



EDITH COWEN UNIVERSITY

FORENSIC INVESTIGATION REPORT

Uncovering Digital Evidence

ACCESS: AUTHORIZED PERSONAL ONLY

CSG2305 .3 – Computer Forensics
NAME: Tanushka ELVITIGALA
SID: 10663914

Lecturer: Roshan Priyashantha

DISCLAIMER

This report and its accompanying evidence will be securely stored and accessible only to authorized personnel. Readers are warned that they may be exposed to sensitive, offensive, or objectionable material. Supplemental storage devices contain similar content. Clicking on links within this document may open content that is offensive, objectionable, or illegal. Unauthorized access to this file may result in severe legal consequences, including fines or imprisonment, as per applicable laws.

CONFIDENTIAL

Table of Contents

1.0 Executive Summary	4
2.0 Time Zone Differences	6
2.1 Importance of Time Zone Differences	6
3.0 Issue #01: Content Related to the Offence	7
4.0 Issue #02: Linking John to the Illegal Content	11
5.0 Issue #03: Intentional Access/Distribution of Content	14
6.0 Issue #4: File Analysis	17
7.0 Issue #5: Software Usage	20
APPENDIX A	23
Appendix B.....	25

1.0 Executive Summary

This investigation was initiated to uncover potential illegal activities involving drugs and firearms on a company-issued laptop used by John Hopkinson, a Senior Analyst at the company. The inquiry began following a complaint from John regarding an antivirus signature updating error. During the attempted update, an IT technician discovered digital content suggestive of illegal activities.

To maintain the integrity of the evidence, the hash values of the original forensic image were first calculated. A verified copy of the image was then created, ensuring the original remained untouched and stored in a secure environment. This meticulous approach ensured that the evidence was preserved without any alterations.

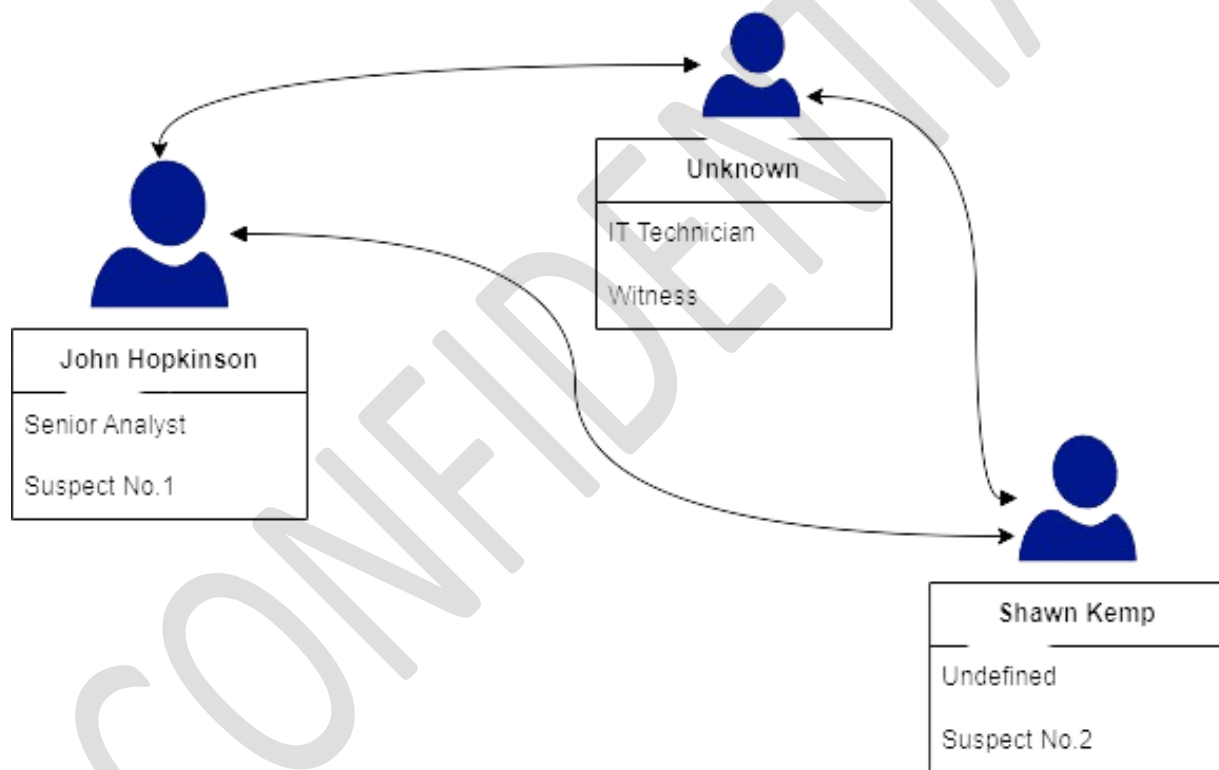


Figure 1: Involvements

Key individuals identified in this case include John Hopkinson, the IT technician who discovered the suspicious content, and suspect Shawn Kemp. The investigation determined that while John was attempting to update the antivirus software, the illicit content was discovered by the IT technician.

Using a suite of advanced forensic tools including Autopsy 4.21.0, Access Data FTK Imager, Registry Viewer, DB Browser (SQLite), OSForensics, and IrfanView 64, a thorough examination of the laptop's contents was conducted. Each tool was selected for its specific strengths in analyzing different aspects of the data,

Autopsy 4.21.0	For overall forensic analysis and timeline reconstruction.
Access Data FTK Imager	To image and view the data.
Registry Viewer	For examining Windows Registry entries.
DB Browser (SQLite)	To inspect SQLite database files.
OSForensics	For comprehensive system analysis and file recovery.
IrfanView 64	For viewing image files.

