Universiti Teknologi MARA

Social Network Anomaly Keyword Detector (SNeAKeD)

of

Investigation Information Autopsy (IIA)

Muhammad Syazwan Bin Khairani

Thesis submitted in fulfillment of the requirements for
Bachelor of Science (Hons.) Data Communication and Networking
Faculty of Computer and Mathematical Sciences

July 2013

ACKNOWLEDGEMENTS

"By the name of Allah, the Most Gracious and Most Merciful"

The project presented in this report could not been done without the support, encouragement and cooperation of many people. First of all, I would like to express my gratitude to my supervisor, Dr. Fakariah Hani binti Hj. Mohd Ali, who has always given valuable advice and encouragement to me. I also would like to thank him for giving this opportunity to learn and work under guidance, which has been memorable experience.

Special thanks to Dr. Nor Shahniza Kamal Bashah for her guidance to write this thesis report and her thoughtful suggestion at each stage in preparation of this project. Also thanks to all of my lecturers, which guide me to make this project paper successful. Without their cooperation, I would not be able to finish this project.

I also would like to thank to our entire family for their encouragement, knowledge and their constant prayer for me. Last but not least, thanks to my friends and associated for their encouragement, criticism and support for this project.

ABSTRACT

Forensic investigator across the globe getting busy each and every day getting complain from people about the social network abuse but they have difficulty in acquiring the evidence. According to the investigator from Digital Forensic Department of Malaysian Communication and Multimedia Commission (MCMC), they state that when a crime happened they usually having difficult times to trace and identify the criminal inside Local Area Network environment. Social Network Anomaly Keyword Detector (SNeAKeD) is a tool that can capture all the keystroke and information press by the user from their machines keyboard. SNeAKeD use the concept of keylogger. SNeAKeD can remotely send evidence from the client computer to the server database. Thus create a tools that can work invisibly behind the client computer. The type of data will be capture and analyse is text file where further enhancement of data type will be enhance in the future project. At the end of the project, SNeAKeD is expected to assist the digital forensic investigator to acquire evidence easily and accurately without complex hassle that they have to face before.

Table of Contents

CHAPTER ONE

INTRODUCTION

1.0 Background of Study

Cyber security in today world is getting more complicated each and every day coming. In the world, where internet is essential to our life privacy protection is very important to make sure crime can be avoided in the first place. Social network applications that increase with social network user make controlling the privacy protection difficult. Capturing cyber criminals is difficult as acquiring the evidence is usually complicated. Most of country today's lack of cyber security law and specialist unit in cybercrime investigation. Another reason is that most social network companies refuse to cooperate with forensic investigator to give crucial information for evidence. This is now getting a worldwide cyber problem.

In our country, Malaysian Communications and Multimedia Commission (MCMC) face the same problem. The latest issues like the infamous 'Calvin Gani' and 'Rakyat Anarki' case where they reportedly accused for using abuse word to Prophet Muhammad and the Royal Malaysia Police (PDRM) in the social network. This two case is the example of what the investigator have to face this day in the social network world, where they need to investigate and collect the evidence to proof the criminal guilty. This problem are getting worst and worst each and every day, so a tools is really needed to help the investigator especially to help cure these community that start to lost good manner affected by this problem. It is a step that would advance cyber security on a global basis ahead. At the least, it is a solution that worthy to try and maybe a step that will open to another good solution.