DIGITAL FORENSIC INVESTIGATION – METHOD FOR IDENTIFICATION AND ANALYSIS OF MALICIOUS SOFTWARE ON LINUX SYSTEM

By

Ahmad Zaid Zam Zami

A Thesis submitted to the Master Study Program of

INFORMATION TECHNOLOGY

In Partial Fulfillment of the Requirements for

MASTER'S DEGREE

IN

INFORMATION TECHNOLOGY

Swiss German University
Education Town BSD City
Tangerang 15339
Indonesia

January 2014

Revision after the Thesis Defense on 18 February 2014

STATEMENT BY THE AUTHOR

I hereby declare that this submission is my own work and to the best of my knowledge, contains no material previously published or written by another person, nor material which to a substantial extent has been accepted for the award of any other degree or diploma at any educational institution, except where due acknowledgement is made in the thesis.

Ahmad Zaid Zam Zami

_____ _____

Student Date

Approved by:

Dr. Ir. Moh. A. Amin Soetomo, M.Sc.

_____ _____

Thesis Advisor Date

Charles Lim, M.Sc., ESCA, ECSP, ECIH, CEH, CEI

_____ _____

Thesis Co-Advisor Date

Dr. Ir. Gembong Baskoro, M.Sc.

_____ _____

Dean Date

ABSTRACT

DIGITAL FORENSIC INVESTIGATION – METHOD FOR IDENTIFICATION AND ANALYSIS OF MALICIOUS SOFTWARE ON LINUX SYSTEM

By

Ahmad Zaid Zam Zami

Dr. Ir. Moh. A. Amin Soetomo, M.Sc.

Charles Lim, M.Sc., ESCA, ECSP, ECIH, CEH, CEI

SWISS GERMAN UNIVERISTY

Malware (malicious software) has become the most serious security threats on the Internet. There is a malware that is created to provide remote access to the victim computer by bypassing normal authentication known as backdoor. Criminals are making extensive use of backdoor to control computers and steal confidential or proprietary information. The information can be used to commit fraud, identity theft, or can be sold or traded to others. Therefore, forensic investigator need to have suitable methodology to identify and analyze a computer that is compromised by malware. This study aimed to identify artifacts or digital trail that can be potentially as evidence that may be left by the backdoor installed on a victim's computer. The final results of this study will be used as a guide or user manual for law enforcement officers in conducting searches of digital evidence, especially on an infected computer.

Keywords: Computer forensic, cyber crime, malware, linux.

DEDICATION

I dedicate this thesis to my family, my parents and faculty of engineering and information technology in SGU (Swiss German University), Tangerang - Indonesia and all people who need guidance in implementation of Incident Handling using Computer Forensic Methodology.

ACKNOWLEDGMENTS

The author also wishes to express utmost gratitude to my beloved wife Dhahiri Hagyar Siwi, my bautiful daughters Aisha Mughny Shaliha and Qanita Izzatul Himmah. The author thanks them for all encouragement, the strength, patience, and supports they give for the completion of this research

The author also thanks to Dr. Ir. Moh. A. Amin Soetomo M.Sc. as the advisor and Mr. Charles Lim, M.Sc, as co advisor. They have provided guidance, suggestions, idea, feedbacks, and supports that helped to shape of this work.

Thanks to Prof. Dr. Heiko Schoeder, Prof. Dr. Ing Wolfram Stanek, Mr. Kho I Eng, Dr. Ir. Gembong Baskoro, M.Sc., Dr. Harya Damar Widiputra, Mr. Reggio Hartono, Ms. Rachmawati, Ms. Cornelia Manik and other Swiss German University members for the supports.

Last but not least, the author also would like to thank all of MIT students and friends: Prof Richardus Eko Indrajit, Dwi Ade Handayani Capah, Tita Latifah, Muhammad Salahudien Manggalani, Carlia for their support in providing information and references that helped in completion of this work.

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES