# Introduction

The WA Police requested forensics investigations based on the allegation against Mr Damon. The allegations are identity theft and fraud. Based on the accusation, the Authorities inspected the suspect workplace’s network log and then requested a digital forensic analysis of the suspect to see if it contains relevant information for the case. The forensics examination 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 laws 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; 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 prepared. 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 trial day. PUT A DATE

# 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 demanded and obtained a warrant to access 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 analysis. In saying that, further investigation will be performed on the forensics images to determine whether or not there is evidence of illegal activities on his PC.

# Objectives

The main goal of this forensic evaluation is to provide relevant and pertinent 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 type, metadata, timestamp, versions of files, bitmap, file format, presence of stenography tools, and virus activities. The aim of this process is 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. The aim of it is to provide evidence for the court to make a judgment. It will provides valid evidence that are important for the case.

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?

Is there any file in the allocated storage that the suspect tried to delete?

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?

Is in the file history any relevant piece of information that can be used to triangulate facts?

Is there any email that can be correlated with illegal activities?

Are there any file that have been intentionally modified?

Collect -> process-> investigate -> report

Non-obvious data:

View previous versions of files

Recover “deleted” files

Find out what was typed

Report websites visited in the past

Standard bitmap file formats

– Joint Photographic Experts Group (.jpg, .jpeg)

– Portable Network Graphics (.png)

– Tagged Image File Format (.tif, .tiff)

– Graphic Interchange Format (.gif)

– Windows Bitmap (.bmp)

# Strategies

At least two copies of the original drive will be created as per the contingency plan. the M5 and the SHA-1 hashing methods will be used to verify the integrity. This method will ensure that the copies and the original are identical. A backup of the forensic copy will be created and verified. During the analysis, all processes will be meticulously recorded, and a backup copy will be kept in case of contamination. FTK Imager, Encase, and x-ways will be used to extract, keep, and analyse data. All information will be handled and verified in a secure environment using the azure virtual lab to avoid intentional and/or unintentional data modification. The chain of custody will be maintained and documented during the investigation while the integrity of the data will be verified using the M5, SHA-1 hash algorithms and HashCalc every time there is an update. Also, 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 digital pieces of evidence from the suspect’s device. The first part (week1) focuses on data acquisition, while the second part (week2) aims to identify data that needs more attention and, the third part is to analyse specific files and generate evidence.

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

Verify integrity of image  
– MD5, SHA1, etc.  
• Recover deleted files & folders  
• Conduct keyword list searches  
– What are you searching for  
• Create timelines  
– What is the time zone setting of the suspect system  
– What time frame is of importance  
– Graphical representation is very useful

School of Science  
Edith Cowan University  
Starting Our Investigation (Cont’d)  
• Examine evidence directory tree  
– What looks out of place?  
– Are any steganography tools installed?  
– Any Evidence Scrubbers?  
• Perform keyword searches  
– Indexed  
– Slack & unallocated space

School of Science  
Edith Cowan University  
Starting Our Investigation (Cont’d)  
• Search for relevant evidence types, i.e.,  
– Hash sets can be useful  
– Graphic Files  
– Spreadsheets  
– Hacking tools   
• Look for the obvious first  
• When is enough evidence, enough??

School of Science  
Edith Cowan University  
Starting the Investigation (Cont’d)  
• User/systems/data (intentionally):  
– User profiles  
– Program files  
– Temporary files (temp files)  
– Special application-level files - internet history, e-mail  
• Artifacts (generated by the systems):  
– Metadata  
– Windows system registry  
– Event logs or log files  
– Swap files  
– Recycle bin

End goals based on reading the bg what do you want to find

Fraudulent porches legal warrant

Identity theft

only images

as a forensic investigator, you have to work on which material provided to you

specific goal (what you looking for passport driver license credit card cvv numbers pictures ?malware was installed on the computer is a malware runs on the computer? Cash web pages images pictures)

in addition: I have identified how many images out of how many images? And come out with a percentages

• How will you undertake the analysis?

• What process and method will you use?

• What hardware and software tools will be used?

• Objectives focus on the what, strategies focus on the how!  
• Secure the evidence

How can I acquire the shreds of evidence

Have in mind that new objectives can be generated through ongoing investigation.

# Resources

• What resources will you need to complete the entire

investigation?

• Resources may include.

– People, software, hardware, capabilities

How will you manage specific resources being unavailable?

# Progress Indicator

What are the milestones in the investigation?

• The milestones permit the analyst to reflect back upon the analysis thus far

• Are things going good or bad?

• The milestones also ensure that the investigation is progressing adequately and in a timely manner

• Think project management!!!

|  |  |
| --- | --- |
| Introduction | A simple overview of what you foresee the  investigation to entail. A brief overview of what  happened, who and what was involved. |
| TimeFrame | Demonstrate how you will manage your time  successfully through semester. |
| Background | Consider this your opportunity to discuss and  explain the points raised in the introduction in  detail! |
| Objectives | Explain ~3 key/critical objectives! |
| Strategies | Now explain how you will accomplish your  objectives (this is the difficult part) |
| Resources | What tools/resources do you think you will need |
| Progress/performance indicator | How will you assess successful progress? |

• Bob is suspected of accessing illegal content

• Issue 1: Does content in question exist on

Bob’s computer(s)? Yes/No? Prove it!

