

CHALLENGES IN WINDOWS 8 OPERATING SYSTEM FOR DIGITAL FORENSIC INVESTIGATIONS

TINGTING GOH, BBus

A thesis submitted to the Faculty of Design and Creative Technologies
Auckland University of Technology
in partial fulfilment of the
requirements for degree of
Masters of Forensic Information Technology

School of Computer and Mathematical Sciences

Auckland, New Zealand

2014

Declaration

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

TingTing Goh

Acknowledgements

This thesis was completed at the Faculty of Design and Creative Technologies in the School of Computing and Mathematical Sciences at Auckland University of Technology, New Zealand. During the course of this research project, I have received support and advice from many people in one way or another.

I would like to thank my family, friends and colleagues for providing support and encouragement when working on the thesis as well as throughout my entire post graduate study. I would also like to thank my thesis supervisor Professor Brian Cusack for his guidance throughout the thesis project. Also the assistance from several proof readers is acknowledged.

Abstract

Windows 8 was released in October 2012 and was followed by Windows 8.1 in October 2013. It was hypothesised that the improvements in Windows 8 and new features of Windows 8 may cause new challenges to Digital Forensic investigation. Similarly, the forensic techniques that worked perfectly on the past version of Windows might require changes when dealing with a Windows 8 machine.

The objective of the research was hence to find out the investigation challenges of the new features in Windows 8 that could impact on the Digital Forensic investigation process. The research focuses on the Digital Forensic investigation process gap when dealing with the new version of the operating system.

The research first started by reviewing the past Windows platforms with a focus on comparing Windows 7 and Windows 8 to identify the differences. Digital Forensic areas such as Digital Forensic tools and existing Digital Forensic model were also explored. The problem areas related to Digital Forensic techniques, Windows 8 Digital Forensic issues, and Windows 8 features issues were identified. The reviews were narrowed down to review the gap in research in one area. Then the main research question and sub questions for the research were constructed. The main questions chosen for the research was “What new features in Windows 8 Operating System pose new challenges to the Digital Forensic investigation?” The hypotheses of the research were also defined for testing before the methodology was introduced in order to conduct the experiments to answer the research question and also test the hypothesis.

The research phases followed the six phases “Preparation, Incident Response, Data Collection, Data Analysis, the Report and Incident Closure”. Each of the phases was recorded and the results of the findings were used to assist in answering the research questions. Based on the findings, the three new features in Windows 8 of significance were the secure boot, after reset option and communication applications. These features, in Windows 8 were found to bring new challenges for Digital Forensic investigations.

Table of Contents

Formalities

| | |
|-------------------------|-----|
| Declaration..... | i |
| Acknowledgements | ii |
| Abstract..... | iii |
| Table of Contents | iv |
| List of Tables | x |
| List of Figures | xii |

Chapter 1 – Introduction

| | |
|-----------------------------------|---|
| 1.0 INTRODUCTION | 1 |
| 1.1 PROBLEM AREAS | 2 |
| 1.2 MOTIVATION | 3 |
| 1.3 STRUCTURE OF THE THESIS | 5 |

Chapter 2 – Literature Review

| | |
|--|----|
| 2.0 INTRODUCTION | 8 |
| 2.1 REVIEW OF WINDOWS 7 RESEARCH | 9 |
| 2.1.1. History of Windows Platform | 9 |
| 2.1.2. Review of Windows 7 Platform | 11 |
| 2.1.3. Forensic Benefits Areas in Windows 7..... | 12 |
| 2.1.4. Forensic Problems Areas in Windows 7..... | 14 |
| 2.2 REVIEW OF WINDOWS 8 RESEARCH | 16 |
| 2.2.1. Windows 8 Consumer Review | 17 |
| 2.2.2. Windows 8 Consumer Review Advantages..... | 17 |
| 2.2.3. Windows 8 Consumer Review Disadvantages..... | 18 |
| 2.2.4. Differences Between Windows 7 and Windows 8 | 19 |
| 2.3 WINDOWS 8 NEW FEATURES | 20 |

| | | |
|---------|---|----|
| 2.3.1. | Language and Standards Support | 20 |
| 2.3.2. | Windows Store | 21 |
| 2.3.3. | User Login..... | 22 |
| 2.3.4. | Microsoft Account Integration | 22 |
| 2.3.5. | File Explorer..... | 23 |
| 2.3.6. | Internet Explorer..... | 23 |
| 2.3.7. | Task Manager | 24 |
| 2.3.8. | File History..... | 26 |
| 2.3.9. | Hardware Support..... | 27 |
| 2.3.10. | Hybrid Boot..... | 28 |
| 2.3.11. | Installation..... | 29 |
| 2.3.12. | Networking..... | 29 |
| 2.3.13. | Repair Recovery | 30 |
| 2.3.14. | Security | 32 |
| 2.3.15. | Video Subsystem..... | 33 |
| 2.3.16. | Windows To Go | 33 |
| 2.3.17. | Hyper-V | 34 |
| 2.3.18. | Storage Spaces..... | 34 |
| 2.4 | WINDOWS 8 FORENSIC RESEARCH..... | 35 |
| 2.4.1. | Windows 8 Forensic Professionals Review | 35 |
| 2.4.2. | Windows 8 Digital Forensic Investigation Process..... | 37 |
| 2.4.3. | Windows 8 Forensic Tools and Techniques | 40 |
| 2.5 | EXISTING DIGITAL FORENSIC MODEL..... | 42 |
| 2.6 | LATEST DEVELOPMENT IN WINDOWS 8 OPERATING SYSTEM. 45 | |
| 2.7 | CONCLUSION | 46 |

Chapter 3 – Methodology

| | | |
|--------|--|----|
| 3.0 | INTRODUCTION..... | 48 |
| 3.1 | REVIEW OF ISSUES AND PROBLEMS | 50 |
| 3.1.1. | Review Past Windows Platform Digital Forensic Issues And Problems | 50 |
| 3.1.2. | Review of Current Windows 8 Issues And Problems | 54 |

| | | |
|--------|--|----|
| 3.1.3. | Review of Windows 8 Digital Forensic Issues And Problems | 57 |
| 3.1.4. | Review of Windows 8 New Features Issues and Problems | 59 |
| 3.2 | SELECTION OF RESEARCH PROBLEM | 60 |
| 3.2.1. | Relevance Past Windows Platform Issues And Problems | 61 |
| 3.2.2. | Relevance Current Issues And Problems in Windows 8 | 63 |
| 3.2.3. | Relevance Windows 8 Digital Forensic Issue And Problems..... | 64 |
| 3.2.4. | Relevance Issues And Problems In Windows 8 New Features..... | 65 |
| 3.3 | RESEARCH QUESTION AND HYPOTHESIS | 65 |
| 3.3.1. | Review of Challenges in Windows 8 New Features For Digital Forensic Investigation | 66 |
| 3.3.2. | Research Question And Sub Questions | 66 |
| 3.3.3. | Hypothesis..... | 67 |
| 3.4 | RESEARCH DESIGN | 68 |
| 3.4.1. | Case Based Reasoning | 68 |
| 3.4.2. | The Digital Forensic Process | 69 |
| 3.4.3. | Research Phases | 70 |
| 3.4.4. | Data Map..... | 72 |
| 3.4.5. | Pilot Test | 73 |
| 3.5 | DATA REQUIREMENT | 74 |
| 3.6 | DATA COLLECTION | 74 |
| 3.7 | DATA ANALYSIS | 76 |
| 3.8 | LIMITATIONS OF RESEARCH | 77 |
| 3.9 | CONCLUSION | 78 |

Chapter 4 – Research Findings

| | | |
|--------|--|----|
| 4.0 | INTRODUCTION | 80 |
| 4.1 | ALTERATION IN RESEARCH PHASES | 81 |
| 4.1.1. | Data Requirement | 81 |
| 4.1.2. | Data Collection..... | 82 |
| 4.1.3. | Data Analysis | 83 |
| 4.1.4. | Pilot Test | 84 |
| 4.2 | Preparation Phase of Data for Windows 8 Machine..... | 84 |

| | | |
|----------|---|-----|
| 4.2.1. | Equipment Available | 84 |
| 4.2.2. | Windows 8 Operating System Forensic Techniques..... | 86 |
| 4.2.3. | Windows 8 Operating System Forensic Tools..... | 87 |
| 4.2.4. | Windows 8 Operating System Data..... | 88 |
| 4.3 | Incident Response Phase For Windows 8 Machine Acquisition..... | 90 |
| 4.3.1. | Scenario for Windows 8 Machine Acquisition | 90 |
| 4.3.1.1. | Before Recovery Machine | 91 |
| 4.3.1.2. | After-Refresh Machine | 91 |
| 4.3.1.3. | After-Reset Machine..... | 91 |
| 4.3.2. | Windows 8 Machine Upgrade to Windows 8.1 Changes | 92 |
| 4.3.3. | Windows 8 Recovery Options..... | 92 |
| 4.4 | Data Collection Phase For Windows 8 Machine Acquisition..... | 93 |
| 4.4.1. | Imaging Windows 8 Pre-Recovery Machine | 93 |
| 4.4.2. | Imaging Windows 8 After-Refresh Machine..... | 93 |
| 4.4.3. | Imaging Windows 8 After-Reset Machine | 94 |
| 4.4.4. | Data Verifying and Processing for Windows 8 Machine | 94 |
| 4.5 | Analysis Phase For Windows 8 Machine Acquisition | 94 |
| 4.5.1. | Data Existence For Different Recovery Options on Windows 8 Machine | 95 |
| 4.5.1.1. | EFI System Partition..... | 96 |
| 4.5.1.2. | The Recovery Partition | 98 |
| 4.5.1.3. | Microsoft Reserved Partition | 99 |
| 4.5.1.4. | Operating System Partition | 100 |
| 4.5.1.5. | NTFS Partition | 102 |
| 4.5.1.6. | Data Partition | 102 |
| 4.5.1.7. | Restore Partition..... | 103 |
| 4.5.2. | Tools Effectiveness For Confirmatory Analysis on Windows 8 Machine | 104 |
| 4.5.2.1. | FTK Imager..... | 104 |
| 4.5.2.2. | Encase V7 | 105 |
| 4.5.2.3. | Bulk Extractor | 106 |
| 4.5.2.4. | Registry Ripper | 106 |
| 4.5.2.5. | Registry Decoder | 107 |

| | | |
|-----------|--|-----|
| 4.5.3. | Potential Evidence For Event Reconstruction on a Windows 8 Machine | 107 |
| 4.5.3.1. | Keywords Search..... | 108 |
| 4.5.3.2. | Website Visited | 108 |
| 4.5.3.3. | Emails Sent and Received..... | 109 |
| 4.5.3.4. | Pictures Saved On My Document Folders..... | 109 |
| 4.5.3.5. | SkyDrive’s Documents Synchronizing..... | 110 |
| 4.5.3.6. | Calendars Entries..... | 110 |
| 4.5.3.7. | Word Documents Saved In My Documents Folder | 111 |
| 4.5.3.8. | Messaging Text Sent And Received..... | 111 |
| 4.5.3.9. | Installed Applications | 112 |
| 4.5.3.10. | Microsoft Store Applications | 113 |
| 4.6 | CONCLUSION | 114 |

Chapter 5 – Research Discussions

| | | |
|----------|---|-----|
| 5.0 | INTRODUCTION | 116 |
| 5.1 | Answering Of Research Sub Questions | 116 |
| 5.1.1. | Data Existence And Hypothesis Test | 117 |
| 5.1.2. | Tools Efficiency And Hypothesis Test..... | 119 |
| 5.1.3. | Event Reconstruction And Hypothesis Test | 121 |
| 5.2 | Discussion of Research Main Question | 123 |
| 5.2.1. | Data Existence On Different Recovery Options | 123 |
| 5.2.2. | Tools Efficiency For Windows 8 Investigation | 124 |
| 5.2.3. | Event Reconstruction From Potential Evidence Acquired | 125 |
| 5.2.4. | New Features Challenges..... | 125 |
| 5.2.4.1. | Secure Boot..... | 126 |
| 5.2.4.2. | Reset Functions | 126 |
| 5.2.4.3. | Communications Applications | 127 |
| 5.2.5. | Answers To Main Research Question | 128 |
| 5.3 | Discussion Of Findings..... | 131 |
| 5.3.1. | Data Existence | 132 |
| 5.3.2. | Tools Capability | 133 |

5.3.3. Event Reconstruction..... 134
5.3.4. Digital Forensic Challenges 138
5.4 Recommendation..... 140
5.4.1. Bypass Secure Boot Technique For Better Integrity 140
5.4.2. Combining Different Tools For Better Analysis Results..... 141
5.4.3. Forensic Readiness For After Reset Machine 141
5.5 CONCLUSION 142

Chapter 6 – Conclusion

6.0 INTRODUCTION 144
6.1 SUMMARY OF FINDINGS 145
6.2 LIMITATIONS OF THE RESEARCH 147
6.3 RECOMMENDATION SUMMARY 148
6.4 FUTURE RESEARCH 148
6.5 CONCLUSION 149

References List

References..... 151

Appendices

APPENDIX A: EQUIPMENT SETUP ENVIRONMENT..... 165
APPENDIX B: FINDINGS SCREENSHOT 165
APPENDIX C: POTENTIAL EVIDENCE DATA INTEGRITY..... 174

