

UNIVERSITI TEKNOLOGI MARA

**DIGITAL FORENSICS READINESS
IN PUBLIC SECTOR**

MOHAMAD AFIZAL BIN MD TAHIR

IT Project submitted in partial fulfillment
of the requirements for the degree of
Master of Science in Information Technology

Faculty of Computer and Mathematical Sciences


January 2016

AUTHOR'S DECLARATION

I declare that the work in this IT Project was carried out in accordance with the regulations of Universiti Teknologi MARA. It is original and is the results of my own work, unless otherwise indicated or acknowledged as reference work. This IT Project has not been submitted to any other academic institution or non-academic institution for any degree or qualification.

I, hereby, acknowledge that I have been supplied with the Academic Rules and Regulations for Post Graduate, Universiti Teknologi MARA, regulating the conduct of my study and research.

Name of Student : Mohamad Afizal bin Md Tahir
Student I.D. No. : 2012734331
Programme : Master of Science in Information Technology
Faculty : Computer and Mathematical Sciences
IT Project Title : Digital Forensics Readiness in Public Sector

Signature of Student : 

Date : 26 January 2016

ABSTRACT

Digital Forensics is a part of forensic science on investigation found in digital devices that has expanded from computer forensics to investigation of storing digital data. Digital forensics is a wide topic that been focused nowadays as Malaysia have implementing Malaysian Computer Crimes Act 1997 (CCA 1997) on providing important guidelines for computer crime investigation. As in public sector, the government under the Ministry of Science, Technology and Innovation (MOSTI) set up an agency called CyberSecurity Malaysia (CSM) to deal and lead in computer forensic evidence. Malaysian Administrative Modernization and Management Planning Unit (MAMPU) also can review this study as an input on consult service to ensure that procedures and implementation of digital forensics readiness in public sector are in line to improve the public service delivery system. Participation from agencies in public sector on readiness to implement digital forensic as an incident responder will help on protecting digital evidence at the first stage. This research is about Information Technology (IT) management using qualitative approach to identify several aspect of indicator towards readiness, adopted from several digital forensics readiness frameworks that will explain more in this report. Therefore, the purposes of this study are to identify factors that affect digital forensics readiness in public sector, and to recommend based on the findings to identify the digital forensics readiness among public sector. This study is using qualitative analysis and participated by five respondents from IT personnel of public sector with more than four years' experience in IT security or digital forensics readiness. The findings of the study perform in respondent identification and open-ended question interview. There are five categories with several sub-questions that focused on respondents' experience towards digital forensics readiness built from adopted conceptual framework. Recommendations from this study are based on findings of factors that affect digital forensics readiness consists of strategy, policies and procedures, technology, digital forensic response and compliance and monitoring. Based on the findings, there are lots to do especially on guidelines, policy and procedure that focused on digital forensics readiness as for now the public sector are focusing on securing Information and Communications Technology (ICT) in their working environment. As education purpose, this research helps organization to identify factors towards digital forensics readiness in public sector.

ACKNOWLEDGEMENT

Alhamdulillah, in the name of ALLAH, the Most Beneficent and the Most Merciful, praise and blessing upon the Prophet Muhammad, His family and companions. Thank you ALLAH for His willing on making this Information Technology (IT) Project completed successfully.

IT Project is a part of requirements for degree of Master in Information Technology at Universiti Teknologi MARA (UiTM), Malaysia. This project was completed with supportive from numbers of valuable people in my life and worthy of appreciation.

I would like to thank my supervisor, Puan Fauziah binti Redzuan for her knowledge, supervision, support, patience, and advice through completing this project. To other lecturers that teach me from beginning to the end on completing this degree of Master, I state my appreciation for their time on sharing valuable knowledge through semesters.

To my wife, parents, family, colleagues, and friends who have given moral support and understanding through this learning period, I really appreciate for every moment and helps when needed.

To all responders for interview session and previous researcher for the information and input on findings, I also appreciate for their co-operation and time.

Thank you for inspiration, believing, support, and commitment, May ALLAH bless us.

Thank you.

TABLE OF CONTENTS

	Page
AUTHOR'S DECLARATION	i
ABSTRACT	ii
ACKNOWLEDGEMENT	iii
TABLE OF CONTENTS	iv
LIST OF TABLES	viii
LIST OF FIGURES	ix

CHAPTER ONE: INTRODUCTION

1.1	Background of the Study	1
1.2	Digital Forensics	2
1.3	Readiness	2
1.4	Problem Statements	3
1.5	Research Questions	3
1.6	Research Objectives	4
1.7	Research Methodology	4
1.8	Scope of the Study	5
1.9	Significant of the Study	5
1.10	Report Outline	6
1.11	Definition of Terms	6

CHAPTER TWO: LITERATURE REVIEW

2.1	Introduction	8
2.2	Overview on Digital Forensics	8
2.2.1	Digital Forensics (DF) and Information Security (IS)	9
2.2.2	Digital Forensics Investigation Lifecycle	9
2.2.3	Digital Forensics in Malaysia	10
2.2.4	Professional Certificate	11