DIGITAL FORENSIC INVESTIGATION MODEL BASED ON MALAYSIAN STANDARDS WITH LIVE FORENSIC INVESTIGATION TOOL.

Sundresan Perumal
(Matric No. 4090083)

Thesis submitted in fulfillment for the degree of
DOCTOR OF PHILOSOPHY
IN
SCIENCE AND TECHNOLOGY

Faculty Of Science and Technology
UNIVERSITY SAINS ISLAM MALAYSIA
NILAI

DECEMBER 2012
AUTHOR DECLARATION

I hereby declare that the work in this thesis is my own except for quotations and summaries which have been duly acknowledge.

Date: 30th JUNE 2012
Signature:
Name:
Matric No:
Address:
BIODATA OF AUTHOR

Sundresan Perumal is a PhD student in University Sains Islam Malaysia under Faculty Science and Technology with matric no 4090083. He is a Malaysian with IC No 810531025819 and currently reside at 42F Jalan Kipark, 2A Taman Kipark Puchong Selangor . He have been lecturing for the past 9 years on various network security technology in private colleges and university. He also has vast industry experience. In the past 4 years, He is concentrating more into developing an improvised digital forensic investigation model and also develops a live forensic tool that could perform live data acquisition from suspected computer.
ACKNOWLEDGEMENT

This thesis was not by any means a solo effort. It’s my pleasure to convey my gratitude to them all in my humble acknowledgement.

At the first place I would like to record my gratitude to Associate Professor Dr. Norita Md Norwawi for her supervision advice, and guidance from the very early stage of this research as well as giving me extra ordinary experience throughout the work. Out of all she has provided me unflinching encouragement and support in various way. With her constant oasis of idea which exceptionally inspire and enrich my growth as a student and as a researcher. I am indebted to her more than she knows.

A special thanks goes to En. Muhammad Marwan Ismail from faculty of major language studies in USIM as he is my Arabic language lecture. As he have guide me a lot into learning the language in the easiest way and that have helped me in some part of developing the forensic tool in Arabic language.

I would like to gratefully acknowledge the whole Islamic Science University Malaysia for giving me a status as a student and also provide the best facility in the university.

Many thanks go in particular to Mr. Jegathesan and Ms. Michele Chan. Mr. Jega who helps me in solving most of my technical problems in developing my digital forensic tool. He seriously has the patient to sit with me for hours and figure out the solution for every problem that I refer to him. I also benefited by advice and guidance from Ms. Michele who always kindly grant me her time in checking all my grammatical mistake, towards the writing process of this thesis.

I would also like to thank Cyber Security Malaysia, People Tech Digital Forensic Lab Chennai India, Royal Malaysian Police Cyber Crime Unit and Blazenet IT & Security Consultancy Sdn.Bhd for their guidance and platform for me to do testing and presentation.

It is my pleasure to thanks my best friends Geeta, Julie, Muguthan, Subramaniam, Shankry, Suresh, Shalini and Kalim Rahaman for their encouragement towards my research.

Where would I be without my family? My parents deserve special mention for their support and prayers. My father Perumal Kannan a man who show me the joy of intellectual pursuit ever since I was a child. My mother Pushphavalli Muniandy who sincerely raised me up with her carrying and gentle love. Not to be forgotten my brother-in-law Govin @Murali and my elder sister Mahaletchumy who gave me shelter to stay all the while. Sivananthan and Selvambigai thanks for being supportive and carrying siblings.

Finally I would like to thank everybody who was important to the successful realization of this thesis.
ABSTRACT (Bahasa Malaysia)

Dunia digital kini telah lebih maju daripada dekad yang sebelum ini kerana ciptaan dan inovasi yang dibawa melalui perkembangan yang kompleks dalam bidang perkomputeran. Penyelesaian teknologi digital telah terkimpal di dalam kehidupan seharih kita, pembocoran atau kehilangan teknologi maklumat akan membawa kerugian dan malapetaka kepada penguna teknologi tersebut. Dengan keupayaan dan liputan ruang siber yang luas ini telah mewujudkan satu jenayah baru yang dikenali sebagai Jenayah Siber. Seiring dengan perkembangan teknologi maklumat dan jenayah siber, satu soalan utama telah dibangkitkan oleh golongan professional dan pegawai penguatkuasa, “Apakah kaedah yang paling konkrit dan berkesan untuk mendakwa penjenayah siber?” “ Untuk menjawab soalan ini, forensic computer prosedur dan undang-undang siber telah diperkenalkan dan dilaksanakan”. Prosedur forensic komputer di Malaysia masih diperingkat awal dan tidak mempunyai kaedah dan prosedur yang seragam dalam kaedah penyiasatan, antara masalah-masalah yang wujud di dalam jenayah siber adalah seperti bukti yang tidak mencukupi, kaedah “live forensik” yang tidak menepati peraturan, forensic computer dan standard operasi yang tidak seragam. Dengan ketiadaan alat mudah alih yang canggih and mudah digunakan untuk menjalankan “live forensik” pegawai penyiasat forensik digital mengalami masalah seperti bukti “live forensik” tidak dapat dikumpul secara formal atau bukti yang dikumpul tercemar.