List of Tables

| | |
|--|-----|
| Table 2.1: Highlights From the First 25 Years | 10 |
| Table 2.2: Review New Features in Windows 7..... | 12 |
| Table 2.3: Forensic Artifacts Location In Windows 7 Files System | 13 |
| Table 2.4: IE Private Browsing Forensic Implications | 16 |
| Table 2.5: Comparing the differences in Windows 7 and Windows 8 | 19 |
| Table 2.6: GUID command line Table A | 23 |
| Table 2.7: Tab in Windows 8 Task Manager and their impact to Digital Forensic investigation..... | 25 |
| Table 2.8: Comparison Windows 8 and Windows 7 hardware support requirements..... | 27 |
| Table 2.9: Elements Preserved and returned to default state..... | 31 |
| Table 2.10: Potential evidence found in Windows Operating System..... | 39 |
| Table 2.11: Summary of tools reviewed for Windows 8 Digital Forensic Investigation..... | 41 |
| Table 2.12: Comparison of three existing Forensic model..... | 42 |
| Table 3.1: Data Acquisition Problem & Issues..... | 51 |
| Table 3.2: Digital Forensic Analysis Problems & Issues | 53 |
| Table 3.3: Windows Artifact Analysis Cheat Sheet..... | 61 |
| Table 3.4: Case-based Reasoning Process for This Research | 69 |
| Table 3.5: Windows 8 Research Phases Objectives..... | 70 |
| Table 4.1: Equipment Available | 85 |
| Table 4.2: Microsoft Account..... | 85 |
| Table 4.3: Tools Chosen For Research | 87 |
| Table 4.4: Operating System Data Created | 89 |
| Table 4.5: Partition Type | 95 |
| Table 4.6: Items of Artifacts | 96 |
| Table 4.7: EFI system partition..... | 97 |
| Table 4.8: Recovery Partition | 98 |
| Table 4.9: Microsoft Reserved Partition | 99 |
| Table 4.10: Operating System Partition | 100 |
| Table 4.11: NTFS Partition..... | 102 |
| Table 4.12: Data Partition..... | 103 |

| | |
|---|-----|
| Table 4.13: Restore Partition | 103 |
| Table 4.14: Microsoft Store Applications | 113 |
| Table 5.1: Data Existence And Hypothesis Test | 117 |
| Table 5.2: Tools Efficiency And Hypothesis Test | 119 |
| Table 5.3: Event Reconstruction and Hypothesis Test | 121 |
| Table 5.4: New Features Challenges and Hypothesis Test | 128 |
| Table 5.5: Comparison of Data in Partitions | 133 |
| Table 5.6: Tools Capability Summary | 134 |
| Table 5.7: Event Reconstruction Method for Potential Evidence | 134 |

List of Figures

| | |
|--|----|
| Figure2.1: Data Stored during InPrivate Session..... | 15 |
| Figure2.2: Windows 8 Platform and Tools slide shared at Build Conference | 21 |
| Figure2.3: Representation of different phases between cold boot and fast start up | 28 |
| Figure2.4: GUID subkey information | 37 |
| Figure2.5: Digital Crime Scene Investigation Process..... | 38 |
| Figure3.1: Approach for each research phases | 49 |
| Figure3.2: Data Map for Windows 8 Research | 73 |
| Figure3.3: Data Analysis Guide for Windows 8 Research..... | 76 |
| Figure 4.1: Forensic Techniques with Equipment Available to Acquire Potential Evidence on Laptop..... | 86 |

Chapter 1 – Introduction

1.0 INTRODUCTION

At the age of a great information explosion anyone who controls the internet has great power. Control comes through information and computer networks provide users the accessibility to many digital resources on online. Computer improvements have allowed its users to be more productive and informative rich, particularly with the access to communicate freely on the internet (Berkeley Law, 2003). Large Corporations like Microsoft created information opportunities and is well known for its many versions of Windows operating systems (Kooten, 2011). Bright (2013a) reported that Windows 8 after being released for 6 months had sold 100 million licenses and during the same time frame 250 million applications were downloaded. There is still a rising popularity for Windows based system as described in Microsoft case studies that depict the transition to Windows 8. The application programming interfaces allow users to enhance their mobility and boost productivity in and out of the office (Microsoft Case Studies, 2013). Similarly, in another report by Bertolucci (2010), on user's contentment with Microsoft products many users were happy with Windows 7 and the customer satisfaction with PCs has increase for another 4% to 78%. The results could mean that eventually these Windows 7 users will move up to the Windows 8 operating system. Microsoft Windows being one of the most acknowledged operating system with many computer users worldwide would also be a perfect target for an attacker (Forensic KB, 2011). The attackers doesn't only focus on small and large organisations but also the government sector and non-profit sectors. Attackers can gain access to sell personal data and credit card information stored on the database (Microsoft Business, 2013). The addition of Windows 8 will eventually replace the most of the Windows 7 version and Microsoft were urging users and organisations to upgrade to Windows 8 in order to protect against the cyber security threats by making sure that data are secure with the latest hardware and software technologies.

The improvements in Windows 8 by adding new features may cause new challenges to Digital Forensic investigation and the techniques that worked in the past might require certain changes when dealing with Windows 8 machines. There was little literature on Windows 8 forensic however most of the articles reviewed had done testing on the preview version of Windows 8 and also with Windows 8 images on virtual machines. This creates a new problem area as it is uncertain how the actual scenario for Digital Forensic investigation processes will be when dealing with a brand new machine that already has Windows 8 installed. Section 1.1 outlines the problem areas and how they eventually built up to the main question of the research. Section 1.2 will focus on the motivation for the research. Section 1.3 will conclude with the thesis structure.

1.1 PROBLEM AREAS

For windows forensic there are a wide variety of problems that can be researched given that the process of Digital Forensic investigation has matured over the years to build up an efficient Digital Forensic model. The understanding of the problem areas of each Digital Forensic investigation method was defined from the past Windows operating system investigations. These are discussed in more details in chapter 2 the literature review and chapter 3 sections to review the problem areas when selecting a suitable main research question. The problem areas raised from each phase of digital investigation requirements can be identified. The various challenges that were discovered through the process can be managed to ensure the availability of the data for successful prosecution of a crime that can occur on any of the digital devices. Windows 8 the successor of Windows 7 will be implemented as the research platform for a new computer, a laptop, a mobile device and a tablet. That would mean that in general Windows 8 will be built on the many new technologies available to the market and that would introduce new features which could bring in new challenges especially to the Digital Forensic investigation (Rosenblatt, 2012). One of the new features will be the recovery options that would be accessible by all users to refresh the setting of a default or to reset their machine back to factory settings. In the user's perspective these new

features have a simple purpose such as trying to solve a user setting problem or just wanting to pass on the machine to another person so the intention was to just remove the files that were no longer needed anymore. However in the Digital Forensic perspective, it would actually have potential to destroy the evidence that may actually be crucial to a case (Johnson, 2012a). There still needs to develop a full understanding about the implications of the new features of Windows 8 for Digital Forensic investigation processes and to have a better picture of the actual problem areas related to Windows 8 machines. The research process will look into the problem area as to the amount of data that can be actually collected after the recovery option is performed on a machine by performing an actual scenario applied to a Digital Forensic data acquisition after the recovery option is attempted. The other problem area that will be covered in this research will be the attempt to analyse the data acquired with tools compatible for Windows 8 to find out the actual challenges that a Digital Forensic investigator could face when conducting Digital Forensic examinations on a system with new features that are different from the previous operating systems. The research is to fill a gap in the literature and provide an update to the current problem areas with new information found when conducting Digital Forensic investigation on machines installed with Windows 8. Also the research will observe any other Digital Forensic processes that are required to further look into the challenges of the Windows 8 new features.

1.2 MOTIVATION

The motivation of the research was to research the Digital Forensic investigation process gap when dealing with new types of operating system. It was understood that the world is not a safe place as many crimes occur using new computer technologies and particularly when new ones are released. A computer misuse act was introduced in 1990 and under the act hacking and viruses related criminal activity was an offense in the US. The act was to make provision for securing computer material against unauthorised access or modification, to require or

authorised the taking of measures to ensure cyber security, and for matters related thereto (Ellis-Christensen, 2013). Most well-known operating systems had minimal defences against any intruders, and the cyber security law was there to protect any victim that was harmed by any computer related crime and hence changes had to be made by software companies. The impact of computer crime was overwhelming and the motivation of cybercrime was targeted not only to property or governments but also against a person. Computer crime brings a real threat to society that could result in massive losses in profit and cause hindrance for jobs to function effectively (Babu & Parishat, 2004).

The evolution of computer devices means that most communication made between one person to another will be done in digital form and the better way to establish an event will be based on the digital evidence. Therefore, in a place with digital devices available to be utilized by people there will also be evidence left behind by people from their actions and activities (Sommer, 2012). If a crime associated with computer technologies is suspected then a Digital Forensic investigation will be required to be used in order to reconstruct the event and to uncover the person responsible for the crime (Rouse, 2007). The objectives of computer forensic techniques as interpreted by Strickland (2011), was to undertake an inquiry, preserving and analysing data on a computer system to hunt for potential digital evidence in order to be successful used in a court of law (Strickland, 2011). To allow potential evidence to be valid in the court of law which means the evidence must be obtained in a forensically sound manner which Murr (2006) makes clear that evidence must not be altered by any of the acquisition tools, using any techniques and during processing.

The motivation of the research was to find out any new challenges present on Windows 8 operating system when attempting to recover computer data that was hidden, deleted, damaged or lost in order to assist with the legal professional in litigation should a case related to the Windows 8 machine happen (Virtue, 2003). The higher chance to be success in a litigation case or a favorable prosecution of a criminal case related to a computer device will depend greatly on the availability of potential evidence collected during the Digital Forensic acquisition (Sommer, 2012). The Windows 8 operating system could be one of

the most widely used operating systems for computer users in the coming years, so therefore the research in these areas will be practical for Digital Forensic investigators as well as IT professionals who should review the new features on Windows 8 machines and make improvements to the IT Policies with implementation for forensic readiness.

1.3 STRUCTURE OF THE THESIS

In this thesis there will be six chapters. In chapter 1 the introduction to the research and problem areas are identified. Next is the motivation of the research that is to identify the possible gap when dealing with new types of operating system. In the chapter 2 literature review the objectives were to review related articles on Windows platforms and Digital Forensic areas. The chapter reviews the Windows 7 features and the Windows 8 new features. The forensic implications of the Windows 7 show the advantages and disadvantages that are discussed in section 2.1. Articles related to Windows 8 were reviewed in section 2.2 based on the current consumer reviews together with the advantages and disadvantages of the Windows 8 system. Windows 8 new features were reviewed in section 2.3 to understand more about the changes made in the Windows 8 operating system. Digital Forensic reports of past researchers are reviewed in section 2.4 to explore and to see whether Digital Forensic tools and Digital Forensic models can be fitted into the Windows 8 research. The existing Digital Forensic models were reviewed in section 2.5 and latest development in Windows 8 operating system in section 2.6.

In chapter 3 the problem areas and issues are review based on the past research done with Windows Forensic. Section 3.1 reviews the issues and problems of the Windows platform Digital Forensic by looking at the various challenges that happened during data acquisition stage and also during analysing of Digital Forensic evidences. The section will then review the differences with Windows 8 such as user interface issues, security issues, new features and Digital Forensic issues. The next section in chapter 3.2 will narrow down the issues and problems that were raised in the previous section by selecting one related problem

on each area for further research in order to select the main question for the research. The research questions and hypothesis are defined in this chapter in section 3.3. In section 3.4 the processes for the experiments are defined. The data requirement and data collection and data analysis methods are also defined in this chapter, followed by the limitations of the research.

In chapter 4 any alterations in the research phases were recorded to update any changes made to the methodology that were defined in chapter 3 to resolve any issues that were found during the experiments. The changes made in the data requirement, data collection and data analysis and pilot test were recorded in this chapter. This chapter consisted of details from the preparation phase of data for Windows 8 in section 4.2, the Incident response phase for Windows 8 machine acquisition in section 4.3 and data collection phase for Windows 8 machine in section 4.4. The findings of the research will be updated in the analysis phase based on the three sub questions asked in section 4.5 and the results were classified into three areas for data existence in different recovery options, tools effectiveness for confirmatory analysis and potential evidence for event reconstruction.

In chapter 5 the results are discussed with reference to chapter 4. This is done by testing the sub question hypothesis before answering the sub questions that were defined in chapter 3. Section 5.1 aims to answer the three research sub questions based on the findings in chapter 4 and the result from the sub questions were be further discussed in chapter 5.2 to construct the hypothesis for new features that could pose challenges to the Digital Forensic investigation. The hypothesis for the main question will be tested to answer the research question in sub section 5.2.5. The discussion of findings in this chapter will be the extension on the findings from chapter 4 and this section will discuss in detail how the findings were tested for each hypothesis. The recommendation to propose a better solution of the problems uncovered will be presented in section 5.4. The three areas of problems covered are those that were faced due to secure boot, the Digital Forensic tools ability and Forensic readiness for after reset machine.

In chapter 6 the research will concludes with the summary of findings in section 6.1. In section 6.2 the limitations of the research will be summarised and

followed by the summary of recommendation that were outlined in chapter 5. The possible things for future research will be discussed in section 6.4.

Chapter 2 – Literature Review

2.0 INTRODUCTION

The Windows 8 operating system was released to public on 26th October 2012 and it was preceded by Windows 7 which was available to consumers on 22th October 2009. Windows 7 was launched two years after Windows Vista was released in 2007. Numerous articles were reviewed in order to help identify the differences in the Windows 7 and Windows 8 products based on the new features. The question of whether identified problems in Windows 7 are corrected in Windows 8 or do such problems come over to Windows 8. The literature review aims to identify any new area that can be significant for Windows 8 Digital Forensic and if more research on the topic could be done to further understand the research topic better. The new features have provided forensic benefits for the Windows 7 operating system where the potential evidence such as file systems and registry keys are identified thus allowing the investigator to find information on the files and website that a user has access most of the time. Windows 8 new features were also explored in this review to have a better understanding of the new artifact that helps to improve user experience and could be a potential area to explore for Digital Forensic investigation.

