24 |
| PDF | 5 | 0.75 |
| Other | 8 | 1.19 |

# Issue #5 - Was Any of the Installed or Previously Removed Software Used for the Alleged Crime?

|  |  |  |
| --- | --- | --- |
| **Software** | **Purpose** | **Date Accessed** |
| Tor Browser 10.0.12 Installer | Install Tor Browser in order to access dark web for criminal marketplace | 2021-03-24 07:47:50 AWST |
| TrueCrypt 7.2 | Used to encrypt files and hide the contents of files | 2021-03-29 09:43:34 AWST |
| VeraCrypt 1.24 | Used to encrypt files and hide the contents of files | 2021-04-15 09:30:16 AWST |
| CryptoTokenExtension 0.9.74 | Extension that is used to manage and transfer cryptocurrency | 2021-05-13 11:07:43 AWST |

# Running Sheet

|  |  |  |  |
| --- | --- | --- | --- |
| Date/Time | Event | Result | Duration |
| 16/09/2024 11:32 | Using HashCalc to verify integrity of filed.  A screenshot of a computer  Description automatically generated | Hashes align with original values.  This means the integrity of the device image files are good. | 26 minutes |
| 16/09/2024 12:05 | Open Autopsy 4.21.0 and opening Recent Cases > Assignment2 case | Case file opened | 3 minutes |
| 16/09/2024 12:08 | Use Autopsy 4.21.0 and navigate to the File Views > File Types > By Extension > Images to begin finding artefacts for Issue #1.  Add Notable tag to any suspicious looking images found that relate to the crime.  Continue through Autopsy 4.21.0 and navigate through the rest of the file extensions including Videos, Audio, Archives, Databases. | 670 files were tagged as notable to be able to look back and analyse. Majority of these were jpg image files that were related to marijuana, cocaine and cryptocurrency. | 1 hour and 45 minutes |
| 16/09/2024 13:54 | Extract some image files by right clicking on the chosen files and selecting Extract File.  Add to bookmark by right clicking the 5 files and going Add File Tag > Bookmark  Files will then be sent via email to be put as artifacts in report. | Files successfully extracted. Sent via email to be placed in report.  Issue #1. | 8 minutes |
| 16/09/2024 14:02 | On the left of screen in evidence tree click on Tags > Bookmark > File Tags to see bookmarked files.  Click on first file and bottom should show image. Navigate to File Metadata option in order to then enter values in artifacts. | Issue #1 | 15 minutes |
| 16/09/2024 14:17 | Back in Autopsy 4.21.0 go to File Views > File Types > By Extension and look through Documents and Executables to find more evidence.  Right click and Add File Tag > Notable Item when finding suspicious items for later analysis. | Found multiple pdfs, executables, chrome extensions, bookmarks. | 52 minutes |
| 16/09/2024 15:08 | Extract PDF file named Marijuana Grow Bible.pdf to be used as artifact.  Open PDF in online PDF viewer and take screenshot of front cover page by using Snipping Tool in Microsoft Windows environment.  Send screenshot via email to host OS to be placed in report. | Screenshot sent via email. Artifact #6 made and Issue #1 complete. | 9 minutes |
| 23/09/2024 12:42 | In Autopsy 4.21.0 go to Keyword Search in top right hand corner of application.  In search field enter “user” and untick Save search results. Click Search when completed.  Look through files and see any reoccurring names. | Shawn is listed as a user in file locations. This is the user for the device. | 17 minutes |
| 23/09/2024 13:00 | Keyword Search for “shawn” and click Search when completed.  Look through files and right click and Add File Tag > Notable Item on files related to a Shawn and a potential last name.  Note any email addresses, contacts, phone numbers and accounts under the name. | Shawn Kemp is the user of the device. Has multiple emails using parts of his name. Also has a google account in which the incriminating evidence is linked to.  This is added to Issue #2. | 53 minutes |