Objectif kajian ini adalah untuk memperkenalkan modal forensik digital yang baru. Modal baru yang diperkenalkan adalah untuk memberi tumpuan kepada “live forensic” dan juga “SOP” penyiasatan forensik digital yang kukuh. Untuk memudahkan tugas penyiasatan dan proses pengekstraksian maklumat di lokasi jenayah, satu aplikasi yang berbentuk “GUI” dan mudah alih akan dibangunkan. Dengan kewujudan model dan aplikasi yang berorentasikan “GUI” ini di dalam process penyiasatan forensik digital di Malaysia akan secara langsung manjadikan tugas pegawai penyiasat dan process penyiasatan lebih produktif dan maningkatkan kebolehan dalam pegawai operasi untuk mencari bukti digital yang kukuh dah memperolehnya dengan cara yang paling mudah.
ABSTRACT (English)

The digital world has advanced beyond that was imaginable decades before due to the inventions and innovations brought forth through developments in the complex field of cybertronics. These digital technologies and solutions are now so welded into our lives that the loss or absence of it may possibly mean utter catastrophe to mankind. The computer distinguishes itself and provides a better advantage by presenting the ability to interact with the user via the keyboard and its processed output. The cyberspace with the limitless capabilities it holds made innumerable lives easier as well as more difficult with a dark side known as digital crime. Therefore, due to the growing sophistication of digital crime, the ultimate question raised by professionals and enforcement officers is “What is the most concrete and effective method to prosecute digital criminals?” To answer this question, computer forensic procedures and cyber law have been introduced and implemented. The digital forensics regulation in Malaysia is still in the initial stages not having concise methods and standardized procedures in cybercrime investigation, no attention is being paid over the fragile evidence as live forensic stage is missing in the current digital forensic standard operating procedure. No portable live forensic tool currently being used by digital forensic investigator in Malaysia at the crime scene. The objective of this research is to introduce a new digital forensic model which focuses on live forensic data acquisition stage in digital forensic standard operating procedure and also to develop a handy GUI oriented live forensic data acquisition tool. The methodology used in validating the model and the tool will be by the digital forensic expert user from Malaysia and India. With the existence of this digital forensic model and digital live forensic tool the Malaysian digital forensic investigators will be more productive in accessing the crime scene and also able to effectively acquire the live data and proceed into solving the case.
ABSTRACT (Arabic)

لقد تقدم العالم الرقمي وراء ما كان يمكن تصورها قبل عقود بسبب الاختراعات والابتكارات لأخرج من خلال التطورات في مجال نسبي من cybertronics.

والآن هذه التقنيات الرقمية والحلول المرتبطة بشكل أساسي حتى في حياتنا فأن خسارتها أو عدم وجودها قد يعني كارثة ربما من المنطقت للشركة إلكترونتريبيز نفسه، وتتوفر أفضل المزايا من خلال تقديم النشر على التفاعل مع المستخدم عبر لوحة المفاتيح واتنافها واعطائها في الفضاء الإلكتروني مع قدرات لا حدود لها جعلت من حياة البشر أسهل وفي نفس الوقت كذلك أصبح عن طريق الجانب المظلم الذي يعرف بالجريمة الرقمية. ويرجع ذلك إلى التطور المتزايد للجريمة الرقمية والسؤال الجوهري الذي يفرض نفسه من قبل المتخصصين والمسؤولين عن تنفيذها هو "ما هو الأسلوب الأكثر ملمسية وفعالية لمحاكاة مجري الرقمية؟" للاجابة على هذا السؤال، فقد تم إدخال الكمبيوتر في إجراءات الطب الشرعي وقانون الإنترنت وتنفيذها.

تنظم الطب الشرعي الرقمي في ماليزيا لا يزال في مرحلة الأولية لعدم وجود طرق مختصرة وإجراءات موحدة في تحقيق الجرائم الإلكترونية. فلا يوجد أي اهتمام على نوعية الأدلة البشريه كما يعشق المرحلة الشرعية المفقودة في الطب الشرعي الرقمي الحالي. إجراءات تشغيل قياسية لا يوجد اداة محفزة للبحث في الطب الشرعي المستخدمة حاليا من قبل المحققين من الطب الشرعي الرقمي في ماليزيا في مسرح الجريمة. والهدف من هذا البحث هو تقديم نموذج جديد في الطب الشرعي الرقمي الذي يركز على الأدلة الحية في الطب الشرعي أثناء مرحلة الحصول على البيانات الرقمية. الطب الشرعي يدور على بيانات الطب الشرعي المهنية، التشغيل القياسية أيضاً تطور واجهة المستخدم الرسومية المرجعية بادية للحصول على بيانات الطب الشرعي المعروفة المستخدمة في التحقق من صحة النموذج والأدلة ستكون من قبل الخبر المستخدم للطب الشرعي الرقمي من ماليزيا والهند، مع وجود هذا النموذج في الطب الشرعي الرقمي والأدلة الخاصة يمكن للحصول على نموذج تفتيش وتعليم المحققين الأمثلة والإخراج. و تكون أكثر إنتاجية في الوصول إلى مسرح الجريمة، وقائدة أيضاً على نحو فعال للحصول على بيانات حية، والشروع في حل هذه القضية.
TABLE OF CONTENT

Author Declaration......................................................................................... i 
Biodata of Author........................................................................................ ii 
Acknowledgment.......................................................................................... iii 
Abstract(Bahasa Malaysia)........................................................................... iv 
Abstract(English)........................................................................................ v 
Abstract(Arabic).......................................................................................... vi 
Table of Content........................................................................................ vii 
List of Table................................................................................................ x 
List of Figure................................................................................................. xiii 
List of Appendix.......................................................................................... xvi 
Glossary........................................................................................................ xvii 
List of Acronyms........................................................................................ xxii

CHAPTER I INTRODUCTION
1.1 Introductions To The World of Digital Forensic.................................... 1 
1.2 Incident Response Statistic For Year 2010......................................... 4 
1.3 Forensic Timeline.................................................................................. 6 
1.4 Computer Forensics in Todays World............................................... 7 
1.5 Problem Statements........................................................................... 8 
1.6 Objectives............................................................................................ 10 
1.7 Significance of the Study..................................................................... 11 
1.8 Scope and Limitation.......................................................................... 11 
1.9 Overview of Thesis and Contributions............................................... 11 
1.10 Summary .......................................................................................... 13