The chapter also compares the differences between Windows 7 and Windows 8 to find if there were any similarities between the two different platforms. To prepare for the Forensic research the Digital Forensic investigation processes were reviewed to select the best approach and decision for the tool and techniques that can be compatible to a Windows 8 forensic investigation. An important question is to understand whether the tools in the current market have been updated to meet the requirement of Windows 8. With computer technology being of a fast changing nature it would be very important to have the information on Windows 8. The latest developments in Windows 8 are included in the review to provide the latest knowledge of any changes that were done on the operating system.

In this chapter the objective was to review related articles on Windows platforms from the history of the very first operating system followed by the Windows 7 platform. Secondly the Windows 8 platform review includes the Windows 8 consumer reviews to see the advantages and disadvantages from the consumer perspective. This is followed by a review of the various Windows 8 new features listed such as the file history, Windows Store and the new Internet Explorer 10. Then the following sections give the Digital Forensic related research, such as Windows 8 Digital Forensic professional review, Windows 8 Digital Forensic investigation process and Windows 8 forensic tools and techniques. This chapter will conclude by reviewing the current existing Digital Forensic investigation models and the latest developments in the Windows 8 operating system.

2.1 REVIEW OF WINDOWS 7 RESEARCH

The following sub sections review the history and forensic benefits of previous operating systems.

2.1.1. History of Windows Platform

In 1981, the first operating system from Microsoft was called MS-DOS and in order to use it and complete tasks a user would type instructions to do a task. Windows 1.0 was released in November 1985 which has a graphical operating system (IBN Live, 2012). It was followed by 2.0 in 1987, 3.0 in 1990 and 3.1 in 1992. In 1993 Windows NT a more robust operating system was released to perform more complex tasks for engineering and had scientific programs to handle large numbers (Lim, 2010). Windows 95 will be considered the biggest update which was far better and more successful compared to the previous earlier versions due to the use of the internet (Microsoft US, 2011). The other changes were the launch of Windows XP in 2001 that had better internet tools and built in wireless support (IBN Live, 2012). The Windows Vista release was delayed until November 2006. However was considered a failure as it did not do very well to improve user experience, hence causing some users to downgrade back to XP. Windows 7 on the other hand has overtaken Windows XP as the most popular

desktop operating system and is now running at 50% of enterprise desktop (Warren, 2012). They are the most popular commercial software in the technology era with 700 million windows users in the world and it impacts the lives of humans in their work, entertainment and communication (Feng, 2005). Moving forward since the launch of Windows 8 in October 2012, (O’Mahony, 2012) from The Telegraph reported that the software has sold more than 60 million licenses which are as numerous as the sales of Windows 7. The result is beneficial to the sales of the licenses as users can now from Windows XP skip directly to Windows 8 without having the requirement to upgrade to Windows vista and Windows 7 (Swider, 2013). The following table shows the highlights of Windows Operating System from MS-DOS to the latest Windows 8.

Table 2.1: Highlights from the first 25 years (Adapted from “A History of Windows” (Microsoft, 2013))

| Timeline | Operating System | Used On | Operating System Features |
|---------------------|--------------------------------------|---|---|
| <i>1975 to 1981</i> | MS-DOS | *Personal Computer | <ul style="list-style-type: none"> - Difficult to understand for many people - Typing “C:” and various cryptic commands become part of daily work |
| <i>1982 to 1985</i> | Windows 1.0 | *Personal Computer | <ul style="list-style-type: none"> - Have drop down menus, scroll bars, icons and dialog boxes - Included program such as Paint, Notepad and Calculator |
| <i>1987 to 1992</i> | Windows 2.0 and 2.11 | *Personal Computer | <ul style="list-style-type: none"> - Design for Intel 286 Processor and Intel 386 processor - Extended memory capabilities and Control Panel first appearance |
| <i>1990 to 1994</i> | Windows 3.0 and Windows NT | *Personal Computer *Terminal Server | <ul style="list-style-type: none"> - Virtual Memory improve advance visual graphics with 16 colours and better icons - Included program and games such as File Manager, Print Manager and Minesweeper |
| <i>1995 to 2001</i> | Windows 95 | *Personal Computer | <ul style="list-style-type: none"> - The beginning of Start button and built-in internet support - Plug and play capabilities making it easier to install software - 32-bit Operating system with enhanced multimedia capabilities |
| <i>1998 to 2000</i> | Windows 98, Windows 2000 and Windows | *Personal Computer *Laptop *Windows | <ul style="list-style-type: none"> - Quick Launch bar and System Restore - Support Universal Serial bus devices |

| | | | |
|---------------------|---------------|--|--|
| | Me | 2000 Server | - Advanced networking and Wireless products |
| <i>2001 to 2005</i> | Windows XP | *Personal Computer *Laptop *Tablet PCs *Windows Server 2003 | - Network Setup wizard and Remote desktop support - Encrypting file system for better security - Tablet PCs version consisted of handwriting recognition |
| <i>2006 to 2008</i> | Windows Vista | *Personal Computer *Laptop | - Strongest security system and prevent harmful software from making changes - Bit locker Drive Encryption provides better data protection |
| <i>2009</i> | Windows 7 | *Personal Computer *Laptop *Windows Server 2008 | - Laptops selling better than desktops and more typical to connect to public wireless hotspots and private networks at home - New Taskbar and System tray with quick launch toolbar - Evaluated by 8 million beta tester before released |
| <i>2012</i> | Windows 8 | *Personal Computer *Laptop *Tablet *Windows Server 2012 | - No longer have Start button on desktop - Feature a Start screen with tiles that connect to people, files, application and websites - Functioning as both a tablet and full-feature PC |

2.1.2. Review of Windows 7 Platform

According to Fulton's (2012a) review, Microsoft announced that Windows 7 will be the breakthrough version for personal computers. Windows 7 has better web browsing that enables its user to integrate their browser and web application together to improve work efficiency (Fulton, 2012a). The new features were designed by Microsoft to help users to take lesser steps to achieve the task they have to do regularly.

The release of Windows 7 was anticipated by many Windows Operating system users due to Windows Vista failure to improve the user experience, hence causing some users to downgrade back to Windows XP. An article (PC Plus, 2009) showed that Windows Vista was not very welcome by computer users as during that time computer manufacturers were still selling new systems with XP. Research was conducted to test the performance of Windows XP, Windows Vista

and Windows 7 and it concluded that Windows 7 has the best scores while Windows Vista has the worst scores (PC Plus, 2009).

The Windows 7 operating system was researched by Otnes (2011, p.7) to enable his reader a better understand the software changes and improvements. The following table 2.2 shows the new features and how these new features can benefit the users.

Table 2.2: Review new features in Windows 7 (Adapted from “New and improved in Windows 7” (Otnes, 2011, p.7) & “Windows 7)

| New Features in Windows 7 | Advantages of new features in Windows 7 |
|--|---|
| <i>Aero Shake</i> | Shaking mouse to minimize all other open Windows and Shaking pane again to bring back the windows to original size |
| <i>Backup and Recovery</i> | Better backup and recovery features to protect computer and data. |
| <i>Finding files and programs</i> | Easier to search for files and programs. Using start menu the Search Programs and Files box allows user to find the files, programs and folder by name. |
| <i>Home group</i> | This feature allows the users to share their files and printers with other Windows 7 computers on their home network easier. |
| <i>Libraries</i> | Storing documents, pictures, music and video in a more organize way |
| <i>Jump lists</i> | See a list of recently used files that use that program when right click a program icon |
| <i>Accessible reading on computer screen</i> | Users can freely adjust the size of text showing on the screen |
| <i>Multiple Monitors</i> | All in one multiple monitor position, screen resolution and screen rotation |
| <i>Enhance Taskbar</i> | Replacing small old icons and text labels allowing user to quickly launch a program. |
| <i>User Interface improvements for Bit locker Encryption</i> | Removable devices are protected and provide support for automatic creation of hidden boot partition. |

2.1.3. Forensic Benefits Areas in Windows 7

The forensic benefit areas for Windows 7 operating systems were reported by many researchers. These researchers not only provide many interesting areas that

have not been discovered or fully researched before, but also provide useful information on the new features that can help a Digital Forensic investigator to identify potential evidence on their target. Crenshaw (2009) discussed the interesting points in the Windows 7 file system and registry keys.

Table 2.3: Forensic Artifacts locations in Windows 7 file systems (Adapted from “Forensically Interesting spots in Windows 7, Vista and XP files system and registry” (Crenshaw, 2009))

| File System | Descriptions | File/Registry Location |
|--------------------------|--|---|
| Windows Explorer | <ul style="list-style-type: none"> a) Recently opened files b) Network Shortcut c) Recent Document d) Recently opened or saved files | <ul style="list-style-type: none"> a) C:\Users\<username>\appdata\roaming\microsoft\windows\recent< li=""> b) C:\Users\<user li="" name>\appdata\roaming\microsoft\windows\network="" shortcuts<=""> c) HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\RecentDocs d) HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\ComDlg32\OpenSavePidlMRU </user></username>\appdata\roaming\microsoft\windows\recent<> |
| Windows General | <ul style="list-style-type: none"> a) Recycle Bin b) Event logs c) List of installed USB storage devices d) Temporary Folder | <ul style="list-style-type: none"> a) C:\\$Recycle.Bin b) C:\Windows\System32\config or C:\Windows\System32\winevt\Logs c) HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Enum\USBSTOR d) C:\Users\<user li="" name>\appdata\local\temp<=""> </user> |
| Internet Explorer | <ul style="list-style-type: none"> a) IE cache (Temp folder) b) IE history c) IE Cookies d) IE typed URLs | <ul style="list-style-type: none"> a) C:\Users\<user files<="" internet="" li="" name>\appdata\local\microsoft\windows\temporary=""> b) C:\Users\<user li="" name>\appdata\local\microsoft\windows\history<=""> c) C:\Users\<user li="" name>\appdata\roaming\microsoft\windows\cookies<=""> d) HKEY_CURRENT_USER\Software\Microsoft\Internet Explorer\TypedUrls </user></user></user> |
| Other App Data | <ul style="list-style-type: none"> a) Outlook attachments temp folder b) Offline Outlook Mailbox c) Flash cookies d) Office document opened recently | <ul style="list-style-type: none"> a) C:\Users\<user files\content.outlook\<random="" internet="" name>\appdata\local\microsoft\windows\temporary="" value="">\</user> b) C:\Users\<user li="" name>\appdata\local\microsoft\outlook\outlook.ost<=""> c) C:\Users\<user name>\appdata\roaming\macromedia\flash="" player\#sharedobjects\<random="" value="">\</user> d) C:\Users\<user li="" name>\appdata\roaming\microsoft\office\recent<=""> </user></user> |

His research includes the information of files and websites that a user has accessed repeatedly. The following table 2.3 shows the Digital Forensic artifact locations in Windows 7 file systems.

Digital Forensic artifact file system analysis was further supported by in other research done by Carvey (2012) where he wrote a book about the advance analysis technique for Windows 7 systems. His research focused on a detailed discussion about the existence of several files that were mentioned in Crenshaw's research on the interesting information that can be found in the Windows 7 file system. He pointed out that being aware of the existence of the different files in the file system such as Windows Event Log, Recycle Bin, Scheduled Tasks and Jump List, as well as the analysis techniques such as Registry Analysis that can benefit the value of Digital Forensic investigation found in Windows artifacts. The forensic benefit value of Jump List was further explored and analysed by Barnett (2011) where he proposed that the potential of Jump List in Windows 7 can be of great interest to an investigator. The objectives of his research were to provide an outline on the aspect of jump list that can allow further research that can be useful for future Digital Forensic investigations.

2.1.4. Forensic Problems Areas in Windows 7

The implications of Windows 7 operating systems were researched by various Digital Forensic investigators such as Harms, (2006); Hargreaves & Chivers, (2007); and, Hayes, Reddy & Qureshi, (2010). They examined the various artifacts in the Vista and Windows 7 operating systems. Experimental research was conducted to search for noticeable implications that may be present due to the changes made to improved consumer use of the technologies in the Windows operating systems. For example the BitLocker, according to Hayes, Reddy, & Qureshi, (2010) say that the Windows Vista operating system has caused greater challenges for the Digital Forensic investigator. In order to access the encrypted file, an investigator would need to obtain a password from the suspect or spent time figuring out the passphrase. Casey & Stellatos (2008) show this in their research about the impact of the full disk encryption and have criticized that the

strong encryption in operating system poses a risk for forensic examiners as it ultimately stops them from recovering any potential evidence from a computer during their investigation (Casey & Stellatos, 2008).

