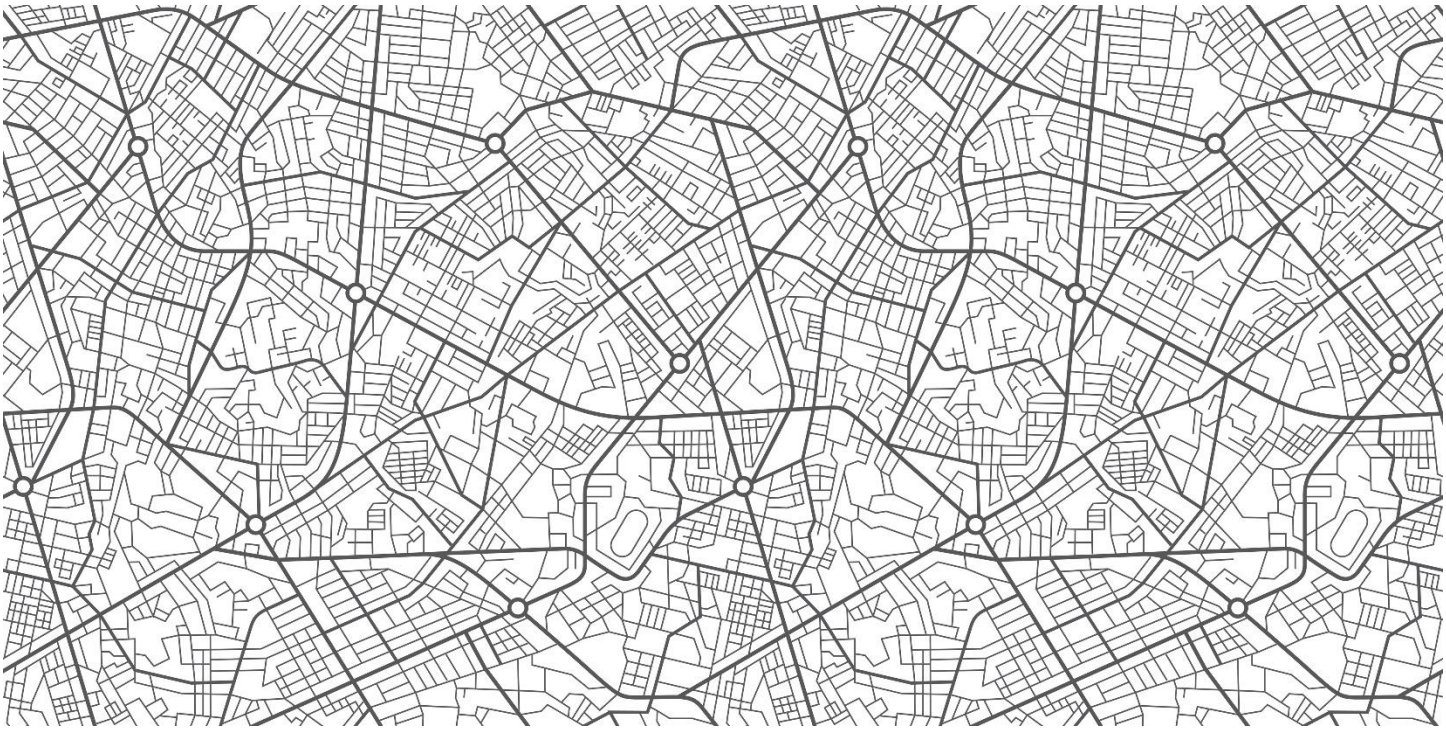
Digital Forensics Plan

Author: Marco CAVANI



Student ID: 10570027

Contents

Introduction 2

Timeframe 2

Background 2

Objectives 2

Strategies 3

Resources 4

Progress Indicator 4

INTRODUCTION

The WA Police have issued a forensics investigation against Mr Damon based on allegations of identity theft and fraud. After analysing the suspect's network traffic, the authorities decided to Seize the suspect's computer to investigate further. As result, a copy of the drive was prepared to conduct a digital forensic investigation. The digital investigation will be conducted to determine whether or not there is evidence of a crime in the suspect's drive. Steps and actions will be undertaken and documented in observance of the law and best practices.