CHAPTER II LITERATURE REVIEW
2.1 Introduction.......................................................................................... 14 
2.2 Type of Crime....................................................................................... 16 
2.2.1 Escrow Service Fraud.................................................................... 16 
2.2.2 Harassment via E-mails................................................................. 16 
2.2.3 Cyber Stalking.................................................................................. 17 
2.2.4 Dissemination of Obscene Material (Indecent,Exposure,Pornography).. 18 
2.2.5 Defamation...................................................................................... 19 
2.2.6 Spoofing and Information Phishing.............................................. 20 
2.2.7 Denial of Service........................................................................... 20 
2.2.8 Cyber Terrorism Against the Government Organization................ 21 
2.2.9 E-bombing and Spamming.......................................................... 22 
2.2.10 Unauthorized Access to Computer System or Data.................... 22 
2.2.11 Hacking....................................................................................... 23 
2.2.12 Virus Programmers................................................................. 23 
2.2.13 Theft on Intellectual Property................................................... 23 
2.2.14 Identity Theft.............................................................................. 24
2.2.15 Online Auction Fraud……………………………………………........... 25
2.3 Overall Conclusion About MYCERT Cybercrime Statistics………………….. 32
2.4 Digital Forensic Investigation……………………………………………......... 33
2.5 Various Models Being Presented…………………………………………….... 33
  2.5.1 Single Tier Approach…………………………………………………… 34
  2.5.2 Lee’s Model on Scientific Crime Scene Investigation……………......... 35
  2.5.3 Palmer Model (DFRWS)……………………………………………….. 36
  2.5.4 Abstract Model of Digital Forensic Procedure by Reith, Carr and Gunsch………………………………………………………………….. 37
  2.5.5 An Integrated Digital Investigation Process by Carrier and Spafford….. 38
  2.5.6 Computer Forensic Field Triage Process Model……………………….. 38
2.6 Overall View on the Existing Digital Forensic Model……………………….. 39
2.7 Live Forensic and Toolkit……………………………………………………… 40
  2.7.1 E- Fense Live Response………………………………………………... 40
  2.7.2 Sysinternals Tools…………………………………………………........ 41
  2.7.3 Microsoft COFEE (Computer Online Forensic Evidence Extractors)…. 42
  2.7.4 Forensic Live CD and Live DVD………………………………............. 43
2.8 Overall View on the Existing Digital Live Forensic Tools………………….. 45
2.9 Summary…………………………………………………………………. 45

CHAPTER III DESIGN METHODOLOGY 46
3.1 Introduction…………………………………………………………………… 46
3.2 Stages Involved In Achieving the Objectives......................................... 46
3.3 Stages Involved in Proposing and Designing a Digital Forensic Model……… 47
3.4 Digital Forensic Investigation Tool…………………………………………… 49
3.5 Summary………………………………………………………………........... 53

CHAPTER IV DEVELOPMENT OF DIGITAL FORENSIC FRAMEWORK AND LIVE FORENSIC TOOL 54
4.1 Introduction…………………………………………………………………… 54
4.2 Digital Forensic Model Development .................................................. 55
  4.2.1 Assumption……………………………………………………………… 55
  4.2.2 Authorization…………………………………………………………… 55
  4.2.3 Planning ……………………………………………………………….. 57
  4.2.4 Obtaining of Search Warrant………………………………………… 57
  4.2.5 Identification Seized of Items………………………………………… 57
  4.2.6 Fragile Evidence Identification……………………………………… 57
  4.2.7 Gathering Evidence…………………………………………………… 58
  4.2.8 Transport of Evidence………………………………………………… 58
  4.2.9 Storage and Security………………………………………………….. 58
  4.2.10 Analysis……………………………………………………………….. 58
  4.2.11 Result……………………………………………………………….. 59
  4.2.12 Report Preparation for Court Submission…………………………... 59
  4.2.13 Diffusion of Information…………………………………………......... 59
4.3 Second Stage of Improvement…………………………………………….. …. 59
  4.3.1 Planning……………………………………………………………….. 61
CHAPTER V IMPLEMENTATION & EVOLUTION OF LIVE FORENSIC TOOL

5.1 Introduction

5.2 List of Open Source Digital Forensic Self Executable File

5.2.1 DiskExt
5.2.2 FirePassword
5.2.3 IpConfig
5.2.4 PsService
5.2.5 PsGetSid
5.2.6 PsInfo
5.2.7 PsList
5.2.8 PsLoglist
5.2.9 PsLoggedOn
5.2.10 TCPVCon