In other research, Smulikowski (2009) found new implications caused by InPrivate browsing that was found in Internet Explorer 8. This new feature allows users to explore the internet and not leaving any traces on the user local machine. When no traces were found, it will affect the data collected during Digital Forensic investigation. This will minimize the possibility to piece together any online activity from the suspect's local machine. The author demonstrates how the potential information can be impacted by InPrivate Browsing in the figure 2.1.

| Information | How it is affected by InPrivate Browsing |
|-------------------------------------|---|
| Cookies | Kept in memory so pages work correctly, but cleared when you close the browser. |
| Temporary Internet files | Stored on disk so pages work correctly, but deleted when you close the browser. |
| Webpage history | This information is not stored. |
| Form data and passwords | This information is not stored. |
| Anti-phishing cache | Temporary information is encrypted and stored so pages work correctly. |
| Address bar and search AutoComplete | This information is not stored. |
| Automatic Crash Restore (ACR) | ACR can restore when a tab crashes in a session, but if the whole window crashes, data is deleted and the window cannot be restored. |
| Document Object Model (DOM) storage | The DOM storage is a kind of "super cookie" web developers can use to retain information. Like regular cookies, they are not kept after the window is closed. |

Figure 2.1: Data Stored during InPrivate Session. (Retrieved from "First Look at the Windows 7" (Smulikowski, 2009))

Another private browsing mode was researched by Aggarwal, Burzstein, Jackson and Boneh (2010) where they provide a more detailed information on the data stored in the Internet Explorer private browsing mode. The results proved that private browsing has successfully achieved the desired security goals, however it was also discovered that a well-designed private browsing mode could impact the Digital Forensic tools that are used to collect the user's online activity hidden in the browser history and cookies. The table 2.4 below shows the type of data

collected when IE private browsing was used in various states in the Digital Forensic investigation process.

Table 2.4: IE Private Browsing Forensic Implications (Adapted from “An Analysis of Private Browsing Modes in Modern Browsers” (Aggarwal, Burzstein, Jackson & Boneh, 2010))

| Is the state set in earlier public mode(s) accessible in IE private mode? | | | | | | | | | |
|--|----------------|--------------|-----------------|-----------------|------------------|------------|-----------------------|-------------------|------------------|
| <i>History</i> | <i>Cookies</i> | <i>HTML5</i> | <i>Bookmark</i> | <i>Password</i> | <i>Auto Form</i> | <i>SSL</i> | <i>Download Items</i> | <i>Search box</i> | <i>Web Cache</i> |
| No | No | No | Yes | Yes | No | Yes | Yes | Yes | No |
| Is the State set in earlier private modes(s) accessible in IE public mode? | | | | | | | | | |
| <i>History</i> | <i>Cookies</i> | <i>HTML5</i> | <i>Bookmark</i> | <i>Password</i> | <i>Auto Form</i> | <i>SSL</i> | <i>Download Items</i> | <i>Search box</i> | <i>Web Cache</i> |
| No | No | No | Yes | No | No | Yes | Yes | No | No |
| Is the state set in IE private mode at some point accessible later in the same session? | | | | | | | | | |
| <i>History</i> | <i>Cookies</i> | <i>HTML5</i> | <i>Bookmark</i> | <i>Password</i> | <i>Auto Form</i> | <i>SSL</i> | <i>Download Items</i> | <i>Search box</i> | <i>Web Cache</i> |
| No | Yes | Yes | Yes | No | No | Yes | Yes | No | Yes |

2.2 REVIEW OF WINDOWS 8 RESEARCH

Windows 8 was released to the public on October 26, 2012 and the latest market share data from Net Application reported that as of February was a strong one for Windows 8 and the result showed a rise of 0.43 percentage points (Protalinski, 2013a). The worldwide operating system market share consists of 91.62% of Windows operating system users and in this 2.80% are currently using Windows 8 operating systems (Protalinski, 2013a). The sales of Windows 8 is keeping up with Windows 7 and on the latest report by Protalinski (2013b) the software has sold 100 million Windows 8 licenses in just over 6 months since the launch. The following sub-section below will follow Windows 8 consumer review, the advantages and disadvantages and comparing the differences between Windows 7 and 8.

2.2.1. Windows 8 Consumer Review

Windows 8 is a totally new version of Windows as compare with other versions of Windows. It includes a new style incorporating a touch screen. Grabham (2012) wrote a technology blog at Tech Radar to compare the differences ways why Windows 8 is different from Windows 7. He pointed out that the start screen consists of live tiles and data similar as Windows phone's home screen. The start screen work as an application launcher for Windows 8 Modern UI apps. The next differences are that the integration of SkyDrive allows a user to sync data, save them and moving them from the cloud storage. The sync functions allow users to sync their setting to any other Windows platform that include browsing history for IE and images can be shared on multiple computers (Grabham, 2012).

In a review on Performance comparison Windows 8 VS Windows 7 Muhammad (2013) conducted an experiment to compare Windows 8 and Windows 7 on their speed and performances. The series of experiments includes the boot time, shutdown time, file copying, browsing, gaming and similar synthetic benchmarks on two identical machines and system was identically configured to ensure fairness. His experiment proved that Windows 8 performed better than Windows 7. The results were recorded as Windows 8 fast boot up, shut down and wake-up from sleep time when compared with Windows 7. There were no much changes when comparing the transferring of multiple large files and small files together. Although Windows 8 has featured a new explorer interface for transferring files that was intended to give a more precise data on transfer speed and approximated time of completion. On the other hand, performance of different internet browsers varies the result shows that Chrome performs faster than Firefox on Windows 8. Although all other browsers perform faster in Windows 8 computer yet for Internet Explorer 10 which runs in Windows 8 has the same performance as Internet Explorer 9 on Windows 7 (Muhammad, 2013).

2.2.2. Windows 8 Consumer Review Advantages

The advantages of Windows 8 were listed out by Bowers (2012) on whether companies should migrate from Windows 7 to Windows 8. The advantages

consist of the new user's interface that can help to combine the tablet and computer to work together on the similar platform and the Reset button that would help the IT department to collect issues with one click without the need to re-image a PC (Bowers, 2012). The advantages of the Reset and Refresh function were supported by Vogel (2012a) where indicated that this is a potential method to speed up the restoring of malware infested computers to a stable state from a security perspective. These functions will allow a computer to recover quickly should any security software failed to protect the system (Vogel, 2012).

Although many businesses tend dislike upgrading their computer operating system because the process can bring us the cost of budget and appears to consume a lot of time. Nevertheless there is still a couple of reasons business can still benefit from upgrading to Windows 8 (Bradley, 2013). One of the top reasons why people would consider upgrading is because of the faster boot time, which were emphasized by most reviewers such as Muchmore, (2012; Fikar (2013); and, Brinkmann, (2011). The next reason is that Windows 8 can be operated using a variety of devices such as a laptop, tablet and Smartphone. The software supports touch screen technology where a user can operate the system with their fingers. Windows 8 consist of a Dynamic Display where the user account is connected to the World Wide Web and automatically connected to the data storage provided by Microsoft that allows a user to store data securely on the internet.

2.2.3. Windows 8 Consumer Review Disadvantages

The acceptance of a new operating system can be a long process as there are still some skeptical reviews on Windows 8 that stop enterprises from upgrading and according to Larkin (2013) Windows 7 is not too old and many enterprises are still not confident to replace a new operating system to Windows 8. In fact, there can be many enterprises that have become more familiar with Windows 7 and therefore changing to a new platform may be a bad idea. The reason was also supported by Snyder (2013) where she stated that although the new user interface can be attractive but it can be difficult to use on computers that do not have a touch screen. It will require more training to be able to use Windows 8 effectively. In the research as of February 2013 there were only 2.8% of internet

users using Windows 8 although for most people it was not hard to switch from the older operating system to Windows 7 (Protalinski, 2013a). The next disadvantages are the additional hardware requirements to fully utilize the features of Windows 8. Snyder (2013) also discusses that compatibility can be an issue because there may be some existing computer components and accessories that lack drivers to run properly on Windows 8. That means enterprises might need to make an extra investment to purchase more hardware. Lastly is the time and money that can be spent to upgrade the operating system and adding new business software and memory upgrades will increase expenses, which matches Lakin's (2013) explanation, in which he pointed out that Windows 8 can be different from all other traditional Windows operating system platforms therefore resources must be spent to train the workforce to understand all the new interface (Snyder, 2013).

2.2.4. Differences Between Windows 7 and Windows 8

With the release of Window 8 and new features being introduced, Team windows 8 (2012) did a detailed post about the 15 differences between Windows 7 and Windows 8. The table 2.5 below displays some significant differences between Windows 7 and Windows 8 operating systems.

Table 2.5: Comparing the differences in Windows 7 and Windows 8. (Retrieved from “Top 15 Differences between Windows 7 and Windows 8” (Team Windows 8, 2012))

| Windows 8 New Features | Comparing With Windows 7 |
|---|--|
| <i>Metro UI Start Screen</i> | The start menu button no longer appeared in Windows 8. |
| <i>Simpler Windows Task Manager</i> | More simple than Windows 7 and displays a box with the running apps and a button to kill them. |
| <i>New Data Copy and Move Dialogue Box</i> | The conventional dialogue box showing the copy and moving progress of data been replaced with new display of graph and allows users to pause the move and copying operation. |
| <i>Improved Windows Explorer</i> | Lesser steps to show hidden files as compared to Windows 7, Windows 8 users just need to click the new ribbon to find a simple check box to show and hid hidden files. |
| <i>Sign in to Windows with their Microsoft Account</i> | Using Windows account can store information such as their files and personal preferences in the cloud so users can use the same setting on any other computers with Windows 8. |
| <i>Faster Boot up time for Windows 8</i> | Boot in half-time or even less as compared to Windows 7 on the same computer. Windows 8 has composite the cold boot and hibernation process so that it will behave like the system |

| | |
|--|--|
| | continues to boot from hibernation condition. |
| Windows Defender (Integrated Antivirus) | Windows defender as the built in antivirus for maximum security as compared to Windows 7 there is no need to install it manually from Microsoft Website. |
| Plug-in for Free Browsing | Internet Explorer 10 is compatible for both desktop and Metro UI. Support HTML 5 and do not required plug-in such as Flash Players |
| Modernized Boot Options | Improved boot experience for system restored and system recovery. Now with more graphical and user friendly interface as compared to Windows 7. Removing black and white DOS menu |
| Capability to Reset and Refresh System | Allow to reset and refresh system with just one click. Choosing reset will remove all personal data, files and settings. On the other hand, the refresh option will re-install Windows and restores the backup selected. |
| Windows 8 Charms | This feature is not available in Windows 7, the charms appear in the upper left or upper right corner of desktop giving quick access to start screen setting to change volume and connecting to a network |
| Windows Store | This feature is not in Windows 7, is like a app store with Microsoft apps that provides both free and paid app. |
| Auto Scaling for Different Screen Size | A default for Windows 8 which does not exist in Windows 7. The screen size and resolution can be scale automatically that is suitable for Windows phone screen to a large LCD screen. |
| Picture Password | Add on security for Windows 8 users and this feature is not available in Windows 7. Users can set a specific secret pattern on their chosen picture. |
| Snap View for Multitasking | For Windows 7 users have to move the applications manually for multitasking. Having this function in Windows 8 can allow the users to automatically move program one side of the screen or side by side without having to switch between them. |

2.3 WINDOWS 8 NEW FEATURES

Before Windows 8 was released technology experts like Muchmore (2012); Moorhead (2012); and, Emigh (2011) provided an outlook on the latest features that will be appearing in Windows 8 computers. The technology review experts listed the new artifacts such as the Internet Explorer 10 browsers, the Windows 8 Metro Style apps, File history and the repair and recovery functions (Fulton, 2012b). These new features will be reviewed in the sub sub section to have a better overview about each of their functionalities.

2.3.1. Language and Standards Support

The language and standards support uses a new platform that runs in a secure sandbox. The new platform Windows Runtime was developed as a new type of application that assists the progress of data sharing between different applications

and enhance multi-tasking for widescreen display. The programming languages that were used to code application consist of Visual Basic, .Net, HTML5, C++, C++/CX, C# and Java Script. Figure 2.2 below shows the breakdown of the type of programming languages used to code applications that can be integrated with a Windows 8 Platform and Tools:

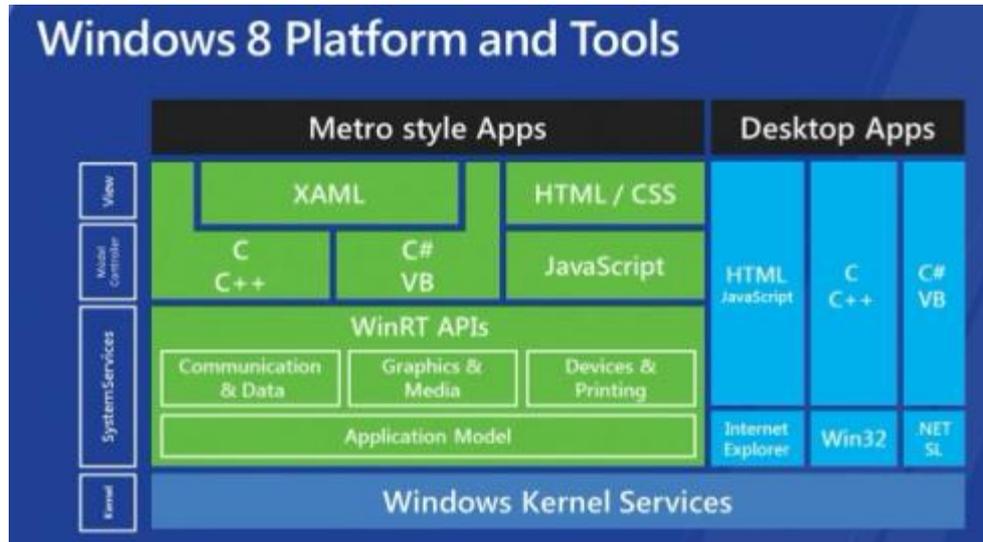


Figure 2.2: Windows 8 Platform and Tools slide shared at Build Conference. (Retrieved from “Part 3: Introduction to WinRT, the new ‘Windows Runtime’ in Windows 8” (Gaddam, 2012))

Gaddam (2012) demonstrated in his article that the new runtime (WinRT API) is a new programming model that makes the core of the new immersive apps in the Windows 8 operating system, thus solving existing problems in Win32 and making Apps created for WinRT safe, secure and sandboxed. On the other hand, in an article by Callaham (2012), he shared that Windows 8 will be adding 14 new display languages to the 95 display languages in Windows 7. This added up to a total 109 languages that will reach out to 4.5 billion people around the world.