Table 1: Tools

The investigation revealed significant evidence of illegal drug-related activities, including,

- ❖ Incriminating images and documents.
- ❖ Suspicious web cookies and browsing history.
- ❖ Bookmarked websites and favicons indicating interest in drug-related content.
- ❖ Specific software installations related to anonymous communication and transactions.
- ❖ Web searches and bookmarks for drug purchasing and sales.
- ❖ Use of anonymous payment methods, such as cryptocurrencies, to facilitate illegal transactions.

The forensic process involved a detailed analysis and correlation of digital artifacts. Each piece of evidence was meticulously catalogued and examined to determine its relevance and significance. The findings indicate that another user on the laptop was engaging in drug-related activities. Although there is no direct evidence linking John to these activities, as the laptop owner, he remains responsible for its usage.

The outcome of this investigation pointed to Shawn Kemp as an individual connected to the illegal activities. Detailed analysis and evidence link this individual to the discovered content. This report provides a comprehensive overview of the evidence, methodologies, and conclusions drawn from the forensic analysis, underscoring the importance of vigilance and security in digital environments.

the investigation confirmed the presence of illegal drug-related content on the laptop. While John Hopkinson was not directly linked to the illegal activities, his responsibility for the laptop necessitates further scrutiny. The evidence points to Shawn Kemp as the main suspect, providing a solid foundation for any subsequent legal actions.

2.0 Time Zone Differences

This forensic investigation accounts for significant time zone differences between the case evidence and the analysis system. John Hopkinson's laptop, where the alleged illegal activities occurred, operates in the time zone of Coordinated Universal Time (UTC) + 8, as does the forensic analysis system.

2.1 Importance of Time Zone Differences

Understanding and accounting for these time zone disparities is crucial for accurate interpretation of timestamps associated with the evidence. This ensures precise event correlation, user activity analysis, and conversion accuracy, ultimately maintaining the integrity and reliability of the forensic investigation.

Ex:

For instance, an event timestamped as 2024-05-15 14:30 in UTC would equate to the same time in the forensic analysis system.

3.0 Issue #01: Content Related to the Offence

Our investigation begins with a detailed analysis of digital content extracted from John Hopkinson's work laptop. Allegations of illegal drug and firearm trafficking prompt us to meticulously examine all data for any materials indicating such activities. We aim to identify and analyze documents, media files, or communications that may directly relate to the alleged offenses. Each piece of content will be carefully scrutinized to determine its relevance and significance to the investigation, shedding light on the presence and extent of illicit activities within the digital domain.

PDFs:

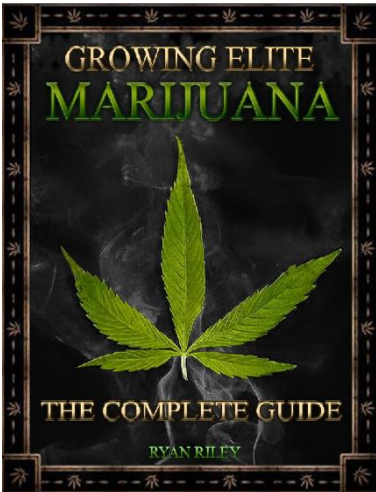
 <p>Figure 2: Growing Elite Marijuana</p> <p>Start Sector: 34,775,168</p>	Name	how-to-grow-elite-marijuana.pdf
	Type	File System
	MIME Type	application/pdf
	Size	38569182
	File Name Allocation	Allocated
	Modified:	2021-03-25 09:40:33 AWST
	Accessed:	2021-05-13 11:12:49 AWST
	Created:	2021-05-13 11:12:49 AWST
	Changed:	2021-04-09 11:26:28 AWST
	MD5:	d64aed98330277fcf2afbb1f5a4af9cc
	SHA-256:	b1e96a9571d478b98c26b9f177428b40a0ac66b3b1c3d5c e1e7d899be518f3d5
	Artifact ID	-9223372036854775732
	Associated Artifact	-9223372036854775733
	Source File Path	/img_drugs.E01/Users/shawn/Downloads/how-to-grow- elite-marijuana.pdf

Table 2: Evidence 1

The PDF file "how-to-grow-elite-marijuana.pdf" found in user Shawn's Downloads folder on John Hopkinson's laptop potentially indicates involvement in illegal drug cultivation activities. Created and accessed on May 13, 2021, the file's metadata suggests recent interest by Shawn. Timestamps and hash values ensure the file's integrity, crucial for forensic analysis linking Shawn to illicit behavior. Additionally, the presence of another downloaded marijuana-related PDF and evidence of an email sent to the author of the "I Love Marijuana" book further implicates Shawn in activities related to drug cultivation and distribution.

Score:	Likely Notable
Type:	Keyword Hits
Configuration:	Email Addresses
Conclusion:	
Keyword:	robert@ilovegrowingmarijuana.com
Keyword Preview:	de, let me know on «robert@ilovegrowingmarijuana.com». i'm always looking

Table 3: Evidence 3

The presence of the email address "robert@ilovegrowingmarijuana.com" in the email content suggests potential involvement in activities related to marijuana cultivation.

IMAGES:

 <p>Figure 3: cocaine</p> <p>Star Sector: 34,768,456</p>	Name:	/img_drugs.E01/Users/shawn/Downloads/cc2.jpg
	Type:	File System
	MIME Type:	image/jpeg
	Size:	9119
	File Name Allocation:	Allocated
	Metadata Allocation:	Allocated
	Modified:	2021-04-19 10:01:03 AWST
	Accessed:	2021-05-13 11:12:47 AWST
	Created:	2021-05-13 11:12:47 AWST
	Changed:	2021-04-19 10:01:03 AWST
	MD5:	ae6941b2f7aa5cc738b9a15005297762
	SHA-256:	02b92ebec15afbb6d2126c97707275 332383fbbd30361934188ca6536db215a5
	Hash Lookup Results:	UNKNOWN
	Internal ID:	30806

Table 4: Evidence 4

The forensic analysis of image files on John Hopkinson's laptop revealed significant findings. Specifically, 603 images related to drugs were discovered, sourced from the PDF file "how-to-grow-elite-marijuana.pdf" and other sources. Among these, 10 downloaded images directly correlated with marijuana and drug use. This evidence strongly suggests illicit activities, as the images depict substances, paraphernalia, and activities associated with drug cultivation and use. Furthermore, the inclusion of Shawn in the analysis underscores the potential involvement of specific individuals in these illegal activities. Further examination of these images may provide valuable insights into the extent and nature of Shawn's participation in illegal drug activities.

Associated Artifact	-9223372036854775786
Source File Path	/img_drugs.E01/Users/shawn/Downloads/cc2.jpg
Artifact ID	-9223372036854775785

Table 5: Evidence 4 Artifacts

BOOKMARKS:

https://www.csoonline.com/article/3287653/what-is-the-to... https://www.sciencedirect.com/science/article/pii/S095539... https://www.growweedeasy.com/10-step-cannabis-grow-... https://weedmaps.com/learn/the-plant/parts-of-cannabis-... https://www.leafly.com/news/cannabis-101/costs-of-cann... https://cannabusinessplans.com/much-cost-grow-cannabis... https://www.ponderingpot.com.au/misc/australian-weed-prices/	Name:	/img_drugs.E01/Users/shawn/AppData/Local/Google/Chrome/User Data/Default/Bookmarks
	Type:	File System
	MIME Type:	text/plain
	Size:	7390
	File Name Allocation:	Allocated
	Metadata Allocation:	Allocated
	Modified:	2021-03-25 13:07:29 AWST
	Accessed:	2021-05-13 11:07:42 AWST
	Created:	2021-05-13 11:07:42 AWST
	Changed:	2021-03-25 13:07:29 AWST
	MD5:	bf007e2be02564f41a15311336cc8e0f
	SHA-256:	4e16218187d548047ea9b8b5a6c5dfb9a69a72da912c12e4ace9b4c79dfd1aca
	Hash Lookup Results:	UNKNOWN
	Internal ID:	2779
	Name:	/img_drugs.E01/Users/shawn/AppData/Local/Google/Chrome/User Data/Default/Bookmarks
	Type:	File System

Table 6: Evidence 5

The presence of bookmarks related to drugs and selling platforms strongly suggests an active involvement or interest in illegal drug activities. Such bookmarks may include websites facilitating the sale and purchase of illicit substances, as well as forums or communities discussing drug-related topics.

Bookmark Details

Title: Illicit drug prices and quantity discounts: A comparison between a cryptomarket, social media, and police data - ScienceDirect
Date Created: 2021-03-24 09:16:37 AWST
Domain: sciencedirect.com
URL: https://www.sciencedirect.com/science/article/pii/S0955395920303078
Program Name: Google Chrome

Figure 4: Evidence 6

Illicit drug prices and quantity discounts: A Comparison between a cryptomarket, social media, and police data – ScienceDirect

This evidence provides further support for the allegations of drug trafficking and indicates a deliberate effort to engage with such activities. Further investigation into the contents of these bookmarks may reveal valuable insights into the individual's participation in illegal drug-related endeavors.

Local State			Default	102181526126579431019	NO_HOSTED_DOMAIN	Shawn
-------------	--	--	---------	-----------------------	------------------	-------

Figure 5: Logging

Person 1	skemp19951@gmail.com	Google Chrome	drugs.E01
----------	----------------------	---------------	-----------

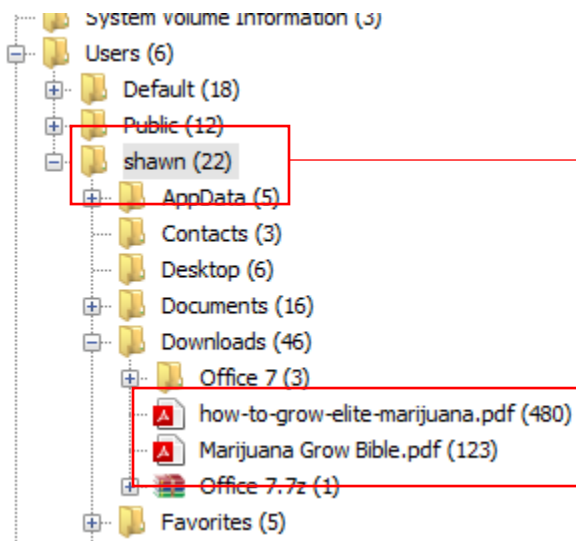
The association of Shawn's usage with Google Chrome suggests a direct link between Shawn and the bookmarks related to drugs and selling platforms. As the primary user of the browser, Shawn's bookmarks likely reflect his personal interests and activities online. Therefore, the discovery of drug-related bookmarks implicates Shawn in the deliberate engagement with platforms facilitating drug trafficking and sales. This strengthens the case against Shawn's involvement in illegal drug activities and underscores the significance of his role in the investigation. Further scrutiny of these bookmarks is crucial for determining Shawn's level of participation in illicit drug-related endeavors.

WEB SEARCHES:

The presence of drug-related web searches in Shawn's browsing history reinforces the notion of his active engagement with illegal drug activities. As the primary user of Google Chrome on the device, Shawn's search history directly reflects his online behavior and interests. The discovery of such searches alongside the drug-related bookmarks strengthens the case against Shawn, suggesting a deliberate and sustained involvement in illicit drug endeavors. Further examination of these web searches may uncover additional insights into Shawn's role and level of participation in drug-related activities.

