Universiti Teknologi MARA

Investigation on Anonymous Email in Online Social Networking

Fatma Husna binti M Mazlin

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

JANUARY 2016

ACKNOWLEDGEMENTS

Alhamdulillah..

First and foremost, praise to Allah, the Almighty Lord of all creations who has given me strengths and courage throughout this learning process. Without His loves and blessings, this proposal would not be possible to be completed. Again, praises are given to Him.

Special thanks to my thesis supervisor, Prof Dr Mazani Manaf who has provided me with so much guidance and assistance in completing this proposal. Your kindness, time and effort will always be remembered. May Allah reward you with His blessings for all that had been offered.

Many thanks to the course coordinator, Mdm. Nurshahrily Idura Ramli for giving me the opportunity to experience the new kind of learning process throughout this study. Your advices and cooperation had helped me during my studies in UiTM.

A lot of loves and gratitude must be given to my parents who have been very supportive throughout this research. Without your prayers, loves and supports, this proposal would not be coming true. Therefore, thanks again to my dearest father, Mr. M Mazlin Mamat, my loving mother, Mdm. Ghayah Salleh.

Last but not least, I would like to thank all my friends for the supports that had been given during the process of completing this proposal.

Thank you.

ABSTRACT

Anonymous email is mostly hassle the email user because they do not know where the email comes from. Besides, anonymous email usually related with cyber crime like banking fraud, identity theft and cyber bullying. The forensic investigators or analysts need to know the source of the email before they proceed for other processes of the investigation. The forensic analysts should have to analyze the anonymous email to find the evidence that related with the cyber crime. Process of analyze the anonymous email; the forensic analysts should use a tool that can trace the source of the anonymous email. IP address location tracker system is a tool that can trace the location of anonymous email based on the IP address of the anonymous email. The information that will be received after tracing the anonymous email are information of country name, region name, city, longitude, latitude, country code and postal code of the IP address. At the end of the project, this IP address location tracker system expected to assist the forensic analysts to find the evidence of digital forensic for anonymous email.

TABLE OF CONTENTS

ACKNOWLEDGEMENT iii

ABSTRACT iv

LIST OF FIGURES viii

LIST OF TABLES ix

LIST OF ABBREVIATIONS x

CHAPTER

1 INTRODUCTION

1.0 Introduction 1

1.1 Background of the study 1

1.2 Problem statement 3

1.3 Project Aims and Objectives 4

1.4 Project Scopes 5

1.5 Significance of the Project 5

2 LITERATURE REVIEW

2.0 Digital forensic investigation 6

2.1 General procedure of digital forensic investigation 7

2.1.1 Identification of evidence 7

2.1.2 Preservation of evidence 7

2.1.3 Analysis of evidence 8

2.1.4 Reporting of evidence 8

2.2 Anonymous email 10

2.2.1 How does anonymous email works 12

2.2.2 Analysis of anonymous email 13

2.2.3 Retrieve IP address of anonymous email 14

2.3 Tracking IP address 15

2.4 Python for Digital Forensic Analysis 17
2.5 Related work 18
2.5.1 Forensics tools for social network security solution 18
2.5.2 IP Address Tracking program 18
2.5.3 EmailTracer 18
2.5.4 eMailTrackerPro 19
2.5.5 Email Trace 19
2.5.6 IP Address Geographical Location 19
2.5.7 Email sender location tracer 20
2.6 Summary of the related work 20

3 METHODOLOGY

3.0 Introduction 22
3.1 Research Methodology Framework 23
3.1.1 Feasibility study 26
3.1.2 Analysis phase 26
3.1.2.1 User requirement 26
3.1.2.2 Software and hardware requirement 27
3.1.2.3 Install Python 2.7 and PyQt GPL v.11.4 for Python v2.7 (x32) 28
3.1.3 Research design and development 29
3.1.4 Verification and validation 30
3.1.5 Documentation 30
3.2 Design Phase 31
3.2.1 Flowchart of analysis the IP Address of 31