2.3.2. Windows Store

The windows store is one of the new features that were introduced as a new type of application that runs on Windows 8 Devices. It allows the developer to advertise the applications that were designed for Windows 8 platform. The store allows a developer to market the product they built for Windows 8. This is to

ensure that products created are secure and of a high standard. As stated by (MSDN, 2013a), Windows Store applications include a single window that fulfills the whole screen on default so that applications running on a screen will not be so disoriented. The new controls create a better user experience and consists of two controls such as an application (app) bar and the charms. The app bar works as the primary command interface for app to display navigation, commands and tools. On the other hand, the charms comport with a particular and a compatible set of buttons in every app such as search, share, settings, connect and start (MSDN, 2013a).

2.3.3. User Login

The new features in shell and interface where the user login screen consists of a new lock screen that includes date and time display. Two new login methods were introduced to efficiently work together with the touch screen function. The new login method pointed out by Abrams (2012a) consisted of a four-digit PIN which allows a total of 10,000 combinations and a picture password that allows the user to login to their account using gestures on an image with their finger or mouse (Abrams, 2012b). Alternatively if a user forgot their PIN or picture password they can still go back to the normal Sign-in options link to click on the key icon. They can simply remove the PIN or picture password as long as they are signed in to the operating system.

2.3.4. Microsoft Account Integration

User accounts can now be linked together into one Microsoft account to give users more functionality that include synchronization user data and connecting together with the other services which Microsoft provided such as Xbox, Skype, Outlook, SkyDrive file storage online (Sinofsky, 2012). In another article, Rey (2012) listed out the eight things about windows 8 account integration where all personal devices can link easily with one another in a single account. The idea behind this feature is supported by (O'Brien, 2012) where he pointed out an example such as Skype integrating with a Microsoft account and in addition the latest update has confirmed that Skype will be replacing Windows messenger in

Outlook.com. As also quoted by (Thurrott, 2013) the Messenger program will be retired as a system operating independently and the infrastructure will be used internally by Skype. This change will be a great advantage to people who have a Live Messenger, Hotmail or outlook.com account so that they can connect together with a Microsoft account and overall for these information to be presented in the metro-friendly user interface on Windows (O'Brien, 2012).

2.3.5. File Explorer

File Explorer is renamed from Windows Explorer in Windows 7. As reported by (Shultz, 2013b) users can start the File Explorer from the icon pinned to the desktop taskbar. File Explorer enables the system for up to 200 different types of file management. The Up button is back in file Explorer which many users hope it will return after it was removed in Windows Vista and incorporates a ribbon toolbar that can take advantage of a Globally Unique Identifier also known as GUID. The GUID is stored in the registry and is specially configured with explorer.exe command as a parameter allows Windows to access that object. Using the right code the default setting of Windows 8 File Explorer can be changed. The table 2.6 below shows the command lines that are used to access other object in Windows:

Table 2.6: GUID command line Table A. (Retrieved from “Quick Tip: Make Windows 8 File Explorer launch in Computer View” (Shultz, 2012a))

| Folder Display | Command Line |
|-----------------------|--|
| Documents | %windir%\explorer.exe ::{450D8FBA-AD25-11D0-98A8-0800361B1103} |
| Network | %windir%\explorer.exe ::{208D2C60-3AEA-1069-A2D7-08002B30309D} |
| Home group | %windir%\explorer.exe ::{B4FB3F98-C1EA-428d-A78A-D1F5659CBA93} |
| Libraries | %windir%\explorer.exe ::{031E4825-7B94-4dc3-B131-E946B44C8DD5} |

2.3.6. Internet Explorer

Internet Explorer 10 will be the default browser used in Windows 8 operating system. The new features include Adobe Flash integration and Flip Ahead (Rivera, 2012). Internet Explorer 10 will work on 2 versions being the usual

desktop version and the metro version that is only available on Windows 8 will give users two different experiences. The Flip Ahead allows a user to move through article that span multiple pages as well as search results. This function was turned off by default and turning it on will required your browsing history to be sent to Microsoft in order to provide the features. Furthermore, other options that allow users to pin any site on to the Metro Start Screen, open page in the desktop and search for information on the page.

Whitney (2012) shared about his view on the new features where he stated that printing and emailing will have to be done on the Charms bar. However, due to the simplification the Metro version of IE does not support plug-ins therefore any site that needs Flash, Microsoft Silverlight or other add-ons will not work. Another problem is that users cannot create or manage a list of their favourite's sites separated by folder and subfolder. The only choice is to pin the favourite site on to the start screen and when the list becomes bigger there is no better way to organize it (Whitney, 2012).

2.3.7. Task Manager

The task manager in Windows 8 provides a complete look on how system resources are being used by the system. Javaid (2012a) compared the new features and options in Windows 8 Task manager to Windows 7. He described that it was a complete rewrite of Windows 7 which separated the Windows tasks into separated groups so that users can navigate easily. One example was the auto-classification of processes into Applications, Background processes, and Windows processes categories in Windows 8 Taskbar. The advantage of these categories is to minimise the time that users spent to find threads of certain applications. The extended view for Windows 8 Task manager consists of processes, performance, App History, Start-up, Users, Details and Services tabs which has more information and is different from Windows 7 Task manager where the Processes tab shows only CPU and Memory usage. In addition Windows 8 Task manager has two secondary columns "Disk" usage and "Network" usage. The "Disk" usage helps users to keep track on the disk and the

“Network” allows user to follow up on the usage for all running applications and processes.

The Performance tab has been refurbished with active line graphs, displaying detailed information about CPU, Memory, Disk, and Network/Ethernet/Wifi usage (Javaid, 2012a).

In another article, Zukerman (2013) mentioned that there are many interesting information points that can be discovered and are hidden in Windows 8 Task manager in the clear appearance. For example, it allows each application to distinctly display its resource footprint that matches things discussed in the previous article by Javaid (2012a) where the useful features and options allows advanced users to easily analyse current system health and performance. The difference in their article shows that the less exciting tabs in Windows 8 Task manager give helpful feedback about the potential impacts for Digital Forensic investigation processes as shown in the table 2.7 below (Zukerman, 2013).

Table 2.7: Tab in Windows 8 Task Manager and their impact to Digital Forensic investigation. (Adapted from (Zukerman, 2013) & (Abrams, 2006))

| Tab in Windows 8 Task Manager | Impact to Digital Forensic investigation |
|--------------------------------------|--|
| App History | <ul style="list-style-type: none"> - Displayed resources usage history for application - Theoretically very valuable for Window artifact analysis - However it only works for modern apps |
| Users | <ul style="list-style-type: none"> - The tab provides information that is valuable to investigation if you share your computer with at least one other user - Displayed how much resource each of the user consumes - This can help to determine who is the person utilize the system the most when doing the timeline analysis |
| Details | <ul style="list-style-type: none"> - Old processes tab and still remain the same from other older version of operating system - The details tab providing system information such as the list of process names, PIDs, and |

| | Stats |
|-----------------|--|
| Services | <ul style="list-style-type: none"> - Monitor the status or running and stopped services - There are remain the same as Windows 7 - Provide valuable information that can help investigator determine what services are being controlled by a particular SVCHOST.EXE process |

2.3.8. File History

The features worked as a time machine for Windows that allows it to automatically back up files. This feature saves copies of the user files so that even if a user overwrites a file by accident it can revert back to the original. According to Pinola (2013), this feature needs to be turned on by the users and files will be saved every hour until about 5% of the space available on the drive is taken up. Gordon (2012) compared the difference between File History and Windows Backup on the article he wrote on Lifehacker website. He stated that Windows Backup can still be found in Windows 8 however it was now being renamed as “Windows 7 File Recovery”. The Windows Backup allows users to back up their computer as long as a schedule has been set. Backup can be selected from a small selection of personal file to program files and full system image can be created which is very convenient, especially if required to restore a computer back to its original state. Alternatively for Windows 8’s File History it acts a little differently as they do not back up the whole system, but only backs up files in the Libraries and personal documents, files and media. Users can include the folders they want to back up into the library. This function will take a snapshot of the files every hour. They each have advantages and disadvantages, however depend on the situation Windows 8 files history is preferred because usually personal documents are more important and they can be replaced if they are lost. The setback of this function is that both backup programs cannot be run together and users have to decide which to choose that is more suitable for them (Gordon, 2012).

2.3.9. Hardware Support

The system requirements that hardware support for Windows 8 and Windows 7 are being compared in table 2.8 below according to the resources from the Microsoft Windows site.

Table 2.8: Comparison Windows 8 and Windows 7 hardware support requirements. (Adapted from (Microsoft US, 2012a) & (Microsoft US, 2012b))

| Type | Windows 8 System Requirements | Windows 7 System Requirements |
|-----------------|--|--|
| Processor | 1 gigahertz (GHZ) or faster with support for PAE,NX and SSE2 | 1 gigahertz (GHZ) or faster 32-bit (x86) or 64-bit (x64) processor |
| Memory | 1 gigabyte(GB) (32-bit) or 2GB (64-bit) | 1 gigabyte (GB) RAM (32-bit) or 2 GB RAM (64-bit) |
| Hard Disk Space | 16 GB (32-bit) or 20 GB (64-bit) | 16 GB available hard disk space (32-bit) or 20 GB (64-bit) |
| Graphics Cards | Microsoft DirectX 9 graphics device with WDDM driver | DirectX 9 graphics device with WDDM 1.0 or higher driver |

Gupta (2013) did research to compare Windows 8 and Windows 7 Memory Consumption. In his research, he acknowledged that Microsoft objectives for Windows 8 were to use the same system requirements as Windows 7. As listed the system requirement for Windows 8 and Windows 7 in the table 2.8 there are no huge or significant changes made. However, comparing Windows 8 with Windows 7 there are still many enhancements made in Windows 8 to give enough space for new functionality and minimize the memory use by the current functionality (Gupta, 2013). In the research it was found that Windows 8 has a better method to plan out memory allocations that is accomplished by application and system components. The outcome was that Windows 8 can provide better decisions about memory to keep around and what memory to remove sooner.

The other new support for Windows 8 includes USB 3.0 provides faster data transfer and improved performance for external USB drivers. USB 3.0 driver provides a better performance for external USB drivers and UASP allows hardware that supports it to use command queuing which assists the device to perform transfers in parallel (Plugable, 2012). The USB has become a popular device that is required for data acquisition applications which addressed by Wright and Judd (2004) and since the speed of data transfer has always been a concern during data acquisition, the new features USB 3.0 will allow faster data transfer. This is supported by Vogel (2012b) in her article where she stated that data transfer can move at a rate of up to 5GB per second (GBps) and compared with USB 2.0 the max speed per second will be 480MB per second (MBps). It will be a huge step forward in transfer speed since most users daily activities include from daily backup to sending music to the Smartphone (Vogel, 2012b).

2.3.10. Hybrid Boot

Windows 8 was introduced with a new hybrid boot feature which reduced the boot time. They take on the hibernate function and improved on it giving us a faster boot time. The purpose of hybrid boot is explained by (Gibb, 2012a) is to reserve the kernel session where instead of hibernating both session it only hibernates the session 0. The Hybrid boot will close the user's original session and when the user starts their system back up again it will read the session 0 from hiberfil.sys file. The session 0 will be put back into memory and overall produce faster boot times and they do not affect any other user sessions. The following figure 2.3 below shows the different phases between cold boot and Windows 8 fast start up.

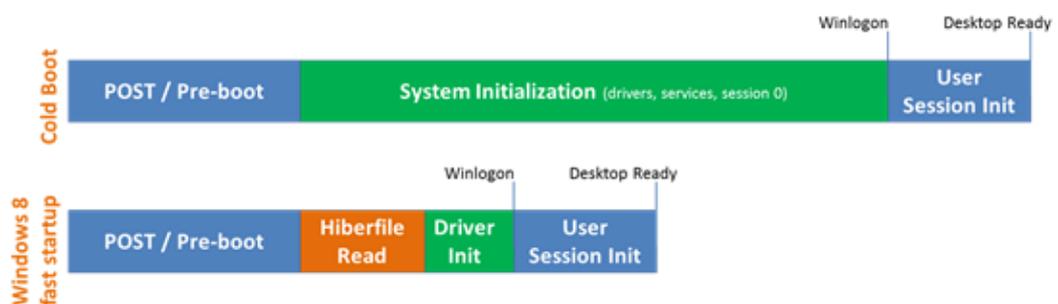


Figure2.3: Representation of different phases between cold boot and fast start up. (Retrieved from “Delivering fast boot times in Windows 8” (MSDN, 2011a))

In other research done Gayan (2012) Hybrid boot helps by giving the 'Kernel' the chance to Suspend and Resume programs. For example, when an active program is suspended they will be in sleep mode and will start to function from the formerly suspended states when it is resumed. This new technology helps to restore a suspended application from disk to the RAM and it is much quicker than trying to open it again from the beginning. The hybrid approach can be helpful to Windows Forensic analysis by Carvey (2012) in collecting volatile data. Windows system memory analysis was researched by Ariffin, Mahmood, Jaafar, and Shamsuddin, (2012) showing the importance of volatile devices in the hybrid approach to retrieve information stored in RAM which can be essential in the Digital Forensic investigation.

