**Forensics Investigation Plan**

# Introduction

The incident happened here is accessing the content related to cat which is an offence according to Western Australia. Clark is the suspected person here. The primary suspected person here in this case is Clark who is reported by Network administrator to Line Manager named Ash and then to junior police officer. It came to light that during the formal interview Clark has disagreed the claims. Also, it’s clear that he has no criminal records up to date. So, the investigator Paul Ekman who was asked to examine the interview video stated that there’s something wrong with Clark and he was interviewed again. But this time it involves the usage of malware for defence. So, Paul and the forensic group asked to go with detailed forensics investigation. The only this which affecting the investigation is Clark’s device Since, the junior investigator wiped the hard disk we have left with only a forensic image which has 044288459e2fd193e446eec8de0acdd9 as MD5 hash value. So, the important things we are looking for as forensics investigator is any evidence that is related to accessing the illegal content Cat and whether it’s accessed by Clark or not if yes then whether it’s intentional or unintentional, if no then the appropriate person who access the illegal content.

# Timeframe

The due date to submit the final digital forensics analysis report is 25th November 2019. Since, digital investigation involves several steps I have devised the following plan.

**Week 1-2** Basic Examination

**Week 3-4** In-depth Examination

**Week 5-7** Detailed Analysis

**Week 8** Report preparation and presentation

# Background

A detailed digital forensic investigation requested by Western Australia police in order to conclude a case related with accessing the illegal content Cats which happened inside the organization named Daily planet. The suspect here is Clark who is an employee in Daily planet. He has been reported by Network administrator to the line manager Ash and then Clark has been investigated by police officers and denied the allegation. The primary obstacle which pertaining the investigation is the main evidence which is Clark’s device seized by police has been formatted accidently by junior investigator and it’s suspected that Malware could have been used.

# Objectives

The Primary objectives of this digital forensic investigations are,

* To analyse the provided digital forensics image to find out all the digital content that are related to the illegal contents i.e. cats.
* Making the running sheet.
* To find out whether Clark is involved in this case based on forensics image examinations.
* If Clark involved what are all and how much is the illegal content being accessed. If not then find out who has done this.
* If it comes to light that Clark is the responsible person then must figure out whether he did it intentionally or unintentionally.
* Provide valid proof which attest/ condemn the involvement of Clark in this case.
* Produce report in timely manner and in acceptable format.
* Very importantly to protect the integrity of the evidence throughout the investigation process.

# Strategy

In order to conclude this case, it’s necessary to analyse and examine the digital evidence thoroughly.

## Basic Examination

* The basic examination includes examining the file systems and find possibility of recovering the deleted file/information that is related to the case.
* It also includes analysing browser history, downloads, email communications.
* Making sure the presence/absence of Clark on given date and time by examining CCTV footages. This can be done by visiting Clark’s office.

## In-depth examination

* In-depth examination includes examining the log files and system dump files. System files may include hidden/password protected / encrypted folder and files. Also extracting metadata included.
* In network wise examining browser cookies, sessions, cache can be done in in-depth examination.
* Since, it’s suspected that malware attack would have included malware analysis can be conducted. This includes behavioural analysis.
* The tools that are going to be used in this investigation are SIFT, FTK manager and Autopsy.

## Detailed analysis

* Detailed analysis includes analysis of examined results from all the tests. This may also include running same testes again with different tools to make sure the results are identical.

## Detailed reports

In this case it’s vital to produce valued and understandable report to the Police department. So, it’s important to make sure the report has followed prescribed format. Also, attaching running sheet need to be done.

# Resources

Hardware **–** Minimum of 75 GB in virtual environment.

## Software

* **VMware Virtual Machine –** To get scalable and reliable Virtualization environment
* **AccessData and X-ways** – For forensics image cloning.
* **ProDiscover Forensics and Autospy –** To examine the hard disk files thoroughly.

The reason why I am using two tools is to make sure the outcome of tests are same and the results are identical also in case if one tool is unavailable for extended period of time then continue the investigation process with another one.

# Progress indicators

1. **Basic Examination**
   1. Examining the files and browser to find out the illegal contents in system,
   2. If the contents deleted, try to recover
   3. Check CCTV footages for physical evidences
2. **In-depth examination**
   1. Examining log/protected files
   2. Examining browser for specific activities
   3. Performing Malware analysis to know about the behaviour of it
3. **Detailed Analysis**
   1. Running same tests again with different tools
4. **Reports**
   1. Making running sheet
   2. Making report in timely manner and in prescribed format

# References

Gerald, L. (2006). Forensics Plan Guide. SANS Institute 2006.