| 30/09/2024 14:12 | Open Autopsy 4.21.0 and in the evidence tree on the left of the screen go to Data Artifacts > Operating System Information.  Click on Source File Metadata and enter device image specifications into table under subsection of report called Summary. Also use Data Artifacts to find the Program Name of the Operating System used on this device. | Summary table created and information is entered into table.  Summary of investigation written before table. | 24 minutes |
| 30/09/2024 14:36 | On evidence tree go to Data Artifacts > Chromium Extensions.  Look through chrome extension files add Notable Item tag to anything suspicious. | CryptoTokenExtension found in Chromium Extensions.  Details and specification of file added to Issue #5. | 12 minutes |
| 30/09/2024 14:50 | Go to Data Artifacts > Run Programs in Autopsy 4.21.0.  Look through files of run programs and add any suspicious software to the table in Issue #5. | TrueCrypt.exe and VeraCrypt.exe added to Issue #5. Details of programs added to table. | 23 minutes |
| 7/10/2024 13:14 | Open Autopsy 4.21.0 and in the evidence tree on the left go to Data Artifacts > Web Bookmarks. Bookmarks from all browsers should appear and add Notable Item tag to any suspicious bookmarks.  Add suspicious bookmark details by clicking on Data Artifacts in the bottom of screen and then Source File Metadata for any other valuable information.  A screenshot of a computer  Description automatically generated | 6 bookmarks found of websites pertaining to the use, growth or selling of cannabis.  1 bookmark found of a website containing information about Tor Browser which is used to access dark web and underground marketplaces.  Details of bookmarks added to table in Issue #3 | 16 minutes |
| 7/10/2024 13:30 | Go back to Data Artifacts in the evidence tree and proceed to the Web Search listing.  Find suspicious searches and add the text entered into the search bar, the program used, and the date of the search. | Searches relating to offence of case found.  Details of each search added to table in Issue #3.  Searches and bookmarks show intent from the user and Issue #3 description is completed. | 43 minutes |
| 19/10/2024 9:23 | Open Autopsy 4.21.0 and in the evidence tree click on the small + symbol next to File Views in order to expand the tree. Then click the + symbol next to File Types and underneath that, press the + symbol next to:  By Extension  Documents  Executables  Numbers should show next to the file type and this represents the number of files in that category.  A screenshot of a computer  Description automatically generated | Completed and number of files shown next to the respective file types in Autopsy 4.21.0 | 2 minutes |
| 19/10/2024 9:25 | Open calculator application and add the number of files up in all file types from By Extension and Documents and Executables. This will give the total number of files in the data source. | Total number of files found were 47,803 files. | 4 minutes |
| 19/10/2024 9:29 | In evidence tree, go down to Tags > Notable Items.  This will include all the notable items found to be suspicious from earlier investigation. Read number next to Notable Item. | Total number of incriminating files was 670. | 2 minutes |
| 19/10/2024 9:31 | Open calculator and calculate percentage of files by dividing file type by total files.  Add percentages and number tallies to the table in Issue #4  A screenshot of a calculator  Description automatically generated | Issue #4 completed.  Summary completed. | 12 minutes |