2.3.11. Installation

Upgrade Assistant is introduced to give a straightforward and rapid process when upgrading to Windows 8 from older versions. The functionality of Upgrade Assistant includes scanning of hardware, apps and connected devices to ensure they work properly with Windows 8. The tools also check the PC hardware to see if the machine meets the Windows 8 system requirements listed out in Table 2.8. When running the program the Windows 8 Upgrade Assistant will check the computer for compatible apps and devices. The program will display a report for users to review in order to check their computer system readiness for Windows 8 (Rhee, 2012).

2.3.12. Networking

The changes in Windows 8 networking are giving a better support for mobile broadband. The target according to Geier (2012) of the new features is to simplify the processes for networking. He listed out the 12 new networking features in Windows 8. A few significant improvements consist of firstly the network list that gets a new look to better match with metro style interface. Secondly Airplane mode is included which is similar like mobile devices that will disable all wireless communication when it is switch on. This feature is useful on a laptop and mobile

devices that run on a Windows 8 operating system. Thirdly is right click will provide additional wireless controls such as enable data usage tracking and connection metering, - forgetting the network can remove saved passwords and turning sharing on or off. The fourth new feature is the data usage tracking can track the amount of data usage per network that can allow user to look at their amount of data they used that will be useful especially for network that have usage limitations. Fifth is the enable control to limit data usage that limit the connection for each separate network and this could possibly reduce data usage used by all applications that run on the system. Next is the real time network usage statistics that user can find data usage statistics that was included in the Task manager to view current network usage and a history of network usage utilize by all applications. Seventh is the network and sharing centre get reorganized, for example the Manage Wireless Network shortcut function no longer exist and WiFi network will be automatically arranged based on the connection behavior. Lastly in Windows 8 there will be a couple of new Extensible Authentication Protocol types, for example in Authentication types, wireless internet services provider roaming (WISPr) and EAP-SIM/AKA/AKA prime can simplify the connection process to Wifi hotspots by not required the use of third-party clients to achieve the 802.1X authentication type (Geier, 2012).

2.3.13. Repair Recovery

The repair and recovery function in Windows 8 can now detect issues experienced by the system and automatically start up the Advanced Startup menu to provide diagnostic of error and repairing options. The repair and recovery disc is the built-in feature of windows 8 that allows users to create a recovery disk just in case they were unable to boot up their operating system. The tools will be very useful for users to recover and fix Windows 8 boot problems. Users can choose this option to format their drive and do a clean install of Windows 8. The repair and recovery feature includes other option such as Automatic Repair, System Restore and Command Prompt. In addition the newly option for Windows 8 has now also include the Reset and Refresh function. Shultz (2013c) has provided a guideline for using the system image recovery tool from the recovery drive to a

restored hard disk where in an event of failure a user may require to utilize refresh and reset function in Windows 8. The system image recovery will enable a user to restore their system in an event of hard drive failure as long as they bought a new hard disk and use the system image recovery tool so that it can go back to the time they created an image. In another article, Shultz (2013d) explains the Windows 8 automatic repair features. He stated that automatic repair will launch when a start-up problem is detected and this will not require user involvement and in most cases it will rescue the system that does not boot up normally.

Niehus (2013a) has a blog about a more details on the push button reset features for this section where he describes that this option can be used to return the system to a known configuration or to return the system to its original factory settings.

Table 2.9: Elements Preserved and returned to default state (Adapted from (Niehus, 2013a))

| Elements Preserved | Return to default |
|---|--|
| <ul style="list-style-type: none"> - User Accounts such as <ul style="list-style-type: none"> ✓ local accounts ✓ connected accounts ✓ cached domain accounts | <ul style="list-style-type: none"> - Contents of the following folders such as <ul style="list-style-type: none"> ✓ \Windows ✓ \Program Files ✓ \Program Files (x86) ✓ \ProgramData ✓ \Users\<profile.\AppData ✓ OEM-created folders are returned to the state in the recovery source |
| <ul style="list-style-type: none"> - All Files on hard drive expect as stated under removed | <ul style="list-style-type: none"> - App settings are reset to their defaults |
| <ul style="list-style-type: none"> - Personalization settings such as <ul style="list-style-type: none"> ✓ Windows Welcome ✓ PC settings | <ul style="list-style-type: none"> - Desktop apps are removed unless they were preloaded on the computer from the manufacturer |
| <ul style="list-style-type: none"> - Windows Store apps are reinstalled automatically | |
| <ul style="list-style-type: none"> - Bit-locker configuration if it is enabled and bit-locker is suspended automatically during the refresh | |

The push button provides two options which were refreshed the system without affecting the user files or remove everything then reinstall Windows. He provided a table (2.9) to show the types of items that were preserved and removed after the refresh was performed.

2.3.14. Security

The security in Windows 8 is more secure than other operating systems and according to Chacos (2012), he mentions that the 3 major enhancements in the security features for Windows 8. One of those being the expanded prominence on UEFI Secure Boot Optimizations that support secure boot mechanism and it uses a public-key infrastructure process to verify the integrity of the Windows boot loader. The next enhancement is the addition of SmartScreen Filter across the operating systems that protect the system from phishing and malware attacks. Finally is the default inclusion of a more robust version of Windows Defender that not only prevents spyware, but also malware infection when the system boot.

In the next article Amorosi (2012) discussed the Secure Boot features in Windows 8, where the purpose of Secure Boot is to block rootkit malware from infecting a system. The method is to prevent a machine from performing 'boot loader' code where all code that's running the boot process must be certified through a digitally signed certificate from a key stored in the UEFI firmware. Nevertheless, Windows 8 is the most secure Windows operating system to date since many of the security features related to enterprise were available in Windows 8 pro, the feature included a self-encrypting drive capabilities and multiple Bit Locker contribution (Amorosi, 2012). However in a test conducted by Bitdefender has proven the security features in Windows 8 still is open to infection by 15% of the most popular malwares that exist. The test was conducted using a variety of most widespread Trojans, bots and rootkits active in the last six months. In the results it was discovered that Microsoft's defender was not protected as it seems because out of the 385 Windows 8 tested there were 61 malware threats that infected the system and one is all it need to put an enterprise system in jeopardy (InfoSecurity, 2012).

2.3.15. Video Subsystem

WDDM version 1.2 and DirectX Graphics Infrastructure (DXGI) Version 1.2 were included as the new optimized features for Windows 8's Video Subsystem (MSDN, 2012a). The improvements include better screen quality, a decrease in the amount of main memory that a program uses, and the sharing of resources were made better and quicker recovery and timeout detection. These improvements provide a new outlook of functionality that were not featured in previous display driver models such as Virtualized video memory, scheduling and cross-process sharing of direct 3-D surfaces (Manik 2012).

2.3.16. Windows To Go

Windows To Go is included as a new feature for Windows 8 Enterprise Version and benefits of Windows To Go which works as a bootable USB Flash drive can be helpful for many enterprises. (Sinchak, 2012) states that it allows enterprises to supply a full corporate environment that will boot from a USB drive and they can be controlled by standard enterprise management tools such as SCCM and Active Directory group policies. The features in Windows To Go were supported by Schauland (2012) as it gives users a chance to take Windows 8 to where ever they go with an external hard drive or USB and let them keep the same environment at all times for their operating system which can allow them to transform any PC into a corporate PC as long as application stack is all on a USB drive. The three things to create Windows To Go media consist of a USB device 32Gb larger as the target device, a Windows 8 Enterprise running on a host PC and Windows 8 installation media (Schauland, 2012).

In another article Bradley (2012) discusses about the new features in Windows To Go could be a good option for an organisation who is still using Windows XP and is a perfect operating system for them if they have plans to adopt a Bring Your Own Device (BYOD) policy. He listed out the benefits where an employee at work can use the safe and secure Windows 8 environment provided by the organisation and once they are finished their task they can simply just shut down and leave. The next benefit will be the lower the risks of malware infection because a new image can be cloned and act like this incident has never

occurred at all. However there are still some features and functions not available by default in Windows To Go such as internal drives of PC, the hibernation features, Windows recovery and Windows 8 App store (Bradley, 2012).

2.3.17. Hyper-V

Hyper-V features are part of Windows 8 Pro that takes over the Windows Virtual PC as a virtualization program for Microsoft Windows. The actual name for this feature in Windows 8 is known as Client Hyper-V and the name are used to tell the difference from the virtualization function provided by Windows Server. Fulton (2012b) describes the technical incompatibilities between hyper-V and the old Virtual PC in his article where he states that Hyper-V is designed for cloud-based systems so in reality the resource size such as computer power are scalable thus virtualized servers are more flexible than a physical one. Next, the configuration files for virtual PC and Virtual server are not suitable with Hyper-V and lastly the elements of a virtual machine that allows it to identify itself as a Virtual Machine cannot be the same when migrating the Virtual Machine to Windows 8 due to the differences in the Windows 8 Kernel. An option is proposed to cross the gap which is also supported by Hicks (2012) where creating a new Hyper-V virtual machine in which the Virtual hard disk file can be installed because Microsoft Virtual hard disk format is still supported in Windows 8. A user can easily mount a VHD by just double clicking the virtual hard disk file in the file Explorer. This allows user to take advantage of the Hyper-V functions where in the past user had to download free virtual box solution in order to run their desire virtual PC system (Hicks, 2012).

2.3.18. Storage Spaces

Storage Space in Windows 8 has changed the way users save and access files. Graham-Smith (2013) described in his article that the storage virtualization technology allows users to combine the storage capacity of multiple disks into storage pools and then form them together like a number of virtual disks. In simple language, these virtual disks are known as the storage spaces. The function of storage space is shown by Cunningham, Smith, Vatto and Walton (2012) to

allow a pool of different physical drive together into one large logical drive and the pool drives were connected by any popular interface which include USB, SATA and SAD. However Grahman-Smith's (2013) article has provided a more in depth information that storage space should not be treated as RAID volumes although they work on similar principle. The advantage of storage space is that it gives a user flexibility option where using more than one disk can improve performance and Windows 8 can read and write data from multiple drives at one time. The disadvantages is that if a user adds a disk to a pool and when it is completely wiped that will become unavailable to Windows. It will be inaccessible from the Explorer or allow saving of regular files onto it if they were removed from the pool and they will have to be reformatted before they can use it again (Graham-Smith, 2013).

2.4 WINDOWS 8 FORENSIC RESEARCH

Windows 8 not only is a focus for technology review experts but also professionals from the Digital Forensic areas. Digital Forensic researchers were interested in Windows 8 so that a new guideline can help to prepare the Digital Forensic investigators on how to conduct data acquisition and analysis on the Windows 8 machine. This section covered Windows 8 Forensic professional review, Digital Forensic investigation process and Forensic tools and technique that can be incorporated into Windows 8 forensic research.

2.4.1. Windows 8 Forensic Professionals Review

Thomson (2012) did research for a Digital Forensic Guide on a Windows 8 machine in the preview version that consisted of the Windows Artifacts and Windows Registry keys. In the research she described about how the Windows Artifact and Windows Registry Keys in Windows 8 can improve the time-line analysis when reconstructing events of a crime during data analysis (Thomson, 2012). In other research, Brunty (2012) posted an article about the first look for Microsoft Window 8 Forensic where he provided more details about Windows 8 Registry Artifacts. He updated information about the various changes within

Windows registry where forensic investigators should be aware - eventhough there are only some slight changes from the previous Windows 7 version. The significant changes included the addition of metro apps which include a registry key that shows what metro apps were installed on the system and the user account installed on the system (Brunty, 2012). Fleisher (2012) conducted similar exploratory Digital Forensic research on a Windows 8 operating system and comparing it with other research that were already done on Windows 7 Operating systems. The main purpose of his research is to look out for any changes that can be useful in the Digital Forensic investigation process. The topics that he explored are the Windows Artifact in Windows 8 such as Recycle bin, Internet history and the new File history features. For example, in the properties of Recycle bin, the files and folders. Windows 8 still has \$R files however these files now do not appear directly in the \$Recycle.Bin folder. Next in the internet history, he described the differences of the folder he found in Windows 8 in the temporary internet files and they were a little different from Windows 7. He reported that in Windows 8 the cookies in the internet history were stored in windows 8 are in a different location and index.dat files that exist in the same location as Windows 7 is now empty. Lastly, in the history backup new features the file history folder will only exist only when the feature is turned on. The log files can be found at root\windows\system32\winevt (Fleisher, 2012).

In different research, Hale (2013) focused on the tracking opened photos where he discovered that Windows 8 photo app saved the usage history information within a user's UsrClass.dat in the registry hive. He found GUID subkeys can be used to trace the user's activities and have populated more than 200 subkeys. The stored information such as file name, the image file path, time stamps, typed of devices used to view images, the last opened date and time. The figure 2.4 below gives information about each value based within one of the following GUID subkeys.

| Value Name | Value Type | Value Data |
|-------------------|------------|---|
| FilePath | REG_SZ | Full path to the file |
| Flags | REG_DWORD | Appears to relate to the media type from which the image was opened |
| LastUpdatedTime | REG_BINARY | 64-bit FILETIME value; appears to reference last time the file was opened |
| Link | REG_BINARY | Variation of Windows LNK file [MS-SHLLINK] |
| Metadata | REG_SZ | Holds the name of the file |
| PackageFamilyName | REG_SZ | microsoft.windowsphotos_8wekyb3d8bbwe |

Figure 2.4: GUID subkey information. (Retrieved from “Windows 8 Tracking Opened Photo” (Hale, 2013))

In addition, Johnson (2012) did an analysis on the forensic impacts of Windows 8 Recovery options. His report covered the recovery options that are available and its Forensic implications. These options are available in Windows 8 and have the possibility to be abused by a user to destroy potential evidence. The recovery options consist of System Restore Point, System Refresh Points and System Reset. In summary, each recovery option can leave different Artifact’s information in the system. The data in the system restore point can be retrieved using the existing tools and techniques, however using the Refresh and Reset options can destroy all system restore points on a machine. The refresh and reset option will leave similar artifact information in the boot system but users setting will be gone when the functions are used. He concludes that the reset option will effectively remove the information evidence from the Windows 8 system (Johnson, 2012).