4.0 Issue #02: Linking John to the Illegal Content

To establish a connection between John Hopkinson and the illegal content found on his laptop, it is imperative to delve into the digital footprint left behind by user activity. Examination of user accounts, file ownership, and access logs will be pivotal in determining the extent of John's involvement with the illicit material. By meticulously analyzing the metadata associated with the files, as well as tracking user interactions with the content, we aim to uncover any direct or indirect associations between John and the illegal activities documented on his device.



Source File Path	/img_drugs.E01/Users/shawn/Downloads/Marijuana Grow Bible.pdf
------------------	---

By analyzing the evidence, it becomes evident that the user named Shawn is associated with the marijuana-related PDF files found on John Hopkinson's laptop. Further examination of other non-suspicious data files reveals that the user's full name is Shawn Kemp. This information helps in linking Shawn Kemp to the illegal content, suggesting that he is the primary individual engaging with these files. Through this analysis, we can establish a clearer connection between the user and the illicit activities documented on the device.

```
{
  "displayName": "Shawn Kemp",
  "givenName": "Shawn",
  "familyName": "Kemp",
  "displayNameLastFirst": "Kemp, Shawn",
  "unstructuredName": "Shawn Kemp"
}
```

Figure 7: Evidence 8

Analysis reveals that the user named Shawn, identified as Shawn Kemp from the office, is linked to the marijuana-related PDF files on John Hopkinson's laptop. This connection suggests Shawn Kemp's primary involvement with the illegal content found on the device.

Analysis reveals that the user named Shawn, identified as Shawn Kemp from the office, is linked to the drug-related image files in Shawn's folder on John Hopkinson's laptop. This connection suggests Shawn Kemp's primary involvement with the illegal content found on the device.

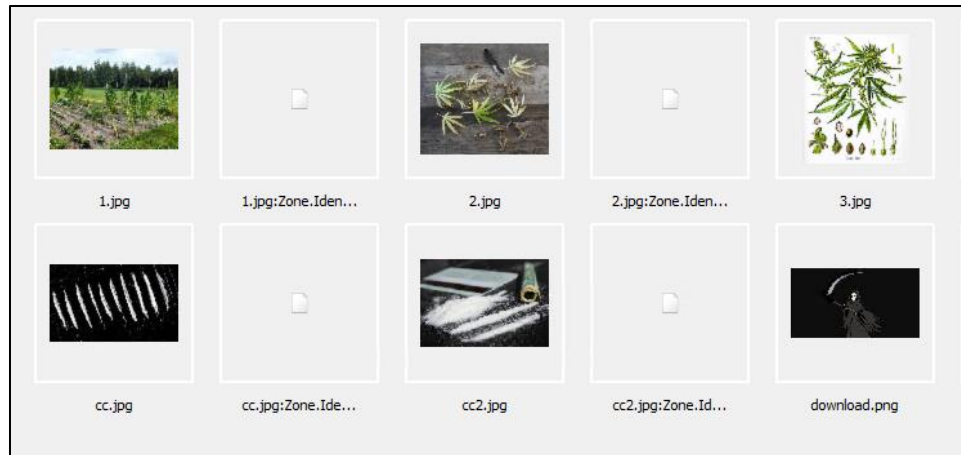


Figure 8: Evidence 9

Analysis reveals that the user named Shawn, identified as Shawn Kemp from the office, is linked to the drug-related image files found in the `img_drugs.E01/Users/shawn/Downloads/` folder on John Hopkinson's laptop.

History	0	C:\Users\shawn\Downloads\how-to-grow-elite-marijuana.pdf
History		C:\Users\shawn\Downloads\download.png
History	2	C:\Users\shawn\Downloads\download.png
History	1	C:\Users\shawn\Downloads\download.png
History	2	C:\Users\shawn\Downloads\cc2.jpg
History	2	C:\Users\shawn\Downloads\cc.jpg

Figure 9: Evidence 10

ow-to-...	2021-03-25 09:40:30 AWST	marijuanaplantsonline.com	Default	Google Chrome
	2021-04-07 13:34:25 AWST		Default	Google Chrome
7e7&a...	2021-04-07 13:34:25 AWST	google.com	Default	Google Chrome
achme...	2021-04-07 13:34:25 AWST	googleusercontent.com	Default	Google Chrome
ANd9G...	2021-04-19 10:00:59 AWST	gstatic.com	Default	Google Chrome
ANd9G...	2021-04-19 10:00:43 AWST	gstatic.com	Default	Google Chrome
5169/...	2021-03-25 09:40:43 AWST	plantgrower.org	Default	Google Chrome
019/0	2021-03-25 09:18:54 AWST	gardenista.com	Default	Google Chrome

Further details indicate these files were downloaded by someone using the default login. Figure 4 shows that the default Google Chrome user is Shawn, and bookmarks related to drug-selling platforms further support this. By analyzing this information, it is evident that the illegal content is linked to Shawn Kemp.

Moreover, examination of cookies unveils Shawn's utilization of PayPal, implying possible participation in distributing or procuring illicit substances via PayPal transactions. Additionally, his search history indicates inquiries about Bitcoin transactions, signaling an inclination towards conducting anonymous transactions. These revelations bolster the association between Shawn and illegal activities, reinforcing the notion of his involvement in drug-related transactions facilitated by digital payment methods.