# Timeline of Events

|  |  |  |  |
| --- | --- | --- | --- |
| **Date/Time** | **Description** | **Event** | **Analysis** |
| 2021-03-22 09:13:41 AWST | /Users/shawn/AppData/Local/Temp/chrome\_installer.log | \_C\_M | User downloads Google Chrome Installer on device that will later be used to access illicit content. |
| 2021-03-22 09:14:33 AWST | /Users/shan/AppData/Local/Google/Chrome/UserData/Default/Code Cache/js/43c643108770d4e1\_0 | \_C\_M | User successfully installs Google Chrome application that will be used for illicit purposes. |
| 2021-03-22 09:16:46 AWST | “drugs” – Google Search  Domain: google.com  Program Name: Google Chrome | Web Searches | Search for drugs. This relates to offence of case. |
| 2021-03-22 09:17:54 AWST | “drugs” – Google Search  Domain: google.com  Program Name: Google Chrome | Web Searches | Search for drugs. This relates to offence of case. |
| 2021-03-22 09:18:21 AWST | “popular drugs among youth” – Google Search  Domain: google.com  Program Name: Google Chrome | Web Searches | Search for popularity of drugs. This relates to offence of case. |
| 2021-03-22 09:18:51 AWST | “What Are the Top 10 Drugs Prescribed in the U.S.?” – Title  Domain: medicinenet.com  Program Name: Google Chrome | Web History Accessed | Website relating to drugs which is an offence of the case. |
| 2021-03-22 09:19:23 AWST | “most common drugs among youth” – Google Search  Domain: google.com  Program Name: Google Chrome | Web Searches | Search for popularity of drugs. This relates to offence of case. |
| 2021-03-22 09:19:41 AWST | “Drugs and Young People: MedicinePlus” – Title  Domain: medicineplus.gov  Program Name: Google Chrome | Web History Accessed | Website relating to drugs which is an offence of the case. |
| 2021-03-22 09:26:12 AWST | “most expensive drugs” – Google Search  Domain: google.com  Program Name: Google Chrome | Web Searches | Search for drugs. This relates to offence of case. |
| 2021-03-24 07:47:04 AWST | Title – “What is the Tor Browser? And how the dark web browser works”  Domain: csoonline.com  Program Name: Google Chrome | Web Bookmark | Bookmark of webpage that includes illicit content. Shows user intent. |
| 2021-03-24 07:47:50 AWST | Domain: [www.torproject.org](http://www.torproject.org)  Torbrowser-install-win64-10.0.12\_en-US.exe downloaded from the webste | Web Downloads | Download of tor browser installer from website. Tor browser used to access dark web for illicit purposes. |
| 2021-03-24 09:16:37 AWST | Title – “Illicit drug prices and quantity discounts”  Domain: sciencedirect.com  Program Name: Google Chrome | Web Bookmark | Bookmark of webpage that includes illicit content. Shows user intent. |
| 2021-03-24 09:18:44 - 54 AWST | Domain: gardenista.com  Cannabis-marijuana-plants-hoop-house-brian-shamblen-flickr-733x454.jpg  &  Cannabis-sativa-marijuana-plant-buds-weedporndaily-733x498.jpg | Web Downloads | Downloads of images from website that relates to the offence of the case. |
| 2021-03-25 09:20:26 AWST | How to Grow Cannabis (Easy 10-Step Guide)  Domain: growweedeasy.com | Web Bookmark | Bookmark of webpage that includes illicit content. Shows user intent.  Refer to artifact #3 |
| 2021-03-25 09:21:04 AWST | The Different Parts Of A Marijuana & Cannabis Plant  Domain: weedmaps.com | Web Bookmark | Bookmark of webpage that includes illicit content. Shows user intent.  Refer to artifact #1 |
| 2021-03-25 09:23:06 AWST | Why Buy at the Dispensary When You Can Grow Cannabis at Home for Cheaper  Domain: leafly.com | Web Bookmark | Bookmark of webpage that includes illicit content. Shows user intent.  Refer to artifact #4 |
| 2021-03-25 09:23:55 AWST | How much does it cost to grow cannabis indoor for business use?  Domain: cannabusinessplans.com | Web Bookmark | Bookmark of webpage that includes illicit content. Shows user intent. |
| 2021-03-25 09:27:16 AWST | Aussie Weed Prices  Domain: ponderingpot.com.au | Web Bookmark | Bookmark of webpage that includes illicit content. Shows user intent. |
| 2021-03-25 09:39:57 AWST | Domain: ongardening.com  Marijuana-The-Ultimate-Organic-Guide.pdf downloaded from webpage | Web Download | Shows intention of learning about illicit drug. |
| 2021-03-25 09:40:16 AWST | Domain: calgarycmmc.com  Marijuana Grow Bible.pdf | Web Download | Shows intention of learning about illicit drug. Shows intention of growing illicit drug.  Refer to Artifact #6 |
| 2021-03-25 09:40:30 AWST | Domain: marijuanaplantsonline.com  How-to-grow-elite-marijuana.pdf | Web Download | Shows intention of learning about illicit drug. Shows intention of growing illicit drug. |
| 2021-03-25 09:40:43 AWST | Domain: plantgrower.org  Cannabis\_cultivation17\_ultimate.pdf | Web Download | Shows intention of learning about illicit drug. Shows intention of growing illicit drug and cultivating. |
| 2021-03-29 09:43:34 AWST | Domain: sourceforge.net  TrueCrypt-7.2.exe downloaded. Program is used for encrypting files | Web Download | Shows intention for hiding material by downloading file encryption software. |
| 2021-03-29 09:43:42 -10:06:56 AWST | TRUECRYPT-7.2.exe  /Users/shawn/Downloads | Program Run | Shows program has been run and activities relating to the case offence occurring at this time. |
| 2021-04-14 13:57:20 AWST | TRUECRYPT-7.2.exe  /Users/shawn/Downloads | Program Run | Shows program has been run and activities relating to the case offence occurring at this time. |
| 2021-04-15 09:30:16 AWST | Domain: launchpadlibrarian.net  VeraCryptSetup201.24-Update7.exe downloaded. Program is used for encryption of files. | Web Download | Shows intention for hiding material by downloading file encryption software. |
| 2021-04-15 09:38:00 AWST | VERACRYPT.exe  /Program Files/Veracrypt | Program Run | Shows program has been run and activities relating to the case offence occurring at this time.  Refer to artifact #5 |
| 2021-04-19 10:00:26 AWST | “cocaine” – Google Search  Domain: google.com  Program Name: Google Chrome | Web Searches | Search for drugs. This relates to offence of case.  Refer to artifact #2 |
| 2021-05-13 11:07:43 AWST | Preferences changed for CryptoTokenExtension 0.9.74  Program Name: Google Chrome | Chromium Extensions | Using cryptocurrency extension/application implying use of cryptocurrency. |