2.4.2. Windows 8 Digital Forensic Investigation Process

Windows 8 Digital Forensic investigation follows the current Forensic process models that are available. A successful investigation will rely on the resources available, the objectives of the investigation, the policies of the organisation and the different circumstances involved in the investigation. According to Harlan (2012) windows Forensic analysis concepts, the most important approach is to meet the objectives and in the same way the Digital Crime Scene Investigation phases goal is to collect and analyse the computer evidence that was acquired

from the physical investigation phases then reconstruct the actions that happened during the incident. As described by Tushabe (2004) it consisted of the six phases in the figure 2.5 below.

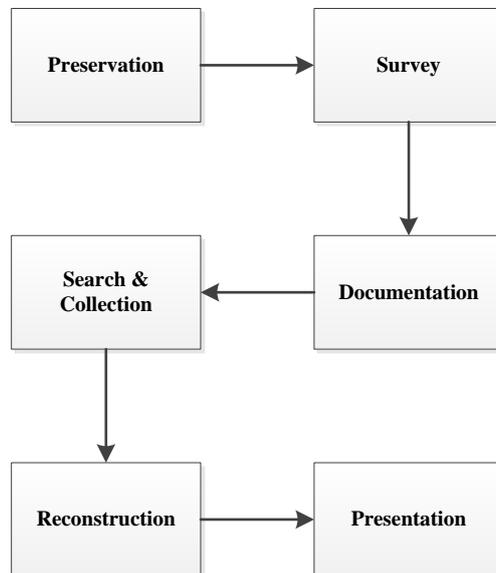


Figure2.5: Digital Crime Scene Investigation Process. (Adapted from “Computer Forensic for Cyberspace Crime” (Tushabe, 2004))

The processes were explained by the author to be firstly the preservation phase that aims to preserve digital evidence in the crime scene so that the evidence can be synchronized and analysed for further evidence. Secondly, the Survey phase needs an investigator to transfer the relevant data from a venue out of the physical drive. Thirdly, Documentation phase includes carefully documenting the digital evidence when it is found that can be useful in the presentation phase. Fourth, Search and collection phase evoke an extensive analysis of digital evidence. Fifth, Reconstruction phase will involve joining all digital evidence collected together and construct investigative suggestions. Lastly, a Presentation Phase will consist of presenting digital evidence that was found in the physical crime scene by the investigation team.

In another guide that can be useful for Windows 8 Forensic investigation process will be the NIJ guide for Electronic Crime Scene Investigation for first responders. Ashcroft (2001) described the Forensic process where electronic evidence offers very special challenges for its admissibility in court. In order to meet the admissibility in court, proper Forensic procedures have to be followed.

The guideline focused on the collection procedure where the potential evidence found in Windows Operating System consisted of the following in table 2.10.

Table 2.10: Potential evidence found in Windows Operating System (Adapted from (Ashcroft, 2001))

| Evidences in Operating System | Types of files |
|--------------------------------------|--|
| <i>User-Created Files</i> | <ul style="list-style-type: none"> - Address books - Audio/Video files - Calendars - Database files - Documents or Text files - Email files - Images/Graphic files - Internet bookmarks/favourites - Spread sheet files |
| <i>User Protected Files</i> | <ul style="list-style-type: none"> - Compressed files - Encrypted files - Hidden files - Misnamed files - Password Protected files - Steganography |
| <i>Computer Created Files</i> | <ul style="list-style-type: none"> - Backup files - Configuration files - Cookies - Hidden files - History files - Logs files - Printer spool files - Swap files - Temporary files |
| <i>Other Data Areas</i> | <ul style="list-style-type: none"> - Bad clusters - Computer date, time and password - Deleted files - Free Space - Hidden partitions - Lost clusters - Other Partitions - Reserved areas - Slack space - Software registration information - System areas - Unallocated space |

2.4.3. Windows 8 Forensic Tools and Techniques

The standard way of conducting a windows operating system Forensic investigation is by using Digital Forensic tools. According to Belkasoft (2013), most information stays hidden in digital devices therefore a Forensic investigator requires a set of purposeful tools to obtain evidence from the computer devices. The Digital Forensic investigator can choose from either one tool to perform the entire task or may use a mixture of tools to acquire the desirable data they needed for the investigation. Such tools consist of acquiring data from digital devices and also can help investigators to reconstruct the suspect's activities on their computers without altering any data on the devices. In a presentation by Leibrock (2003), he described how the advantages of using Digital Forensic tools can impact Windows operating system investigation. The first point he pointed out was Digital Forensic tools can assist in creating an authentic duplicate to avoid the allegation of any destruction of potential evidence. Secondly was to perform a summary of findings in order to look out for hidden artifacts inside file systems. Next, the tool can assist an investigator to carefully distinguish the attributes of the evidence in order to perform a detailed investigation by logging down the details observed such as the date and time, the types of application and the characteristic of the data. Following this, by using the tools, it can let the investigators revalidate their observations and finally prepare a Forensic report to defend their findings.

Windows 8 is relatively new at this stage but because the current tools in the market still support the file system and software has been updated to meet the requirements of Windows 8 thus most commercial tools can still be valid for investigation on the Windows 8 Platform. The Computer Forensic tools testing handbook release by National Institute of Standards and Technology provides the reports on the selection of the tool to determine the tools performance on the core Forensic such as imaging drives. The benefit of referring to the booklet can let the investigators be assured about the capabilities of the tools, find out if a tool has any limitation so that they can take suitable action such as using another tool or

any include new procedure to meet the requirements (NIST, 2012). The table 2.11 below shows a summary of the several tools reviewed for Windows 8 Digital Forensic investigation and were available at the time of the research:

Table 2.11: Summary of tools reviewed for Windows 8 Digital Forensic Investigation

| Name of Tools | Platform Used | Version | Description | Windows 8 OS Compatible |
|------------------------------|----------------------|----------------|---|--------------------------------|
| <i>BlackLight</i> | Windows & Mac | 2013R1 | <ul style="list-style-type: none"> - Forensic Analysis Software for Windows - Extraction of active Registry and active files system | Yes |
| <i>Registry Recon</i> | Windows | 2 | <ul style="list-style-type: none"> - Rebuild and parse Windows Registries from a hard drive for deep analysis - Extract Windows restore points and Unallocated space | Yes |
| <i>EnCase</i> | Windows | 7.04 | <ul style="list-style-type: none"> - Multiple tools that include Digital Forensic process such as acquisition, analysis and reporting | Yes |
| <i>FTK</i> | Windows | 4.2 | <ul style="list-style-type: none"> - Multiple tools that include scanning a hard drive for text strings - Toolkit provides a FTK imager for disk imaging and saving an image of hard disk in one file to reconstruction of a suspect activities | Yes |
| <i>SANS (SIFT)</i> | Ubuntu | 2.1 | <ul style="list-style-type: none"> - Multiple tools that pre-configured with essential tools for Digital Forensic investigation. - File system support for Windows platform such as MS-DOS, FAT & NTFS | Yes |

| | | | | |
|---|---------|-----------------|---|-----|
| <i>OSForensic</i> | Windows | 2.1.101 Beta | <ul style="list-style-type: none"> - Forensic tools for email, file history, images & browsers history - Collect system information and uncover recently activities on the system | Yes |
| <i>Belkasoft Evidence Center</i> | Windows | 5.3 | <ul style="list-style-type: none"> - Extensive Forensic analysis of hard drives and disk images - Retrieving and extracting evidence that was hidden or deleted files as long as information is physically available from memory dump or hibernation files. | Yes |

2.5 EXISTING DIGITAL FORENSIC MODEL

Digital Forensic models are available to boost the efficiency of the Windows 8 Forensic investigation. In a conference article comparison of the existing forensic model by Valjarevic and Venter (2012, p.8) is made so the author can propose a model that can translate Digital Forensic principals into actions that can work together with the Digital Forensic investigation processes. The most important principle in the Digital Forensic process will be the evidence’s integrity must always be preserved. The author has raised the issues where there were currently no harmonised Digital Forensic investigation process models that can be used as a standard guide for Digital Forensic investigation. The following table 2.12 displayed the comparison of three existing models and finally one of these three existing models will be chosen as the final model to be followed through the Digital Forensic process for the case scenario in this research.

Table 2.12: Comparison of three existing Forensic model (Adapted from “Harmonised Digital Forensic Investigation Process Model” (Valjarevic and Venter, 2012,P.8))

| Reference Phases | Authors |
|-------------------------|----------------|
|-------------------------|----------------|

| | (DFWRS, 2001) | (Beebe et al, 2005) | (Casey & Rose, 2010) |
|-------------------------------------|---|---------------------------|--|
| Incident Detection | Yes (1.Identification) | Yes (2.Incident Response) | - |
| First Response | - | Yes (2.Incident Response) | - |
| Planning | - | Yes (1.Preparation) | - |
| Preparation | - | - | - |
| Incident Scene documentation | - | - | - |
| Evidence Identification | - | - | Yes (1.Gather information and make observations) |
| Evidence Collection | Yes (2.Preservation) Yes (3.Collection) | Yes (3.Data Collection) | Yes (1.Gather Information and make observations) |
| Evidence Transportation | - | - | - |
| Evidence Storage | - | - | - |
| Evidence Analysis | Yes (4.Examination) Yes (5.Analysis) | Yes (4.Data Analysis) | Yes (2.Form a hypothesis to explain observations) Yes (3.Evaluate |

| | | | |
|---------------------|-----------------------|--------------------------------|--|
| | | | the hypothesis) Yes (4.Draw conclusions and communicate findings) |
| Presentation | Yes (6. Presentation) | Yes (5. Findings Presentation) | Yes (4.Draw conclusion and communicate findings) |
| Conclusion | Yes (7. Decision) | Yes (6.Closure) | - |

The first Forensic model reviewed from (DFWRS, 2001) aims to follow the concept of the method toward the preserving, collecting, validating, identifying, analysing, interpreting, documenting and presenting of the computer Forensic evidence copied from a digital device to further reconstructed any event found to be an unauthorised action that can be proven to be destroying any outlined actions. The second Forensic model by Beebe and Clark (2005), was a hierarchical, objectives based Digital Forensic investigation process models that have six step process with the objectives to comprehensive comparison the proposed process model to the previous works in the related field. The two tiered proposed by them include the six phases as known on the table 2.12 and there should be sub phases to include the possible types of crime and types of digital evidence. The third model was a more simplify version that consists of four phases such as gathering information, making observations, forming hypothesis to explain observations, evaluating hypothesis and drawing conclusion, then at the final step to communicate the findings (Valjarevic and Venter, 2012).

2.6 LATEST DEVELOPMENTS IN WINDOWS 8 OPERATING SYSTEM

Computer technology progress is rapid and competitive. According to Saran (2013) article in Computer Weekly, the personal computer market failed in the first quarter of 2013. The new personal computer shipments declined 14% as compared with the first quarter in 2012 last year. In the same article, IDC research director David Daoud says that the personal computer industry is going through a critical time and strategic choices will be needed to be made on with the range of different devices around in the market and appropriateness to users (Saran, 2013).

As the Windows 8 Operating System is still a new product in the market, the system will likely go through many changes and updates during the research period. This section discusses about the current developments with the Windows 8 Operating system which includes any latest update and new features released by Microsoft.

The big upgrade for Windows 8 as reported by Limer (2013) was meant to be for all windows 8 users and such an update really matters because it can improve the user's experience when using the operating system. Windows 8.1 was released for download for Windows 8 users one year after the release of Windows 8. He reported that Windows 8.1 changes included the start button that was missing on Windows 8, that allows users to select to boot to desktop and the Bing-powered omnisearch allows searching on a computer that includes web search results. Lastly, the updates also provides a brand new look for Windows Store applications that allows more settings options in metro for customizing the screen in metro, which allows users to view changes such as displayed resolution and mouse settings (Limer, 2013).

In Windows 8.1 security improvements based on the article by Bruzzese (2013) mentioned that Microsoft will be pushing the TPM 2.0 to be on all devices by 2015 although there were no such requirements for current devices. Another improvement will be Windows Defender that has been improvised with network behavior to stop the execution of malware and moving to the Internet Explorer 11. In another article by Geier (2013) shared the same view and he raised that Internet

Explorer 11 will have the new feature to support multiple windows opened and the Enhanced Protected Mode turned on by default to enable the sandbox-like function to restrict internet explorer from picking up sensitive data and system files (Geier, 2013).

Windows 8.1 update 1 will be planned for release in March 2014 to alter the start screen works. Warren (2014) says it will have the boot to desktop option by default. He reported that at the moment Microsoft are reviewing feedback from Windows 8.1 and is planning to make changes for organisations trying to move away from Windows XP ahead of the cut off support in April 2014. The changes will include having shutdown and search buttons on the start screen and a pin application on the desktop task bar so that users can minimize or close applications more conveniently (Warren, 2014).