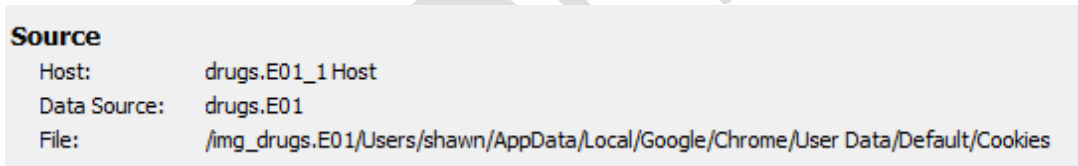
	Cookies		1	.paypal.com	2021-04-29 10:31:21 AWST
	Cookies		1	.paypal.com	2021-04-29 10:31:21 AWST
	Cookies		1	.paypal.com	2021-04-29 10:31:21 AWST
	Cookies		1	.paypal.com	2021-04-29 10:31:21 AWST
	Cookies		1	.paypal.com	2021-04-29 10:31:21 AWST

Figure 10: Evidence 11

the discovery of PayPal cookies within Google Chrome corroborates Shawn's involvement in illicit transactions. This evidence, coupled with data from the previous analysis, solidifies the connection between Shawn and illegal activities. The presence of Shawn's involvement is further supported by Figure, which provides visual confirmation of his association with the identified cookies.



Source	
Host:	drugs.E01_1 Host
Data Source:	drugs.E01
File:	/img_drugs.E01/Users/shawn/AppData/Local/Google/Chrome/User Data/Default/Cookies

Figure 11: Evidence 12

All the evidence presented strongly points to Shawn Kemp's involvement in the illegal activities, with no direct link established between John Hopkinson and the illicit content. However, as the primary user of the laptop, John would have had access to Shawn's bookmarks and the other images stored on the device. While this does not directly implicate John in the illegal activities, it suggests that he could have been aware of the content present on the laptop.

5.0 Issue #03: Intentional Access/Distribution of Content

Our forensic investigation focuses on understanding whether Shawn Kemp purposefully accessed or distributed the illicit content found on John Hopkinson's laptop. We meticulously examine digital evidence to determine Shawn's intentions. By analyzing access logs, timestamps, and user accounts linked to Shawn Kemp, we aim to clarify his actions. While considering external factors like third-party intervention or malware, our main goal is to find evidence supporting Shawn's intentional involvement in accessing or distributing the illicit content.

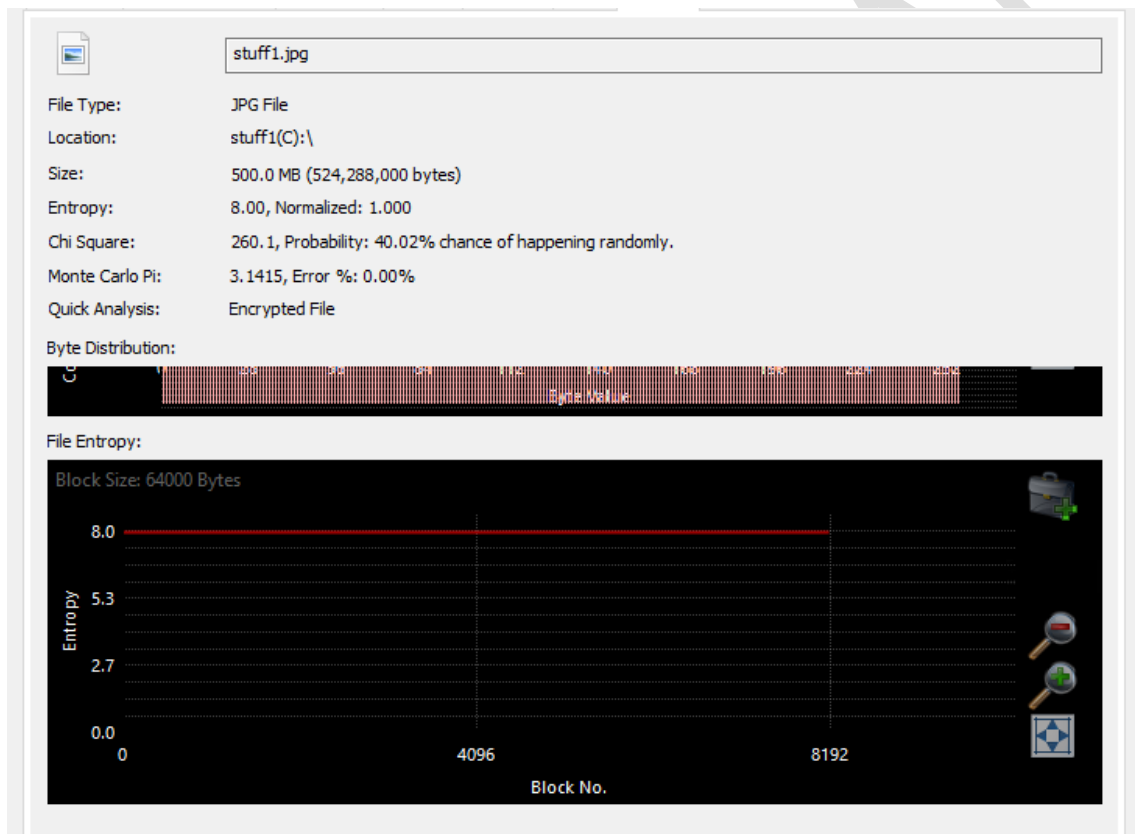


Figure 12:Evidence 13

Upon scrutinizing Shawn Kemp's Download folder, we encountered a JPG file named "stuff1" exhibiting anomalous characteristics distinct from typical JPG files. Unlike conventional JPGs, "stuff1" surpasses average sizes and showcases encryption, resulting in an entropy exceeding 7. These deviations raise red flags, suggesting the potential presence of malware. Further analysis into this file is warranted to ascertain its nature and any associated risks it may pose to the system.

Upon further examination of the downloads and browsing history patterns, it becomes evident that the anomalous file "stuff1" is unlikely to be a result of malware. Analysis reveals a consistent pattern predating the download of the suspected malware, with drug-related content already present in the files. Multiple search histories, numerous image files, and additional activities like downloading the Tor browser indicate deliberate and purposeful actions. The presence of two installed browsers further supports the notion of intentional behavior rather than accidental or malware-induced activity. These findings strongly suggest that Shawn Kemp's actions were deliberate and planned rather than the result of inadvertent or malicious causes.

