# TABLE OF CONTENTS

| 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 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

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
2.4.5 ThreatExpert
2.5 Summary

3. RESEARCH METHODOLOGY

3.1 Introduction
3.2 Research Phase
  3.2.1 Phase 1 – Study of Computer Virus and Anti Virus (AV)
  3.2.2 Phase 2 – Study and Analysis of the Literature Review
  3.2.3 Phase 3 – Collecting Data
  3.2.4 Phase 4 – Implementation
  3.2.5 Phase 5 – Testing
  3.2.6 Phase 6 – Result Analysis
  3.2.7 Phase 7 – Conclusion

3.3 System Development Methodology
  3.3.1 Analysis
  3.3.2 Design
  3.3.3 Coding
  3.3.4 Testing

3.4 Data Collection
3.5 Summary

4. IMPLEMENTATION

4.1 Analysis
  4.1.1 Problem Analysis
    4.1.1.1 The Current System
    4.1.1.2 Problem Identification
    4.1.1.3 The Proposed Architecture
  4.1.2 System Requirement Analysis
    4.1.2.1 Hardware Requirement
    4.1.2.2 Software Requirement
    4.1.2.3 User Requirement

4.2 Design
  4.2.1 Context Diagram
  4.2.2 Data Flow Diagram Level 0
  4.2.3 Architecture
  4.2.4 Input Output Design
    4.2.4.1 Input Design
    4.2.4.2 Output Design

4.3 Coding
  4.3.1 Virus Behavior Monitoring Tool (VBMT)
    4.3.1.1 Pre-Monitoring (Preparation)
    4.3.1.2 Monitoring Process
    4.3.1.3 Post-Monitoring
  4.3.2 Virus Behavior Analysis Tool (VBAT)

4.4 Summary
5. TESTING
  5.1 Testing Process
  5.2 Summary

6. SUMMARY AND CONCLUSION
  6.1 Summary
  6.2 Conclusion
  6.3 Future Work

REFERENCES

APPENDIX A
APPENDIX B
APPENDIX C
APPENDIX D