5.3 Windows XP PsTools

5.3.1 Arp –a
5.3.2 GetMac
5.3.3 HostName
5.3.4 Netstat
5.3.5 Quser
5.3.6 SystemInfo
5.3.7 Tasklist

5.4 Proposed Integrated Digital Live Forensic Tool

5.5 Live Forensic Tool Complete Operation Use Case Diagram

5.6 Use Case Diagram for Live Forensic Programmer

5.7 Use Case Diagram for Live Forensic Investigator

5.8 Use Case Diagram for Senior Investigation Officer

5.9 Live Digital Forensic Investigation Tool Sequence Diagram

5.10 Live Digital Forensic Investigation Tool Level 0 Diagram

5.11 Outcome of Digital Live Forensic Tool

5.12 Decryption Technique

5.13 Questionnaire Result From CyberSecurity Malaysia

5.14 Questionnaire Result From Royal Malaysian Police

5.15 General opinion from CyberSecurity Malaysia and Cyber Crime & Multimedia Division Team
CHAPTER IX CONCLUSION 156
6.1 Introduction ................................................................. 156
6.2 Research Objective Revisited .......................................... 157
6.3 Future Enhancement & Future Work .................................. 158
6.4 Summary ................................................................. 159
Bibliography .................................................................. 175
LIST OF TABLES
Table 1  Categories of Digital Crime ................................................. 2
Table 2  Different Area of Cybercrime and Their Focus Area............... 3
Table 3  Forensic Timeline From Year 1822 Till Year 2000 .................. 6
Table 4  Illustrates Basic Digital Forensic Stages ............................. 8
Table 5  Complete Digital Forensic Investigation Model .................... 34
Table 6  Comparison of the Each Digital Forensic Model Work Flow .... 40
Table 7  List of PSTOOLS and Its Function ................................. 41
Table 8  List of Live CD Which is Currently Available ...................... 44
Table 9  Objective and the Method Used to Archive the Objective ....... 50
Table 10 Type of Operating System (OS) and the Method of Shutdown.. 67
Table 11 List of Standalone Live Forensic Tool ............................. 69
Table 12 Percentage of Understandability of the Live Forensic Tool
               According to Cyber Security Malaysia Team Members ........ 127
Table 13 Percentage of Completeness of the Live Forensic Tool According
               To Cyber Security Malaysia Team Members .................... 128
Table 14 Percentage of Portability of the Live Forensic Tool According to
               Cyber Security Team Members .................................... 129
Table 15 Percentage of Consistency of the Live Forensic Tool According to
               Cyber Security Malaysia Team Members ........................ 130
Table 16 Percentage of Maintainability of the Live Forensic Tool According
               To Cyber Security Malaysia Team Members .................... 131
Table 17 Percentage of Usability of the Live forensic Tool According to
               Cyber Security Malaysia Team Members ........................ 132
Table 18 Percentage of Reliability of the live forensic tool according to
               Cyber Security Malaysia Team Members ........................ 133
Table 19 Percentage of Efficiency of the Live Forensic Tool According to
               Cyber Security Malaysia Team Members ........................ 134
Table 20 Percentage of Security of the Live Forensic Tool According to
               CyberSecurity Malaysia Team Members ........................ 135
Table 21 Percentage of Understandability of the Digital Live Forensic Tool
               According to Cyber Crime and Multimedia Division Team in
               Royal Malaysian Police ............................................. 137
Table 22 Percentage of Completeness Level of the Digital Live Forensic Tool
               According to Cyber Crime and Multimedia Division Team in
               Royal Malaysian Police ............................................. 138
Table 23 Percentage of Portability Level of the Digital Live Forensic Tool
               According to Cyber Crime and Multimedia Division Team in
               Royal Malaysian Police ............................................. 139
Table 24 Percentage of Consistency Level of the Digital Live Forensic Tool
               According to Cyber Crime and Multimedia Division Team in
               Royal Malaysian Police ............................................. 140
Table 25 Percentage of Maintainability of the Digital Live Forensic Tool
               According to Cyber Crime and Multimedia Division Team in
               Royal Malaysian Police ............................................. 141
Table 26 Percentage of Usability of the Digital Live Forensic Tool
Table 27  Percentage of Reliability of the Digital Live Forensic Tool
According To Cyber Crime and Multimedia Division Team in
Royal Malaysian Police................................................................. 142

Table 28  Percentage of Efficiency of the Digital Live Forensic Tool
According To Cyber Crime and Multimedia Division team in
Royal Malaysian Police................................................................. 143

Table 29  Percentage of Security of the Digital Live Forensic Tool
According to Cyber Crime and Multimedia Division team in Royal
Malaysian Police........................................................................... 144
## LIST OF FIGURE

<table>
<thead>
<tr>
<th>Figure</th>
<th>Description</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Figure 1</td>
<td>General Incident Classification Statistics 2010</td>
<td>4</td>
</tr>
<tr>
<td>Figure 2</td>
<td>General Incident Classification Statistic 2011</td>
<td>5</td>
</tr>
<tr>
<td>Figure 3</td>
<td>Overview of the Thesis Structure</td>
<td>12</td>
</tr>
<tr>
<td>Figure 4</td>
<td>Early Days of Computer Crime till 21st Century</td>
<td>15</td>
</tr>
<tr>
<td>Figure 5</td>
<td>Spam Emails Statistics 2010</td>
<td>27</td>
</tr>
<tr>
<td>Figure 6</td>
<td>Botnet Drones and Malware Infection Statistic 2010</td>
<td>28</td>
</tr>
<tr>
<td>Figure 7</td>
<td>Honeynet Project Related Incidents Statistic 2010</td>
<td>29</td>
</tr>
<tr>
<td>Figure 8</td>
<td>Spam Emails Statistic 2011</td>
<td>30</td>
</tr>
<tr>
<td>Figure 9</td>
<td>Botnet Drones Malware Infection Statistic 2011</td>
<td>31</td>
</tr>
<tr>
<td>Figure 10</td>
<td>Honeynet Project Related Incidents Statistic 2011</td>
<td>32</td>
</tr>
<tr>
<td>Figure 11</td>
<td>Single Tier Framework of Digital Evidence Investigation Process</td>
<td>35</td>
</tr>
<tr>
<td>Figure 12</td>
<td>Lee’s Model on Scientific Crime Scene Investigation</td>
<td>35</td>
</tr>
<tr>
<td>Figure 13</td>
<td>Palmer Model</td>
<td>36</td>
</tr>
<tr>
<td>Figure 14</td>
<td>Abstract Model of Digital Forensic Procedure</td>
<td>37</td>
</tr>
<tr>
<td>Figure 15</td>
<td>Integrated Digital Investigation Process</td>
<td>38</td>
</tr>
<tr>
<td>Figure 16</td>
<td>Computer Forensic Field Triage Process Model</td>
<td>39</td>
</tr>
<tr>
<td>Figure 17</td>
<td>Waterfall Model on Stages Involved in Archiving the New Digital</td>
<td>48</td>
</tr>
<tr>
<td></td>
<td>Forensic Investigation Model</td>
<td></td>
</tr>
<tr>
<td>Figure 18</td>
<td>Simplified Work Flow in Achieving the Objective</td>
<td>52</td>
</tr>
<tr>
<td>Figure 19</td>
<td>First Digital Forensic Investigation Framework</td>
<td>56</td>
</tr>
<tr>
<td>Figure 20</td>
<td>The New Digital Forensic Investigation Model</td>
<td>60</td>
</tr>
<tr>
<td>Figure 21</td>
<td>Approved Final Digital Forensic Investigation Model</td>
<td>64</td>
</tr>
<tr>
<td>Figure 22</td>
<td>Pre Forensic Activity</td>
<td>65</td>
</tr>
<tr>
<td>Figure 23</td>
<td>Seizure and Collection Phase</td>
<td>66</td>
</tr>
<tr>
<td>Figure 24</td>
<td>Evidence Analysis Phase</td>
<td>68</td>
</tr>
<tr>
<td>Figure 25</td>
<td>Sample MD5 Hash Value</td>
<td>72</td>
</tr>
<tr>
<td>Figure 26</td>
<td>Sample Salted MD5 Hash Value</td>
<td>73</td>
</tr>
<tr>
<td>Figure 27</td>
<td>Disk Ext Screenshot Which Have Been Executed Via Command Line</td>
<td>75</td>
</tr>
<tr>
<td>Figure 28</td>
<td>Fire Password Screenshot Which is Being Executed Via Command Line</td>
<td>76</td>
</tr>
<tr>
<td>Figure 29</td>
<td>IPConfig Screenshot That is Being Executed Via Command Line</td>
<td>77</td>
</tr>
<tr>
<td>Figure 30</td>
<td>PsService Screenshot That is Being Executed Command Line</td>
<td>78</td>
</tr>
<tr>
<td>Figure 31</td>
<td>PsGetsid Screenshot That is Being Executed Command Line</td>
<td>79</td>
</tr>
<tr>
<td>Figure 32</td>
<td>PsInfo Screenshot That is Being Executed Command Line</td>
<td>80</td>
</tr>
<tr>
<td>Figure 33</td>
<td>PsInfo - d Screenshot That Was Executed Command Line</td>
<td>81</td>
</tr>
<tr>
<td>Figure 34</td>
<td>PsInfo - s Screenshot That Was Executed Command Line</td>
<td>82</td>
</tr>
<tr>
<td>Figure 35</td>
<td>PsList Screenshot That Was Being Executed Via Command Line</td>
<td>83</td>
</tr>
<tr>
<td>Figure 36</td>
<td>PsList – d Screenshot That Was Executed Via Command Line</td>
<td>84</td>
</tr>
<tr>
<td>Figure 37</td>
<td>PsList – m Screenshot That is Being Executed Via Command Line</td>
<td>85</td>
</tr>
<tr>
<td>Figure 38</td>
<td>PsList – x Screenshot That is Being Executed Via Command Line</td>
<td>86</td>
</tr>
<tr>
<td>Figure 39</td>
<td>PsLoglist Screenshot That is Being Executed Via Command Line</td>
<td>87</td>
</tr>
</tbody>
</table>
Figure 40  PsLoggedOn Screenshot That is Being Executed Via Command Line