	Bookmarks	2	https://www.csoonline.com/article/3287653/what-is-the-to...
---	-----------	---	---

Figure 13: Evidence 14

Bookmark Details

Title: What is the Tor Browser? And how the dark web browser works | CSO Online
Date Created: 2021-03-24 07:47:04 AWST

Based on the evidence gathered, it is evident that Shawn Kemp is the likely individual behind the intentional access and distribution of illicit content. His attempt to connect to the dark web using the Tor browser, coupled with the pre-installed Tor browser found during the investigation, strongly implicates him in illicit online activities. This aligns with previous findings indicating deliberate engagement with drug-related content and purposeful actions such as multiple search histories and downloads. The presence of the Tor browser further solidifies Shawn's involvement, indicating a deliberate effort to conceal online activities and access illicit platforms.





	torbrowser-install-win64-10.0.12_en-US (1).exe		1
	torbrowser-install-win64-10.0.12_en-US.exe		1

Figure 14: Evidence 15

The inability of malware to download and execute software or applications points to user-initiated actions or potential third-party involvement with access to the machine. Given this context, the installation of the Tor browser on the system suggests a lack of malware involvement in accessing drug-related content. Instead, it implies deliberate actions either by the user or an individual with access to the machine. The presence of the Tor browser reinforces the notion that the exploration of illicit content and attempts to access the dark web were intentional, rather than the result of malware interference.

Consideration of third-party interaction raises significant doubts regarding their involvement in this scenario. The presence of beginner-level searches such as "how the dark web browser works" and related PDFs contradicts the notion of an external actor orchestrating these actions. Furthermore, if a third party were responsible, the illicit files and activities would likely implicate both Shawn and John. However, the evidence primarily points to Shawn's deliberate engagement with the content, suggesting a personal connection to the activities observed on the system. Thus, the likelihood of third-party involvement appears minimal in light of the specific nature and pattern of actions undertaken.

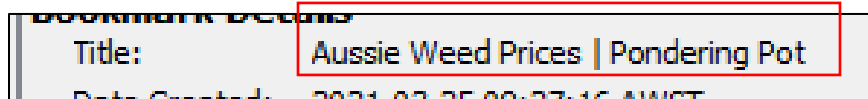


Figure 15: Evidence 16

The evidence strongly suggests that Shawn Kemp's intentions extend beyond mere exploration of illicit content; rather, they point towards active participation in the cultivation and distribution of drugs. The discovery of searches related to purchasing seeds and growing marijuana, coupled with Shawn's attempts to access the dark web for procurement, underscores his direct involvement in these activities. This level of engagement aligns closely with the profile of an individual seeking to buy and sell drugs independently. Moreover, the absence of evidence implicating a third party further supports the conclusion that Shawn Kemp is the primary actor behind these actions. Therefore, the cumulative evidence not only implicates Shawn but also lends credence to the assertion that no third-party involvement exists in this context.

Furthermore, Figure 8 in the web history provides compelling evidence linking Shawn Kemp to the illicit activities under investigation. An examination of the web history reveals details indicating Shawn's involvement, corroborated by additional evidence confirming his status as an employee. Notably, a document identified as the company's employee motivational session guide bears Shawn's authorship, further solidifying his connection to the case. This finding underscores Shawn's direct involvement in accessing and possibly disseminating illicit content, reinforcing the conclusion that he is a central figure in the investigation.

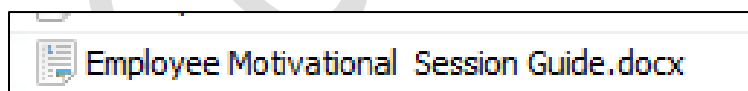
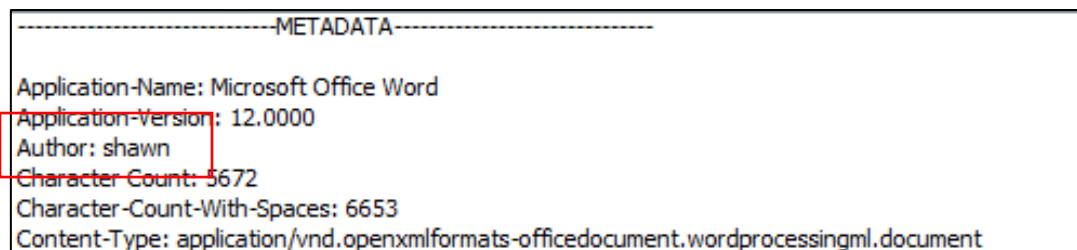


Figure 16: Evidence 17



6.0 Issue #4: File Analysis

Investigating the files stored on John Hopkinson's laptop is essential for uncovering potential illegal activities. We'll carefully examine various types of files, such as documents, images, and applications, to understand their role in the investigation. Our analysis will focus on identifying any suspicious patterns or content that could be linked to illegal behavior. By thoroughly assessing the composition and distribution of files, we aim to provide valuable insights into the nature and extent of the alleged offenses.

File Type	Count	Purpose
Images	9779	Graphic files containing visual content
Videos	387	Multimedia files containing video content
Audio	303	Sound files containing audio content
Databases	93	Structured data storage files
HTML	2004	Web page files written in HTML format
Office Documents	45	Documents created using office software
PDF	21	Portable Document Format files
Plain Text	396	Unformatted text files
Rich Text	1204	Text files with formatting
Executable Files	4414	Files capable of being executed as programs
DLL Files	29029	Dynamic Link Library files used by programs
Batch Files	10	Scripts containing commands to be executed
Command Files	18	Files containing command line instructions
COM Files	43	Component Object Model files

Table 7:File Analysis with purpose

Throughout the forensic examination, we delved into a variety of file types, uncovering 13 distinct categories. These encompassed everything from images and videos to crucial data relevant to our investigation. Each category provided essential insights into the unfolding events. Multimedia files, like videos and images, presented visual evidence, while databases offered a glimpse into how information was organized. Documents, such as emails and text files, revealed digital conversations and strategic plans. Additionally, we scrutinized potentially harmful files like executables and DLLs, requiring careful analysis. By meticulously examining these diverse file types, we pieced together a comprehensive understanding of the digital landscape at the heart of the investigation.

