****­

Version 1.0



31, March 2020

Case #423

Digital forensic Report Plan

**Presented by: n4n05h4d0w5**

[n4n05h4d0w5@gmail.com](mailto:n4n05h4d0w5@gmail.com)

+61 984 2349

**Presented To: Ryan Nye**

Information security and network manager

[ryan.nye@wapolice.com](mailto:ryan.nye@wapolice.com)

+61 8473 284

Contents

[**Introduction.** 2](#_Toc38244640)

[**Timeframe.** 2](#_Toc38244641)

[**Background** 2](#_Toc38244642)

[**Suspect summary:** 3](#_Toc38244643)

[**Suspicious devices summary:** 3](#_Toc38244644)

[**Objectives** 4](#_Toc38244645)

[**Strategies** 5](#_Toc38244646)

[**Resources** 5](#_Toc38244647)

**My Resume**…………………………………………………………………………………………7

# **Introduction.**

The purpose of this report is to obtain permissions or warrant to carry out a digital forensic investigation in order to provide assessment procedures, discoveries and suggestions from evidence regarding the cyberbullying event (presumably) which occurred in CVW creative.LTD office in Perth. An allegation was made to Perth Police Station based on retaining and distributing digital content relating to clowns in the workplace of the above-mentioned organization.The devices in question is now held in the custody of the law. The main intention of the investigation is to recover and capture the metadata relating to the case items and match or identify the offender according to them.

# **Timeframe.**

the final analysis and report relating to this case are expected no later 25 June 2020. However, I will not be available on 13th and 14th of April due to the Sinhala and Tamil new year. However, this case requires the decryption process and the data recovery process. In this manner, these days are not permanent, it could be varied. Nevertheless, the best-case scenario, the trial date could be held on 25 June 2020.

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Objectives | May | | | | | April | | | | | June | | | | |
|  | |  |  |  |  |  | | --- | --- | --- | --- | --- | | 5 | 12 | 18 | 23 | 30 | | | | | | |  |  |  |  |  | | --- | --- | --- | --- | --- | | 4 | 13 | 18 | 23 | 29 | | | | | | |  |  |  |  |  | | --- | --- | --- | --- | --- | | 1 | 12 | 18 | 23 | 25 | | | | | |
| 1.Check the fingerprints on the Laptop |  |
| 2.Recover the Original Disk |  |
| 3.Analyze the entire laptop hard drive |  |  | | |
| 1. decrypt encrypted data |  | |  |
| 4.Analyze the cell phone. |  | | | |  | | |  |  |
| 1. recover deleted data |  | | | | | |  |
| 5.Examine & analyze malware |  | | | | | | | | |  | |
| 6.Examine the CCTV footages |  | | | | | | | | | | |  | |
| 7.Documenting, reporting & Presenting |  | | | | | | | | | | | |  | |
| 8.Final Date for Trial |  | | | | | | | | | | | | | |  |

# **Background**

On March 25, 2020, the witness named Steve Smith who was employed by CVW creative as a network administrator claims that he has seen individually approachable clown-related contents in a computer which belongs to one of his work colleagues who is named Clark Watson. Moreover, his ex-girlfriend(Michelle Jenneke) was also employed in the same office, and Steve evidenced that recently they had a bit of argument in the workplace. And other staff members inferred it. The main suspect (Clark Watson) strictly denies allegations which were made against him. And he already confessed that the computer belongs to him and he does not always bring the computer home or lock it when he is away from his desk. Furthermore, he was inferring that the computer was compromised with malware which brought any potential content showing up on his device.

On 30 March 2020, Scott Morrison (junior Investigator) who was tasked by Mr Keen conducted the logical acquisition. However, he had forensically cleaned the data from the suspect device drive. Fortunately, he managed to obtain the logical acquisition forensically sound manner using FTK imager. In Order to carry this investigation further, I need to use the copy of the FTK imager. Because odds of recovering forensically wiped data are extremely low. Anyway, I will give try to recover them. Moreover, the computer in question, some data had been encrypted. Therefore, the process of description is a must in this case.

The device in questions is an Acer laptop. Moreover, Prime suspect mobile phone was also impounded on suspicion which is a Samsung Galaxy note II. The seizure of the suspect’s devices was performed in a manner consistent with recommendations found in the Australian Institute of Criminology. The device in question is now held in the custody of the law.

## **Suspect summary:**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Priority** | **Name** | **Age** | Connection | Criminal Records |
| 1. | Clark Watson | 32 | Owner of the Computer | None |
| 2. | Michelle Jenneke | 30 | Clark’s Ex-girlfriend | None |

## **Suspicious devices summary:**

ACER ASPIRE E15:

|  |  |
| --- | --- |
| IMEI Number | 371947391741380183 |
| Model | Acer E5-423G-23QB |
| Vendor | Vodafone |
| Version | 5.4.23.2 |
| Internal Build | 5.4.23.2 |

 

SAMSUNG GALAXY NOTE 2:

* No SIM card or External storage was provided.

|  |  |
| --- | --- |
| IMEI Number | 7379719794193413193 |
| Model | GT-N7100 Galaxy Note II |
| Vendor | Samsung GSM |
| Version | 6.2.1.17 |
| Internal Build | 6.2.1.17 |

 