Figure 41  TCPVCon Screenshot That is Being Executed Via Command Line

Figure 42  TCPVCon –c Screenshot That is Being Executed Via Command Line

Figure 43  TCPVCon –n Screenshot That is Being Executed Via Command Line

Figure 44  Arp –a Screenshot That is Being Executed via Command Line

Figure 45  GetMac Screenshot That Was Being Executed Via Command Line

Figure 46  HostName Screenshot That Was Being Executed Via Command Line

Figure 47  Netstat Screenshot That is Being Executed Via Command Line

Figure 48  Quser Screenshot That is Being Executed Via Command Line

Figure 49  SystemInfo Screenshot That is Being Executed Via Command Line

Figure 50  Tasklist Screenshot That is Being Executed Via Command Line

Figure 51  Work Flow of the Live Digital Forensic Tool

Figure 52  Complete Use Case Diagram For Proposed Live Forensic Tool

Figure 53  Use Case Diagram For the Live Forensic Programmer

Figure 54  Use Case Diagram for Investigation Officer

Figure 55  Use Case Diagram for Senior Investigation Officer

Figure 56  Live Digital Forensic Investigation Tool Sequence Diagram

Figure 57  Level 0 Diagram for Live Digital Forensic Investigation Tool

Figure 58  Serial Retrieval Program Screenshot

Figure 59  Serial Number Screenshot

Figure 60  Serial Number Implant Process Into the Source Code

Figure 61  The List of File That Need to be Copied Into the Thumb Drive

Figure 62  The Live Forensic EXE in the Thumb Drive

Figure 63  Live Forensic Login Screenshot

Figure 64  Error Message That Popup When Wrong Username or Password Entered

Figure 65  Digital Live Forensic Language Selection Menu

Figure 66  MDS Screenshot From Language Selection Menu Toolbar

Figure 67  Everest Screenshot From Language Selection Menu Toolbar

Figure 68  ‘About Us’ Screenshot From Language Selection Menu Toolbar

Figure 69  Live Forensic Case Note in English

Figure 70  Live Forensic Case Note in Bahasa Malaysia

Figure 71  Live Forensic Case Note in Arabic Language

Figure 72  Case Type Text Field Screenshot

Figure 73  Case Id Text Field Screenshot

Figure 74  Investigator Text Field Screenshot

Figure 75  Case Description Textbox Screenshot

Figure 76  Automated Columns Identify Current Version of Operating System That is Installed