File Type	Count	Percentage
Images	9779	6.27%
Videos	387	0%
Audio	303	0%
Databases	93	0%
HTML	2004	0%
Office Documents	45	0%
PDF	21	19.04%
Plain Text	396	15.90%
Rich Text	1204	0%
Executable Files	4414	0.45%
DLL Files	29029	0%
Batch Files	10	0%
Command Files	18	0%
COM Files	43	0%

Table 8: File Analysis with Percentage

Despite the file types examined, data artifacts such as Chromium Extensions provided a wealth of additional information. These artifacts offered deeper insights into user behavior and activities, enhancing the overall understanding of the case. By combining traditional file analysis with the examination of these artifacts, a more comprehensive picture of the digital environment and the actions of the user emerged.

CONFIDENTIAL

7.0 Issue #5: Software Usage

In this section, the focus will be on analyzing the various software applications identified during the forensic investigation. Understanding the types of software used, their purpose, and the frequency of their usage can provide significant insights into user behavior, potential intent, and any unauthorized activities. This analysis will also help determine whether the software applications were utilized for legitimate purposes or for facilitating illicit activities.

The following executable files were found in Shawn's Downloads folder. Let's investigate each file.

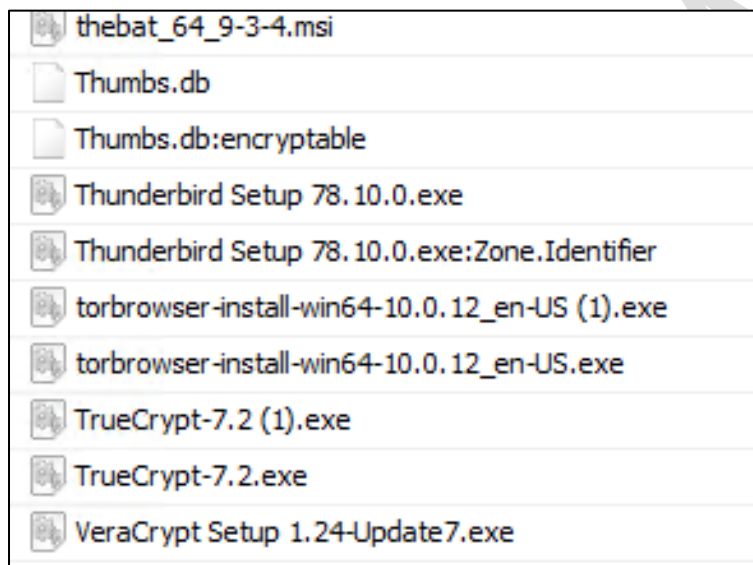


Figure 17: Software's

Thebat 64 9-3-4.msi

The presence of this installer suggests that an email client was potentially set up on John's laptop. The Bat! is known for its robust email management features, including encryption and advanced filtering. If installed and used, this software could impact John's laptop in several ways:

- ❖ **Privacy and Security:** The Bat! supports encrypted email communication, which could be used to send or receive sensitive or illicit information securely.
- ❖ **Email Activity:** It might indicate that the user (Shawn) was managing multiple email accounts or handling a large volume of emails, which could be relevant to the investigation if these emails were related to illegal activities.
- ❖ **System Performance:** The installation and running of additional software can impact the system performance, taking up resources like CPU, memory, and disk space.

Thunderbird Setup 78.10.0.exe

The installation of Thunderbird on John's laptop could have several implications:

- ❖ **Email Management:** Thunderbird is a powerful email client that supports multiple email accounts, message filtering, and advanced search options. Its installation might indicate that the user (Shawn) was organizing and managing emails, which could be pertinent if these emails were linked to illegal activities.
- ❖ **Privacy and Security:** Thunderbird supports encryption and secure email communications through extensions like Enigmail, which could be used for secure correspondence. This might suggest attempts to protect email content from being easily intercepted or read.
- ❖ **System Performance:** Running an additional email client could use system resources such as CPU, memory, and disk space, potentially impacting the laptop's performance.
- ❖ **Digital Footprint:** The use of Thunderbird leaves behind logs and data files that can provide insights into email activity, contacts, and communications. Investigating these logs could reveal more about the nature of the user's email interactions.

Visit Details	
Title:	Sign in – Google accounts
Username:	Default
Date Accessed:	2021-03-19 09:19:53 AWST
Domain:	google.com
URL:	https://accounts.google.com/signin/chrome/sync?ssp=1&continue=https%3A%2F%2Fwww.google.com%2F
Referrer URL:	https://accounts.google.com/signin/chrome/sync?ssp=1&continue=https%3A%2F%2Fwww.google.com%2F
Program Name:	Google Chrome

Figure 18:Thunderbird Visit Details

Tor Browser

The installation of the Tor Browser on John's laptop could have several implications:

- ❖ **Anonymity and Privacy:** The primary purpose of the Tor Browser is to enable anonymous browsing. Its presence suggests that the user (Shawn) might have been attempting to hide their online activities, which could include visiting websites and services that are not easily traceable through conventional browsers.
- ❖ **Access to Dark Web:** The Tor Browser is often used to access the dark web, a part of the internet that is not indexed by traditional search engines and is commonly associated with illegal activities such as drug trafficking, illegal trade, and other illicit transactions. Investigating browsing history and related artifacts could reveal visits to hidden services and marketplaces.
- ❖ **Evasion of Surveillance:** The use of Tor indicates an attempt to evade surveillance and tracking by ISPs, government agencies, and other entities. This could be significant if the user was involved in activities they wished to conceal from authorities.