# **Objectives**

WA Police personnel and I together established the following engagement objectives:

1. Check the fingerprint on the computer and compare them with Clark’s fingerprint to see if anyone has used the computer other than Clark.
2. Attempt to Recover the forensically wiped hard drive for future litigation. (This process may or may not be successful.)
3. Analyse the entire laptop disk and the forensic digital images of it to determine the presence of digital content relating to clowns.
   1. If there is any encrypted content, decrypt them with the help of cryptographer. (This process may or may not be successful.)
   2. Determine whether Clark Watson possessed an explicit image of clowns on his laptop or phone purposely.
      1. If Suspicious device content them, determine whether Clark purposely distribute images for any harassment.
4. Analyse Clark’s mobile phone and the forensic digital images of it to determine the presence of digital content relating to clowns.
   1. If there are any deleted content, recover them
5. Investigate Malware on the sized computer in order to prove or disprove Clark’s statement on.
   1. If there are any malware detects, exams and analyses them.
6. Examine the CCTV footages to determine whether someone logged in and impersonated Clark on his computer.
   1. Adjudge if Clark was (un)present when accessing the content.

# **Strategies**

1. Check whether any unrecognised fingerprints on the computer with the help of junior investigator.
   * If there is any, try to match them with staff members’ fingerprints.
2. Attempt to Recover forensically wiped content using ProDiscover, Autopsy or X-Way. (This process may or may not be successful.)
3. Examine whether any illegal content in the laptop.
   * Attempt to decrypt the encrypted content using Forensic ToolKit (FTK).
   * Examine the browser history, USB devices usage, windows firewall configuration and user information using PlainSight version 0.1.
   * investigating the Windows the file system using the Evidence Tree in Autopsy 4.19.0.
4. Examine whether any illegal content or relating evidence are in Clark’s phone.
   * Using Cellebrite’s UFED4PC version 6.3.5.2, Examine the entire disk to determine any digital evidence about illegal content or any deleted data.
   * Using EnCase Mobile Investigator, Examine whether any possessed explicit photos of clown and purposely distributed illegal content for harassment
   * If there are any deleted content in the phone, recover them using EnCase Mobile Investigator
5. Check CCTV footages,
   * To check whether anyone used Clark computer when he is not around his desk
   * To check whether any suspicious activity happened in the office
   * And confirm whether Clark was Present at the time the clown relating contents were accessed with the help of staff members.
6. Prove or Disprove Clark’s statement about a malware infection
   * Using Volatility Framework 2.4, scan and analyse the malware in the laptop in question.
   * Reverse-Engineer of malware using WindowsSCOPE 3.2.0.

# **Resources**

This case requires:

* FTK image of the original computer which is obtained during the logical acquisition.
* approx. 70GB of storage capacity - To extract relevant files.
* Need to use VMware Workstation 15 Pro - To run necessary software.
* Need 8GB USB Pen Drive and 5 DVDs(writable, 2GB) - To run & copy necessary software.

Moreover, this case will need quite a few software:

* Forensic ToolKit (FTK) - To create forensically sound copy of the original drive
  + Vendor: AccessData
  + Version: 7.2.0
* PlainSight Platform - Examine the browser history, USB devices usage.
  + Vendor: PlainSight Software Technology
  + Version: 0.1
* X-Ways Forensics - For disk imaging and cloning
  + Vendor: X-Way Software Technology AG
  + Version: 19.0
* UFED4PC - To carry out an acquisition of the mobile device
  + Vendor: Cellebrite
  + Version: 6.3.5.2
* EnCase Mobile Investigator - To detect or recover any deleted content of the phone
  + Vendor: EnCase Investigator
  + Version: 1.06
* Volatility Framework - To scan and analyse the malware
  + Vendor: Volatility Foundation
  + Version: 2.4
* WindowsSCOPE - To reverse-engineer malware
  + Vendor: WindowsSCOPE Group
  + Version: 3.2
* Autopsy - Investigate the windows file system and detect deleted items
  + Vendor: Basis Technology
  + Version: 4.14

Cryptographer’s job shall be needed to decrypt the encrypted content and Junior digital forensic Investigator help could be useful to carry this investigation faster. Moreover, “*Digital Evidence and Computer Crime, Second Edition by Eoghan Casey”* the book will be exceptionally valuable to conduct this investigation effectively.

**Progress Indicators**

The Following milestones can be set for the investigative process to be able to track the progress:

* Try to recover the original disk. (This process may or may not be successful.)
* Examine the file system and disk of the laptop in question.
  + If there is any deleted content, Recover them.
  + If there is any encrypted content, try to decrypt them.
* Examine the file system and disk of the main suspect phone.
  + If there is any deleted content, Recover them.
* Acquiring and searching any illegal contents on suspicious devices
* If there any illegal content on the sized laptop or the phone,
  + Examine and analyse that forensically one by one.
* Examine and analyse malware that infected the captured laptop.
* Investigate the office CCTV footage of the last few months.
* Identifying and aligning any issues.
* Acquiring and extracting evidence.
  + Analysis of extracted data
    - Timeframe analysis - what, when, why
    - Data hiding analysis
  + Admissibility of the seized evidence
  + Authenticating the seized evidence
* By analysing the evidence that was found, conclude.
* Documenting and presenting evidence and conclusion.

**My Resume**

….