Figure 77  Windows Version Details Screenshot
Figure 78   Two Button That Might be Clicked by the Investigator Based on the Operating System That is Installed in the System…………………………………… 120
Figure 79   Tool is Launching by Itself in Process Box Screenshot………………………… 120
Figure 80   MD5 Checksum Generated by the Live Forensic Tool……………………….. 121
Figure 81   MD5 Checksum Text File Which is Already Encrypted…………………….. 122
Figure 82   MD5 Checksum Decryption Login Screen……………………………………… 123
Figure 83   Displays Live Forensic MD5 Decryption Screen……………………………… 124
Figure 84   Values That Have Already Decrypted………………………………………… 125
Figure 85   Pie Chart With Percentage Based on Understandability Level of Live Forensic Tool………………………………………………………………… 127
Figure 86   Pie Chart with Percentage Based on Completeness Level of Digital Live Forensic Tool……………………………………………………………… 128
Figure 87   Pie Chart with Percentage Based on Portability Level of Digital Live Forensic…………………………………………………………………………… 129
Figure 88   Pie Chart With Percentage Based on Consistency Level of Digital Live Forensic Tool……………………………………………………………… 130
Figure 89   Pie Chart With Percentage Based on Maintainability Level of Digital live Forensic Tool………………………………………………………………… 131
Figure 90   Pie Chart With Percentage Based on Usability Level of Digital Live Forensic Tool…………………………………………………………………… 132
Figure 91   Pie chart With Percentage Based on Reliability Level of Digital Live Forensic Tool…………………………………………………………………… 133
Figure 92   Pie Chart With Percentage Based on Efficiency Level of Digital Live Forensic tool………………………………………………………………………… 134
Figure 93   Pie Chart With Percentage Based on Security Level of Digital Live Forensic Tool…………………………………………………………………… 135
Figure 94   Pie Chart With Percentage Based on Understandability Level of Digital Live Forensic Tool……………………………………………………………… 137
Figure 95   Pie Chart With Percentage Based on Completeness Level of Digital Live Forensic Tool………………………………………………………………… 138
Figure 96   Pie Chart With Percentage Based on Portability Level of Digital Live Forensic Tool…………………………………………………………………… 139
Figure 97   Pie Chart With Percentage Based on Consistency Level of Digital Live Forensic Tool…………………………………………………………………… 140
Figure 98   Pie Chart With Percentage Based on Maintainability Level of Digital Live Forensic Tool………………………………………………………………… 141
Figure 99   Pie Chart With Percentage Based on Usability Level of Digital Live Forensic Tool…………………………………………………………………… 142
Figure 100 Pie Chart With Percentage Based on Reliability Level of Digital Live Forensic Tool…………………………………………………………………… 143
Figure 101 Pie Chart With Percentage Based on Efficiency Level of Digital Live Forensic Tool…………………………………………………………………… 144
Figure 102 Pie Chart With Percentage Based on Security Level of Digital Live Forensic Tool…………………………………………………………………… 145
Figure 103 Research Methodology Used to Archive the Objective………………………… 158
LIST OF APPENDIX

Appendix.1 Information of User Who Logged On Local.......................... 160
Appendix.2 Information On Physical Network and Virtual Network........... 160
Appendix.3 Memory Details on Process Running.................................... 161
Appendix.4 Complete System Loglist.................................................. 162
Appendix.5 Process and Thread Information....................................... 163
Appendix.6 System Information.......................................................... 164
Appendix.7 Random Access Memory, Virtual Memory and Swap Space Details. 164
Appendix.8 Central Processing Unit(CPU) Information............................ 165
Appendix.9 Desktop Properties and Desktop Effects................................ 166
Appendix.10 Physical Drive, Virtual Drive, Folders and Printers That Have Been Shared.......................................................... 166
Appendix.11 Installed Program Details.................................................. 167
Appendix.12 Internet Setting Details..................................................... 168
Appendix.13 Central Processing Unit (CPU) Overclocking Information........ 168
Appendix.14 Wireless Network Interface(WLAN) and Network Interface Card (NIC) Properties......................................................... 169
Appendix.15 Process Name, File Location and Memory That Being Utilize..... 170
Appendix.16 Windows Storage Properties.............................................. 170
Appendix.17 System Drivers Properties................................................ 171
Appendix.18 User Properties & Features.............................................. 171
GLOSSARY

**AccessData**: A leading provider of computer forensic software tools such as FTK and UTK.

**Active Data**: Data existing on the data and file storage media of computer systems. Active data are easily viewed on the operating system or application software that were used to create it and is directly available to users without un-deletion, alteration, or restoration.

**Active Records**: Those records related to current, ongoing or in-process activities and are referred to on a regular basis to respond to day-to-day operational requirements. An active record resides in native application format and is accessible for purposes of business processing with no restrictions on alteration beyond normal business rules.

**Acquisition**: A process by which digital evidence is duplicated, copied, or imaged.

**AES**: Advanced Encryption Standard.

**Analysis**: The third phase of the computer and network forensic process, which involves using legally justify able methods and techniques, to derive useful information that addresses the questions that were the impetus for performing the collection and examination.

**Anti-Forensic**: A technique for concealing or destroying data so that others cannot access it.

**Archival Data**: Data that is not immediately available to the computer user but that the organization preserves for storage and record keeping purposes, often stored on CD-ROMs, tapes, or other electronic storage devices.

**Array**: An enumerated collection of identical entities.

**BIOS**: Basic Input Output System. The set of routines stored in read-only memory that enable a computer to start the operating system and to communicate with the various devices in the system such as disk drives, keyboard, monitor, printer, and communication ports.

**Bit**: A binary digit having a value of 0 or 1.

**Bit Map**: Provides information on the placement and color of individual bits and allows the creation of characters or images by creating a picture composed of individual bits (pixels).
**Bit Stream Backup:** Bit stream backups (also referred to as mirror image backups) involve the backup of all areas of a computer hard disk drive or another type of storage media. Such backups exactly replicate all sectors on a given storage device. Thus, all files and ambient data storage areas are copied. Bit stream backups are sometimes also referred to as “evidence grade” backups and they differ substantially from traditional computer file backups and network server backups.

**Bit Stream Imaging:** A bit-for-bit copy of the original media, including free space and slack space. Also known as disk imaging.

**Byte:** A group of eight bits that is treated either as a single entity or as an array of 8 individual bits.

**Computer Evidence:** Computer evidence is rather unique when compared to other forms of more traditional documentary evidence. Unlike paper documentation, computer evidence is extremely fragile and it occurs in the form of an identical copy of a specific document that is stored in a computer file. In addition, the legal “best evidence” rules differ for the processing of computer evidence. However, there is the potential for unauthorized copies to be made of important computer files without leaving behind a trace that the copy was made. Computer evidence is not limited to data stored in computer files, rather most relevant computer evidence is uncovered in uncommonly known locations. For example, on Microsoft Windows and Windows NT-based computer systems, large quantities of evidence can be found in the Windows swap files or Page Files. In addition, computer evidence can also be uncovered in file slack and unallocated file space.