- ❖ **System Performance and Security:** The Tor Browser, while enhancing privacy, could impact system performance due to the additional encryption and routing processes. It also introduces the risk of downloading potentially harmful content from the dark web, which could compromise the security of John's laptop.
- ❖ **Digital Footprint:** The Tor Browser leaves behind certain logs and artifacts that could be analyzed to understand the user's behavior and intent. This might include browser history, bookmarks, and session data stored within the Tor Browser's directory.

TrueCrypt-7.2.exe

The presence of TrueCrypt 7.2.exe on John's laptop could have several implications:

Data Encryption: TrueCrypt enables users to create encrypted volumes where sensitive data can be stored securely. The installation of TrueCrypt suggests that the user (Shawn) may have been interested in securing specific files or partitions on the laptop.

Protection Against Unauthorized Access: By encrypting data using TrueCrypt, the user can protect it from unauthorized access, even if the laptop is lost, stolen, or accessed by malicious actors. This could indicate that Shawn was concerned about the confidentiality and integrity of certain files or information.

Concealing Sensitive Information: TrueCrypt's ability to create hidden volumes allows users to conceal sensitive information within encrypted containers. This feature could be used to hide illicit activities, such as storing incriminating evidence or confidential documents related to illegal operations.

Forensic Challenges: TrueCrypt presents forensic challenges due to its strong encryption and plausible deniability features. Investigating TrueCrypt volumes requires specialized knowledge and tools to bypass encryption and analyze the encrypted data.

The presence of various software installations, including Thunderbird Setup, Tor Browser, TrueCrypt, and VeraCrypt, on John's laptop suggests a deliberate effort to enhance security and privacy measures. Thunderbird Setup indicates the use of an email client, potentially for secure communication. Tor Browser usage points to anonymity-seeking activities, while TrueCrypt and VeraCrypt installations signify a commitment to data encryption and protection. These software choices reflect a conscious effort by the user (Shawn) to safeguard sensitive information and maintain privacy, presenting forensic challenges due to encryption and implying potential legal considerations regarding data access.

APPENDIX A

Step No.	Date	Time (UTC+5:30)	Action Taken	Method/Tool Used	Outcome
1	2024-05-18	09:00	Initiated forensic investigation	Logged into Azure environment	Accessed Azure environment successfully
2	2024-05-18	09:15	Opened pre-ingested case in Autopsy	Autopsy (Open Recent Case)	Case loaded successfully
3	2024-05-18	09:30	Verified integrity of forensic image	MD5 hash comparison	Hash values matched
4	2024-05-18	09:45	Examined file structure of forensic image	Autopsy (File Manager)	File structure displayed
5	2024-05-18	10:00	Searched for keywords related to illegal activities	Autopsy (Keyword Search)	Several relevant hits found
6	2024-05-18	10:30	Analyzed email communications	Autopsy (Email Parser)	Identified suspicious emails
7	2024-05-18	11:00	Extracted browser history	Autopsy (Web History Analyzer)	Found evidence of searches related to drugs
8	2024-05-18	11:30	Examined chat logs	Autopsy (Communications)	Identified chat logs discussing illegal trades
9	2024-05-18	12:00	Took a break		
10	2024-05-18	12:30	Extracted relevant documents	Autopsy (Document Analysis)	Retrieved documents on drug transactions
11	2024-05-18	13:00	Checked installed applications	Autopsy (Installed Programs)	Found software related to anonymous browsing
12	2024-05-18	13:30	Analyzed file metadata	Autopsy (Metadata Extractor)	Confirmed creation and modification dates

13	2024-05-18	14:00	Obtained sector locations of important files	FTK Imager	Sector locations retrieved
14	2024-05-18	14:30	Generated report on findings	Autopsy (Report Generator)	Draft report created
15	2024-05-18	15:00	Reviewed report	Manual review	Verified accuracy and completeness
16	2024-05-18	15:30	Created timeline of events	Autopsy (Timeline Analysis)	Comprehensive timeline generated
17	2024-05-18	16:00	Saved and secured all findings	Export to secure storage	Findings securely stored
18	2024-05-18	16:30	Finalized the report	Microsoft Word/PDF	Report Finalized

Appendix B

Date	Time (AWST)	Event Description	File Path/Details
2024-05-18	09:15	Opened pre-ingested case in Autopsy	Case ID: Assignment2, Case Name: Assignment2.aut
2024-05-18	09:45	Examined file structure	Root directory contents displayed
2024-05-18	09:45	Looked into views files	File views
2024-05-18	10:00	Searched for keywords related to drugs	Keywords: "drug", "firearm", Hits: 25
2024-05-18	10:30	Analyzed email communications	/img_drugs.E01/Users/shawn/AppData/Local/Google/Chrome/User Data/Default/Cache/f_0000b4/f_0000b4/0
2024-05-18	11:00	Extracted browser history	/img_drugs.E01/Users/shawn/AppData/Local/Microsoft/Windows/History
2024-05-18	11:00	Analyzed chat logs	/img_drugs.E01/Users/shawn/AppData/Local/Google/Chrome/User Data/Default/Cache/f_0000b4/f_0000b4/0
2024-05-18	12:00	Reviewed system logs	/img_drugs.E01/Windows/System32/winevt/Logs/Application.evtx
2024-05-18	12:30	Extracted relevant documents	/img_drugs.E01/Users/shawn/Documents/transactions.docx
2024-05-18	13:00	Checked installed applications	Path: /Programs/, TOR
2024-05-18	13:00	Installed TOR browser	/img_drugs.E01/Users/shawn/Downloads/torbrowser-install-win64-10.0.12_en-US.exe