TIMEFRAME

The investigation will be completed in the next three weeks. In week one, data will be acquired from the forensics image and in week two, all the data and processes will be analysed and reported meticulously. In week three a detailed document containing all processes and relevant findings will be presented. The forensic analysis will be conducted in a way to avoid contamination, integrity issues, encryption issues and chain of custody issues that can cause delays. In saying that, all findings will be presented before and not after the 17th of October.

BACKGROUND

The WA police have been notified of potential cybercrime. The suspect, Mr Damon, is accused of stealing identities to make fraudulent purchases online. As a consequence, the authorities obtained a warrant to analyse the suspect's workplace network traffic logs which outlined suspicious activities. Despite the defendant denying all accusations and having no previous convictions, the Police confiscated Mr Damon's laptop and created a forensic image that might contain relevant information. The forensic image of the suspect's drive will be provided by the police to conduct a digital forensic investigation. In saying that, further analysis will be performed on the forensic image to determine whether or not there is evidence of illegal activities on his PC.

OBJECTIVES

The 3 main objectives are:

1. Determine whether Mr Demons' computer was used for illegal activities
2. Determine who committed the crime
3. Determine how the crime was committed

The key point of the investigation is to find out whether or not there is evidence of identity theft and fraud on the suspect's computer. This can be verified by looking for pictures such as images of credit cards, CVV numbers, passports, and driver's licences, or by looking at activities such as browser history, emails, and text files. User login data, file timestamps, browser activities, the presence of malware, file histories, the presence of scrubbers, and deleted files can provide evidence to determine who committed the crime and how.

The investigation aims to answer questions like:

- Are there any pictures on the suspect computer that can be related to the crime?
- Is there any information that proves the suspect's intent to delete or obfuscate suspicious files?
- Are there any suspicious activities that can be linked to fraud or identity theft?
- Are there any files in the allocated storage that the suspect tried to delete?
- Is there any user information that indicates who was operating the computer at a specific time?
- Is there any correlation between the browsing history and the suspect's intentions?

- Is there any suspicious software or malware installed on the computer that can have an impact on judgements?
- In the file history, is there any relevant pieces of information that can be used?
- Are there any emails that can be correlated with illegal activities?
- Are there any files that has been intentionally modified?
- What information can be triangulated to form evidence?

STRATEGIES

At the beginning of the investigation, at least two copies of the original drive will be created as per the contingency plan. The MD5 and the SHA-1 hashing methods will be used to verify integrity at all times. This method will ensure that the copies and the original are identical. During the analysis, all processes will be meticulously recorded, and a backup copy will be kept in case of contamination. The chain of custody will be maintained and documented during the investigation while the integrity of the data will be verified using the MD5, SHA-1 hash algorithms and HashCalc every time there is an update. Additionally, the drive will be inspected for potential evidence in the unlocated storage using Autopsy. Triage sandbox will be used in case of malware detection. All findings will be verified using different tools. The table below shows the steps required to gather and triangulate digital pieces of evidence from the suspect's device. The first part (week 1) focuses on data acquisition, while the second part (week 2) aims to identify data that needs more attention, in the third part findings will be triangulated and presented (week 3).

Objectives	Timeframe	Resources	Purpose	Action required
1. Hashing of digital objects	At all times	MD5, SHA-1 HashCalc FTK Imager SIFT	Avoid Obfuscation Check the integrity of the file	Validating data using different tools and hash methods
2. Verify the file type	At all times	Autopsy SIFT	Ovid obfuscation	Checking the headers and the footer of the file
3. Documenting all steps	At all times	Microsoft Word Autopsy	Ensure that people with the right skills can repeat the process and obtain the same results	Generate comprehensive report
4. Validate the copy of the copy	Week 1	SIFT FTK Imager	Ensure the integrity of the copy Have a backup copy	Check if the copy has the same hash output set the read-only permission
5. Recover deleted files & folders	Week 1	FTK Imager	Searching for deleted evidence	Acquiring files from the unallocated folder
6. Conduct keyword list searches	Week 2	Autopsy	Searching for specific file	Looking for specific files
7. Create timelines	Week 2	Autopsy	Examining files updates and user time zone	Exanimating specific files timeline
8. Examine the evidence directory tree	Week 2	Autopsy	Looking for anomalies	Inspecting the directory tree
9. Perform keyword searches	Week 2	Autopsy	Target specific files	Use regular expression
10. Search for relevant evidence types	Week 2	Autopsy	Targeting file types that can be relevant	Looking for files by type
11. Look for the obvious evidence	Week 2	Autopsy	Looking for data which are of easy interpretation	Looking for ID images, credit card numbers, text files, and email.
12. User/systems/data	Week 3	Autopsy	Looking for intent evidence	Looking for data linked with different users' and browsers' history
13. Identify Artefacts generated by the systems	Week 3	Autopsy	Correlate user activities with other pieces of evidence	Looking for file timestamp and footprint
14. Generate a report	Week 3	Microsoft Word Autopsy	Present the findings	Writing a final report