**Collection:** The first phase of the computer and network forensics process, which involves identifying, labeling, recording, and acquiring data from the possible sources of relevant data, while following guidelines and procedures that preserve the integrity of the data.

**Collision:** For a given function, a pair of distinct input values that yield the same output value.

**Digital Forensics:** The application of science to the identification, collection, examination, and analysis, of data while preserving the integrity of the information and maintaining a strict chain of custody for the data.

**Discovery:** Discovery is the process of identifying, locating, securing and producing information and materials for the purpose of obtaining evidence for utilization in the legal process. The term is also used to describe the process of reviewing all materials which may be potentially relevant to the issues at hand or which may need to be disclosed to other parties, and of evaluating evidence to prove or disprove facts, theories or
allegations. There are several ways to conduct discovery, the most common of which are interrogatories, requests for production of documents and depositions.

**Disc wipe**: Utility that overwrites existing data. Various utilities exist with varying degrees of efficiency some wipe only named files or unallocated space of residual data, thus unsophisticated users who try to wipe evidence may leave behind files of which they are unaware.

**Disk Imaging**: Generating a bit-for-bit copy of the original media, including free space and slack space. Also known as a bit stream image.

**Disk Mirroring**: When files are stored on a computer system’s hard disk, a “mirror” copy is made on an additional hard disk or a separate part of the same disk to safeguard information in the case of a disaster.

**Documentation**: Written notes, audio/videotapes, printed forms, sketches, or photographs that form a detailed record of the scene, evidence recovered, and actions taken during the search of the scene.

**Encase**: A leading industry standard in computer forensic investigation technology. Encase allows investigators to acquire data in a forensically sound manner, and to analyze multiple platforms—Windows, Linux, AIX, OS X, Solaris using a single tool.

**Encryption**: The automated process of hiding data so that no unauthorized people can access them; this is done by means of a procedure (algorithm) and a key. Decryption is the reverse process.

**ESDI (Enhanced Small Device Interface)**: A defined, common electronic interface for transferring data between computers and peripherals, particularly disc drives.

**Evidence**: Testimony whether oral, documentary or real, which may legally be received to prove or disprove some fact in dispute.

**Examination**: The second phase of the computer and network forensics process, which involves forensically processing large amounts of collected data using a combination of automated and manual methods to assess and extract data of particular interest, while preserving the integrity of the data.

**Extended Partitions**: If a computer hard drive has been divided into more than four partitions, extended partitions are created. Under such circumstances each extended partition contains a partition table in the first sector that describes how it is further subdivided.

**Forensics**: Computer forensics is the scientific examination and analysis of data held on, or retrieved from, computer storage media in such a way that the information can be used
as evidence in a court of law. It may include the secure collection of computer data; the examination of suspect data to determine details such as origin and content; the presentation of computer based information to courts of law; and the application of a country’s laws to computer practice. Forensics may involve recreating “deleted” or missing files from hard drives, validating dates and logged in authors or editors of documents, and certifying key elements of documents or hardware for legal purposes.

Harvesting: The process of retrieving or collecting electronic data from storage media or devices; an EDiscovery vendor “harvests” electronic data from computer hard drives, file servers, CDs, and backup tapes for processing and load to storage media or a database management system.

Hash: An algorithm that creates a value to verify duplicate electronic documents. A hash mark serves as a digital thumb print.

IP address (Internet Protocol Address): A string of four numbers separated by periods used to represent a computer on the Internet—a unique identifier for the physical location of the server containing the data.

MD5 Hash: An algorithm created in 1991 by Professor Ronald Rivest that is used to create digital signatures (i.e., fingerprints) of storage media such as a computer hard drive. When this algorithm is applied to a hard drive then it creates a unique value. Changing the data on the disk in any way will change the MD5 value.

Message Authentication Code (MAC): A bit string of fixed length, computed by a MAC generation algorithm, that is used to establish the authenticity and, hence, the integrity of a message.

Message Digest: A hash that uniquely identifies data. Changing a single bit in the data stream used to generate the message digest will yield a completely different message digest.

Metadata: Metadata are information about a particular data set or document which describes how, when and by whom it was collected, created, accessed, modified and how it is formatted. Can be altered intentionally or inadvertently. Can be extracted when native files are converted to image. Some metadata, such as file dates and sizes, can easily be seen by users; other metadata can be hidden or embedded and unavailable to computer users who are not technically adept. Metadata are generally not reproduced in full form when a document is printed.

Operating System (OS): An Operating system provides the software platform which directs the overall activity of a computer, network or system, and on which all other software programs and applications can run. In many ways, choice of an operating system will effect which applications can be run. Operating systems perform basic tasks, such as recognizing input from the keyboard, sending output to the display screen,
keeping track of files and directories on the disc and controlling peripheral devices such as disc drives and printers. For large systems, the operating system has even greater responsibilities and powers—becoming a traffic cop to makes sure different programs and users running at the same time do not interfere with each other.

**RAM (Random Access Memory):** Hardware inside a computer that retains memory on a short term basis and stores information while the computer is in use. It is the “working memory” of the computer into which the operating system, startup applications and drivers are loaded when a computer is turned on, or where a program subsequently started up is loaded, and where thereafter, these applications are executed. RAM can be read or written in any section with one instruction sequence. It helps to have more of this “working space” installed when running advanced operating systems and applications. RAM content is erased each time a computer is turned off.