• Issue 2: If content exists...can Bob be linked

to the content? Yes/No? Prove it!

• Issue 3: If Bob can be linked to the

content...was it accessed intentionally?

Yes/No? Prove it!

# Introduction

The WA Police requested forensics investigations based on the allegation against Mr Damon. After inspecting the suspect network log, the accusation converged on the defendant's device which might contain relevant information for the case. The forensics examination will be conducted to determine whether or not there is evidence of a crime in the suspect device. Steps and actions will be undertaken and documented in observance of laws.

# Timeframe

The investigation will be completed in the next three weeks. In week one, data will be acquired from the forensics image while in week two all the data and process will be analysed and reported meticulously. In week three a detailed document containing all processes and relevant findings will be prepared. The forensic analysis is designed 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 trial day.

# 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 demanded and obtained a warrant to access the suspect’s workplace network traffic logs which outlined suspicious activities despite the defendant denying all accusations and having no previous convictions. furthermore, the Police confiscated Mr Damon’s laptop and created a forensic image that might contain relevant information. The forensic image is a bit-by-bit copy of the suspect’s drive. In saying that, further investigation will be conducted on the forensics images provided by the authorities to determine whether or not there is evidence of illegal activities on his PC.

The crime that you investigate cite!

• Factual details pertaining to the investigation

• Where did the offence take place?

• Who was involved?

• Who else may have been involved?

• Statements made by the offender or third parties

• Known problems relating to the suspects/victims or evidence which may inhibit or delay the investigation and analysis

# Objectives

What for?

Provide relevant and pertinent evidence (authenticity)

Evidence:

* Admissible
* Authentic
* Complete
* Reliable
* Believable

Provide complete evidence that are more than just prospective(provide the whole story)

Provide trustworthy evidence

Provide evidence which are understandable by the court (believable)

• A list of S.M.A.R.T objectives relating to the investigation

• What needs to be done?

• Objectives should be Specific, Measurable, Achievable, Relevant and Timely (SMART)

Objective 1,2,3,4,5,6 numerated

Recovering file technique(look for undeleted data)

Bit map

Vector graphic

Meta file

Use the software that concern through the ongoing investigation

Prepare to deal with different file types e.g., RAW images compress images

Triangulation can help to recover files using different software

Image editors to access image data.

Provide estimation of the status of the file whether they are available or corrupted (carving files in SANS forensic)

Find evidence of file use

Describe the context to provide evidence of intentions

File recovery system management layout

Successful file recovery FAT32

File carving to provide evidence of the intent of deleting a file which could be a sign that someone tried to hide or get rid of the file

File header to confirm the file type was the file renamed

File footer

Verify the File signature to establish the file format

CARVING

Potentially overwritten data

Scan the images using the header hand the footer

Scan identifier?

# Objectives

The main goal of forensic analysis is to identify the presence of the crime’s evidence on the suspect’s drive. More precisely, identity theft and fraud. It can include searching for images such as a passport or driver’s licence and other IDs that belong to potential victims. Also, will be searching for potential malware activity that could have harmed the suspect pc using sandboxes in case there will be evidence of is tra of malware activities

End goals based on reading the bg what do you want to find

Fraudulent porches legal warrant

Identity theft

only images

as a forensic investigator, you have to work on which material provided to you

specific goal (what you looking for passport driver license credit card cvv numbers pictures ?malware was installed on the computer is a malware runs on the computer? Cash web pages images pictures)

in addition: I have identified how many images out of how many images? And come out with a percentages

• How will you undertake the analysis?

• What process and method will you use?

• What hardware and software tools will be used?

• Objectives focus on the what, strategies focus on the how!  
• Secure the evidence

How can I acquire the shreds of evidence

Have in mind that new objectives can be generated through ongoing investigation.

# Resources

• What resources will you need to complete the entire

investigation?

• Resources may include.

– People, software, hardware, capabilities

How will you manage specific resources being unavailable?

# Progress Indicator

What are the milestones in the investigation?

• The milestones permit the analyst to reflect back upon the analysis thus far

• Are things going good or bad?

• The milestones also ensure that the investigation is progressing adequately and in a timely manner

• Think project management!!!

|  |  |
| --- | --- |
| Introduction | A simple overview of what you foresee the  investigation to entail. A brief overview of what  happened, who and what was involved. |
| TimeFrame | Demonstrate how you will manage your time  successfully through semester. |
| Background | Consider this your opportunity to discuss and  explain the points raised in the introduction in  detail! |
| Objectives | Explain ~3 key/critical objectives! |
| Strategies | Now explain how you will accomplish your  objectives (this is the difficult part) |
| Resources | What tools/resources do you think you will need |
| Progress/performance indicator | How will you assess successful progress? |

• Bob is suspected of accessing illegal content

• Issue 1: Does content in question exist on

Bob’s computer(s)? Yes/No? Prove it!

• Issue 2: If content exists...can Bob be linked

to the content? Yes/No? Prove it!

• Issue 3: If Bob can be linked to the

content...was it accessed intentionally?

Yes/No? Prove it!