TABLE OF CONTENTS

PAGE

DECLARATION ii
APPROVAL iii
DEDICATION iv
ACKNOWLEDGEMENT v
TABLE OF CONTENTS vi
LIST OF TABLES ix
LIST OF FIGURES xi
LIST OF APPENDICES xiii
ABSTRACT xiv
ABSTRAK xv

CHAPTER
1. INTRODUCTION 1
- 1.1 Introduction 1
- 1.2 Background of Study 2
- 1.3 Problem Statement 3
- 1.4 Research Questions 3
- 1.5 Research Objectives 4
- 1.6 Research Methodology 4
- 1.7 Research Scope 6
- 1.8 Research Contribution 7
- 1.9 Project Report Overview 7
- 1.10 Conclusion 8

2. LITERATURE REVIEW 10
- 2.1 Introduction 10
- 2.2 Computer Virus 11
  - 2.2.1 Traditional Virus 12
  - 2.2.2 Polymorphic Virus 13
- 2.3 MD5 Checksum 15
- 2.4 Current Virus Analysis System 18
  - 2.4.1 CWSandbox 18
  - 2.4.2 Capture 19
  - 2.4.3 MBMAS 21

2.4.4 Joebox 23
2.4.5 ThreatExpert 25
2.5 Summary 26

3. RESEARCH METHODOLOGY 27
3.1 Introduction 27
3.2 Research Phase 28
3.2.1 Phase 1 – Study of Computer Virus and Anti Virus (AV) 29
3.2.2 Phase 2 – Study and Analysis of the Literature Review 29
3.2.3 Phase 3 – Collecting Data 29
3.2.4 Phase 4 – Implementation 30
3.2.5 Phase 5 - Testing 30
3.2.6 Phase 6 – Result Analysis 31
3.2.7 Phase 7 – Conclusion 31
3.3 System Development Methodology 31
3.3.1 Analysis 32
3.3.2 Design 33
3.3.3 Coding 33
3.3.4 Testing 34
3.4 Data Collection 34
3.5 Summary 39

4. IMPLEMENTATION 40
4.1 Analysis 40
4.1.1 Problem Analysis 41
4.1.1.1 The Current System 41
4.1.1.2 Problem Identification 43
4.1.1.3 The Proposed Architecture 44
4.1.2. System Requirement Analysis 45
4.1.2.1 Hardware Requirement 46
4.1.2.2 Software Requirement 47
4.1.2.3 User Requirement 47
4.2 Design 48
4.2.1 Context Diagram 48
4.2.2 Data Flow Diagram Level 0 50
4.2.3 Architecture 52
4.2.4 Input Output Design 54
4.2.4.1 Input Design 54
4.2.4.2 Output Design 88
4.3 Coding 89
4.3.1 Virus Behavior Monitoring Tool (VBMT) 89
4.3.1.1 Pre-Monitoring (Preparation) 90
4.3.1.2 Monitoring Process 92
4.3.1.3 Post-Monitoring 96
4.3.2 Virus Behavior Analysis Tool (VBAT) 97
4.4 Summary 100

5. TESTING **101**
5.1 Testing Process 101
5.2 Summary 116

6. SUMMARY AND CONCLUSION **117**
6.1 Summary 117
6.2 Conclusion 118
6.3 Future Work 119

REFFERENCES **120**
APPENDIX A **126**
APPENDIX B **134**
APPENDIX C **138**
APPENDIX D **141**