The main goal of this forensic evaluation is to provide relevant evidence to the case. During the investigation, files will be collected, processed, investigated, and reported. The analysis will be conducted on suspicious objects like image files such as passports, driver's licences, and other IDs or any other elements that could be linked with fraud or identity theft. During the investigation will be searching for stenographic tools, scrubbers and malware that might obfuscate or compromise pieces of evidence in the suspect pc. In the end, all issues based on admissible, authentic, completed, reliable and believable facts will be investigated and reported. The process of investigation will include looking for obvious pieces of evidence like images, credit card numbers, phone numbers, browser history, bin and unlocated folders, email, and text documents. Also, for non-obvious things like file types, metadata, timestamps, versions of files, bitmap, file formats, the presence of stenography tools, and virus activities. This process aims to find and investigate patterns of fraudulent activities. The final report will include all issues found along with a comprehensive analysis based on the forensic investigation, triangulation, and correlation of the information in other to provide valid evidence to the case.

RESOURCES

Management approval is required to proceed with the investigation. The police will provide a digital copy of the suspect's drive. The digital copy will be validated using FTK imager or using MD5 and SHA-1 Hashing methods on SIFT from Azure lab Windows 10 operating system that has Hyper-V installed to run SIFT as a virtual machine. After the drive is validated, software like Autopsy will be needed to analyse the data. I will be conducting a digital forensic investigation on the suspect device using an Asus VivoBook. However, in case that specific resources are not available similar solutions can be found. For example, if the manager in charge is not available at the moment of the warrant, another figure from the management or a supervisor can approve the proposal on his behalf. Furthermore, if capabilities are constricted, then an expert in digital forensics can be included to provide support. Software and hardware can also be replaced. (See option 1 and option 2 tables below).

Option 1.

PEOPLE	SOFWARE	HARDWARE	CAPABILITY
Police, Marco CAVANI, manager	FTK Imager, Autopsy, HashCalc, azure lab, Windows 10, Windows 11, Hyper-V, Linux (SIFT), Triage sandbox	Asus Vivo Book	Preserve the integrity of data, Identify and triangulate evidence

Option 2.

PEOPLE	SOFWARE	HARDWARE	CAPABILITY
Police, Marco CAVANI, forensic expert, Supervisor, or alternative manager	Encase, X-ways, Windows 11, VirtualBox, Linux (UBUNTU), VirusTotal sandbox	Lenovo IdeaPad	Forensic expert support

PROGRESS INDICATOR

The table shows a list of milestones that will assess successful progress during the investigation. All milestones are comprehensive of required actions, measurable results, and a time frame.

Milestone	Action	Result	Time
1. Ensure the integrity of the drive	Hashing drive and folders and comparing hash outputs	The file has not been compromised	Week 1
2. Ensure the file integrity	Checking that the files extension is the same as the files type	The file can be seen for what they are	Week 2
3. Found images containing illegal content	Searching for the image file on the drive using regex features in Autopsy	Find 3 or more suspicious images	Week 2
4. Found text files containing suspicious content	Searching by file types	Find text files containing suspicious content	Week 2

5.	**Verify intent of actions**	Looking at user log history, presence of malware, deleted file, presence of scrubber	Know what	Week 2
6.	**Found suspicious files/images in the unlocated space**	Looking for unlocated files in Autopsy	The file that has been deleted can represent a good source of information as they could have been deleted to hide information	Week 2
7.	**Gathered additional information from the system and artefacts generated by the computer**	Looking for artefacts or other data generated by the computer and data system	More data can be analysed and triangulated	Week 2
8.	**Another expert can undertake the same steps producing the same result**	Documenting every step meticulously	The investigation can be validated by another expert	Week 3
9.	**The information presented is understandable by the court**	Report all issues providing exhaustive information and analysis Base the analysis on valid evidence	The court can understand the investigation without issues	Week 3