**Steganography:** The art and science of communicating in a way that hides the existence of the communication. It is used to hide a file inside another. For example, a child pornography image can be hidden inside another graphic image file, audio file, or other file format.
<table>
<thead>
<tr>
<th>Acronym</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>ADS</td>
<td>Alternate Data Stream</td>
</tr>
<tr>
<td>ARIN</td>
<td>American Registry for Internet Numbers</td>
</tr>
<tr>
<td>ARP</td>
<td>Address Resolution Protocol</td>
</tr>
<tr>
<td>ASCII</td>
<td>American Standard Code for Information Interchange</td>
</tr>
<tr>
<td>ATA</td>
<td>Advanced Technology Attachment</td>
</tr>
<tr>
<td>BIOS</td>
<td>Basic Input/Output System</td>
</tr>
<tr>
<td>CCIPS</td>
<td>Computer Crime and Intellectual Property Section</td>
</tr>
<tr>
<td>CD</td>
<td>Compact Disc</td>
</tr>
<tr>
<td>CD-R</td>
<td>CD-Recordable</td>
</tr>
<tr>
<td>CD-ROM</td>
<td>CD-Read Only Memory</td>
</tr>
<tr>
<td>CD-RW</td>
<td>CD-Rewritable</td>
</tr>
<tr>
<td>CDFS</td>
<td>CD File System</td>
</tr>
<tr>
<td>CFI</td>
<td>Computer and Financial Investigations</td>
</tr>
<tr>
<td>CFRDC</td>
<td>Computer Forensics Research and Development Center</td>
</tr>
<tr>
<td>CFTT</td>
<td>Computer Forensics Tool Testing</td>
</tr>
<tr>
<td>CMOS</td>
<td>Complementary Metal Oxide Semiconductor</td>
</tr>
<tr>
<td>CVE</td>
<td>Common Vulnerabilities and Exposures</td>
</tr>
<tr>
<td>DoD</td>
<td>Department of Defense</td>
</tr>
<tr>
<td>DVD</td>
<td>Digital Video Disc or Digital Versatile Disc</td>
</tr>
<tr>
<td>DVD-R</td>
<td>DVD-Recordable</td>
</tr>
<tr>
<td>DVD-ROM</td>
<td>DVD-Read Only Memory</td>
</tr>
<tr>
<td>DVD-RW</td>
<td>DVD-Rewritable</td>
</tr>
<tr>
<td>ESP</td>
<td>Encapsulating Security Payload</td>
</tr>
<tr>
<td>ext2fs</td>
<td>Second Extended File system</td>
</tr>
<tr>
<td>ext3fs</td>
<td>Third Extended File system</td>
</tr>
<tr>
<td>FAT</td>
<td>File Allocation Table</td>
</tr>
<tr>
<td>FBI</td>
<td>Federal Bureau of Investigation</td>
</tr>
<tr>
<td>FIPS</td>
<td>Federal Information Processing Standards</td>
</tr>
<tr>
<td>F.I.R.E.</td>
<td>Forensic and Incident Response Environment</td>
</tr>
<tr>
<td>FISMA</td>
<td>Federal Information Security Management Act</td>
</tr>
<tr>
<td>FTP</td>
<td>File Transfer Protocol</td>
</tr>
<tr>
<td>GB</td>
<td>Gigabyte</td>
</tr>
<tr>
<td>GUI</td>
<td>Graphical User Interface</td>
</tr>
<tr>
<td>HFS</td>
<td>Hierarchical File System</td>
</tr>
<tr>
<td>HPA</td>
<td>Host Protected Area</td>
</tr>
<tr>
<td>HPFS</td>
<td>High-Performance File System</td>
</tr>
<tr>
<td>HTCIA</td>
<td>High Technology Crime Investigation Association</td>
</tr>
<tr>
<td>HTTP</td>
<td>Hypertext Transfer Protocol</td>
</tr>
<tr>
<td>IACIS</td>
<td>International Association of Computer Investigative Specialists</td>
</tr>
<tr>
<td>Acronym</td>
<td>Description</td>
</tr>
<tr>
<td>---------</td>
<td>-------------</td>
</tr>
<tr>
<td>ICMP</td>
<td>Internet Control Message Protocol</td>
</tr>
<tr>
<td>IDE</td>
<td>Integrated Drive Electronics</td>
</tr>
<tr>
<td>IDS</td>
<td>Intrusion Detection System</td>
</tr>
<tr>
<td>IGMP</td>
<td>Internet Group Management Protocol</td>
</tr>
<tr>
<td>IM</td>
<td>Instant Messaging</td>
</tr>
<tr>
<td>IMAP</td>
<td>Internet Message Access Protocol</td>
</tr>
<tr>
<td>IOS</td>
<td>Internetwork Operating System</td>
</tr>
<tr>
<td>IP</td>
<td>Internet Protocol</td>
</tr>
<tr>
<td>IPsec</td>
<td>Internet Protocol Security</td>
</tr>
<tr>
<td>ISO</td>
<td>International Organization for Standardization</td>
</tr>
<tr>
<td>ISP</td>
<td>Internet Service Provider</td>
</tr>
<tr>
<td>IT</td>
<td>Information Technology</td>
</tr>
<tr>
<td>JPEG</td>
<td>Joint Photographic Experts Group</td>
</tr>
<tr>
<td>KB</td>
<td>Kilobyte</td>
</tr>
<tr>
<td>MAC</td>
<td>Media Access Control</td>
</tr>
<tr>
<td>MAC</td>
<td>Modification, Access, and Creation</td>
</tr>
<tr>
<td>MB</td>
<td>Megabyte</td>
</tr>
<tr>
<td>MD</td>
<td>Message Digest</td>
</tr>
<tr>
<td>MMC</td>
<td>Multimedia Card</td>
</tr>
<tr>
<td>MS-DOS</td>
<td>Microsoft Disk Operating System</td>
</tr>
<tr>
<td>NFAT</td>
<td>Network Forensic Analysis Tool</td>
</tr>
<tr>
<td>NIJ</td>
<td>National Institute of Justice</td>
</tr>
</tbody>
</table>
Reference


Ayers, R. and W. Jansen (2004). PDA forensic tools: An overview and analysis, NASA Center for AeroSpace Information, 7121 Standard Dr, Hanover, Maryland, 21076-1320, USA.


Delp, E. J. and P. W. Wong Security, steganography, and watermarking of multimedia contents VII(San Jose CA, 17-20 January 2005), SPIE.