2.7 CONCLUSION

In this chapter the Windows 7 new features were covered to understand the upgrades of Windows platform from Windows Vista after Windows 7 succeeded the operating system in 2009. Altogether 10 features were reviewed with each of their advantages. The section that covered the Windows 7 platform included the forensically interesting points from the previous Windows platform with their pros and cons being discussed. The review of Windows 8 research pointed out about 18 new features that included the development platform, infrastructure, security, and the shell and user interface. Similarly, on Windows 8 the current consumer reviews together with the advantages and disadvantages of the Windows 8 system. The top 15 differences between Windows 7 and Windows 8 were compared using Windows 8 features as the benchmark to understand the major changes in Windows 8. The chapter also follows the changes made to Windows 8 platform to look for any upgrades made on the Windows 8 operating system and now at this time Windows 8.1 was released to the public to include a start button and options that allows the users to select so that when the machine started it will boot on to the desktop rather than the metro interface.

For the Digital Forensic part the review also looked into the Digital Forensic area for research on the Windows 8 system for new guidelines for the significant changes of Digital Forensic investigation from windows 7 and Windows 8. It was reviewed by Flesher (2012) that Windows 8 internet history were stored in Windows 8 are on the different locations and files that were supposedly existed on Windows 7 is not empty. The current Digital Forensic process can still be followed on Windows 8 because the most important aspect will be preserved digital evidence at a crime scene so that evidence collected can be used for further analysis. The current exiting model will be reviewed to enhance the ability to preserve Digital Forensic evidence that can be chosen as the standard methodology. The tools and techniques for a Windows 8 operating system after being reviewed also proved that now most tools available in the market were compatible for Windows 8.

Due to the wide selection of problems areas that can be researched for Windows 8, the next chapter for methodology will review the problems areas for similar work of Digital Forensic investigation for Windows operating systems and problems/issues on Windows 8 new features so that a research question can be narrowed down to one final main question for the research. The research design, data collection, data analysis and limitations of the research will be discussed in detail in chapter 3.

Chapter 3 – Methodology

3.0 INTRODUCTION

In Chapter 2 the literature reviewed articles related to the history of the Windows platform with the focus on the user experience in Windows 7 and Windows 8 plus the Digital Forensic processes that were relevant to the Windows Forensic topic. This chapter will look into the problem areas of the past research before narrowing it down to the relevant problem for research. The literature research was reviewed based on the past Windows Platform Digital Forensic Issues and problems, review of current windows 8 current issues and problems, review of Windows 8 Digital Forensic issues and problems and the review of Windows 8 new features issues and problems. The next section which is the selection of research problems attempts to narrow down the problems and issues found to focus on one significant problem and issue so that the main research question will be chosen for this research. Section 3.3 defines the research question and hypothesis by first reviewing the challenges in Windows 8 new features for Digital Forensic investigations in sub section 3.3.1 to come up with a research question and sub questions in 3.3.2. The next sub section 3.3.3 is the testable hypothesis that can lead to the answering of the sub questions. The research design is set out in section 3.4 and the sub section 3.4.1 discusses the case based reasoning being used to form questions and solutions for the research based on past research on the target problems. The Digital Forensic and research phases will follow the approach used by Beebe & Clark (2005), using a hierarchical, objectives-based framework for the Digital Forensic investigation process. The approach to follow and each phase were listed out below based on each research phase and the steps that were in the framework proposed in figure 3.1.

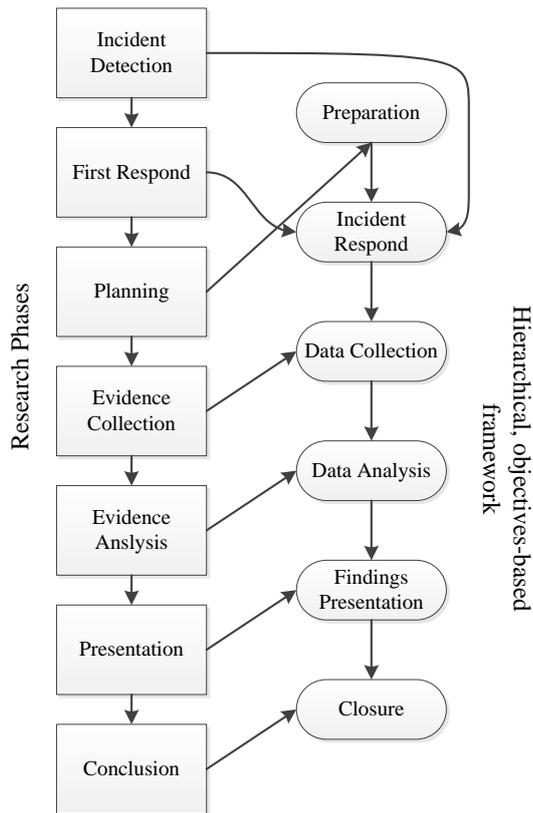


Figure 3.1: Approach for each research phases. (Adapted from “Comparison of the Existing Forensic Model” (Valjarevic & Venter, 2012, P.8))

Pilot tests were planned in sub section 3.4.5 to ensure the required data were collected for the research. The data requirement in section 3.5 will ensure that the setup will be on a controlled scenario for incident detection and a first responder. The planning for the research and the selection of tools that were available for the research is also completed. Section 3.6 will describe the methodology for data collection to ensure the integrity of evidence during the acquisition phases and the expected data to be found. Section 3.7 will focus on how the data collected can be transformed into a more managed size for analysis so that it can help to answer the two sub questions based on the tools used for analysis, the data collection and whether an event reconstruction analysis can be done on a Windows 8 machine for file analysis, registry analysis, timeline analysis and application analysis. The limitations of the research will focus on the challenges of new features and the impact of the new features that may affect Digital Forensic investigation will be discussed in section 3.8.

3.1 REVIEW OF ISSUES AND PROBLEMS

In the following sub sections, section 3.1.1 reviews the past windows platform Digital Forensic issues to have an understanding of problems and issues related to data acquisition and data analysis that occurred in past windows platforms. Section 3.1.2 reviews current Windows 8 issues and problems will focus on how users are currently dealing with the challenges of Windows 8 from a user perspective. The problems and issues discussed were from the totally new user's interface which users have required more time adapting to the changes can be a problem and current security issues that were targeting the Windows 8 operating system. Section 3.1.3 reviews the possible Digital Forensic problems and issues that can happen during a Digital Forensic investigation on a Windows 8 operating system. These were reviewed to have the overview of what are the types of various Digital Forensic investigation that may occur and what are the concerns that should be put into consideration during an investigation on a Windows 8 operating system. Lastly section 3.1.4 reviews the new features issues and problems of Windows 8 that can be a useful guide for investigators conducting Digital Forensic investigation on a Windows 8 machine. The new features reviewed discuss the new storage space, new hybrid boot process and new metro user interfaces in Windows 8.

3.1.1. Review Past Windows Platform Digital Forensic Issues And Problems

The main goal for Digital Forensic on a Windows computer is to collect and examine electronic evidence in detail, which involves making evaluation of the damages of a computer after an incident has happened involving a computer crime. In order to fully understand the challenges of a Windows Forensic investigation and pick out the problems and issues related to Digital Forensic investigation on a Windows Operating System, the following review will look at the past windows issues first related to data acquisition problems and then moving to the data analysis problems that were noted by various Digital Forensic researchers on Windows Operating Systems. The list of problems related to data acquisition were reviewed and shown the table 3.1 below.

Table 3.1: Data Acquisition Problem & Issues (Adapted from “Guide to Integrating Forensic Techniques into Incident Response” (Kent, Chevalier, Grance & Dang, 2006))

| Problems/Issues that were noted | Discussion of the problems/issues |
|---|---|
| <p>Collecting data files when copying files from computer devices many process were spent to search for residue of deleted files and many process were spent to recovering deleted files. All files data attributes can provide the valuable information that could help to determine suspect activities during Windows Analysis.</p> | <ul style="list-style-type: none"> - Remnants of files found in free and slack space on a media are being overlooked - The file name, MAC time attribute is important to an investigation, overlooking this can hinder further event reconstruction of suspect activities during data analysis process |
| <p>Suspect can executed a variety of techniques to obstruct the collection of files in free and slack space as there are many utilities available to destroy potential evidence on a system. The worst case scenario will be using physical means to prevent data collection if the hard drive have been demagnetized or been physically damaged.</p> | <ul style="list-style-type: none"> - Using the utilities could conduct media wiping for a few time by setting values to all 0's that could obstruct the collection during data acquisition process - If required to use advance techniques and hardware will bring up the cost of investigation and lead to lack of evidences for prosecution |
| <p>Collection of hidden data where many operating system permit user to tag certain files, directories and even set the partition as hidden that will reflected that by default the files may not be displayed correctly in the</p> | <ul style="list-style-type: none"> - Applications and OS hiding the configuration files to minimize the chance that users may accidentally modifies or deletes the files - Hidden partition could contain a |

| | |
|--|---|
| <p>directory listing. Directories that were deleted may be mark as hidden and could contains important information</p> | <p>separate OS and many data files when user create hidden partition by altering the partition table to disorganize the disk management and prevent application from seeing that the data area is available</p> |
| <p>Hidden Data can be found within ADS on the NTFS Volumes in the end of file slack space and free space on a medium</p> | <ul style="list-style-type: none"> - HPA on some hard drive is a region of a drive that is intended to be used by vendors only - Collection tools can be used to recognize some of all these methods of hidden data and can be successfully recovered |
| <p>RAID arrays that use stripping such as RAID 0 and RAID 5. Disk with specific RAID array configuration will have a stripped volume consist of equal size partition that located on separate disks and RAID setup must be recreated on the examination system to identify the RAID array used and prevent any writing on the arrays</p> | <ul style="list-style-type: none"> - Data written to the volume is equally distributed across the partitions to speed up disk performance such step may cause problem to investigation as partitions stay on separate physical disk drive - To correctly examine a striped volume, each disk drive has to be imaged and forensic boot disk must acquire the striped volumes and preserve any unused data area |

Next, the review of the Digital Forensic analysis of past windows system investigation problems and issues can help investigators to understand the challenges when doing files analysis, registry analysis, timeline analysis and application analysis. Windows Forensic Analysis Toolkit book by Harlan Carvey

(2012), was chosen in this review to help in identifying the interesting problems in the area that may occur during a Digital Forensic investigation. Windows Forensic issues cover many areas and required to be summarised in order to have a better picture of what the issues are currently and to finally pick out the relevant research questions. The list of problems and issues related to data analysis were reviewed and shown in the following table 3.2 below.

Table 3.2: Digital Forensic Analysis Problems & Issues (Adapted from “Windows Forensic Analysis Toolkit Book” (Carvey, 2012))

| Types of Analysis | Types of Information | Problems & Issues |
|--------------------------|---|--|
| File Analysis | <ul style="list-style-type: none"> - MFT - Event Logs - Recycle Bin - Prefetch Files - Scheduled Task - Jump List - Hibernation Files - Application Files | <ul style="list-style-type: none"> - Last access time for file on the NTFS files system on hard drive is not always current - The Event viewer works only on live systems but does not work on a Forensic image. Investigator have to break up the events logs - Cannot rely on the Windows’s API to read event files as the file can be corrupted and may miss the one that was over written |
| Registry Analysis | <ul style="list-style-type: none"> - System Hive - Software Hive - User Hives - Additional Sources | <ul style="list-style-type: none"> - Registry keys can be affected by WOW64 when keys are being shared by both 32-bits and 64-bit applications on a 64-bit Windows where some redirection may occurred - NTFS disable the last access update. For example it was disable by default on Windows Vista - Page File can be cleared during a |

| | | |
|----------------------|--|--|
| | | normal shutdown |
| Timeline Analysis | <ul style="list-style-type: none"> - Data Sources - Time Formats - Files System Metadata - Event Logs - Registry Data - Prefetch Files - Determine Events into a Timeline | <ul style="list-style-type: none"> - Multiple data source will create more volume of timeline data making it difficult to extra necessary time-stamped data. The data collected have to be convert into a more normalized format - Different method required to break down event files for data found on Windows XP system and Windows 7 for timeline analysis - Current no commercial Forensic analysis application allows Digital Forensic investigator to create timelines from all available data collected just by clicking a button |
| Application Analysis | <ul style="list-style-type: none"> - Log Files - Dynamic Analysis - Network Captures - Application Memory Analysis | <ul style="list-style-type: none"> - Large list of applications available and is just too long to provide a complete view of everything - Assumption is being made all the time especially when not able to find the clues on the existing prefetch file - Additional analysis might be needed to identify the situation that made lead to the artifacts being created or modified |

3.1.2. Review of Current Windows 8 Issues And Problems

The current Windows 8 Issues and problems will focus on where the users are currently dealing with the problems and issues with Windows 8. In this review

there were two parts where users are currently concerned about which are the new user interfaces and the new security issues that may migrate from the previous versions of operating systems to the new Windows 8 system. Understanding the user's challenges can reflect on the new Digital Forensic challenges should any changes being made to improve the users experience on the system and the current security issues on Windows 8 may be useful in identifying the questions for this research.

The Time of India Website (2013), discussed the most common problems of Windows 8 Operating System. The top first problems that were raised by users are the missing start button. This change has made user experience without a central place for launching programs and changing settings. Windows 8 features a new start page that takes over the entire screen when using a web browser program. Users have to switch back to the start page and launch a different browser. Secondly, many programs are designed for older desktop mode and this might make users feels like running two different computers on the same machine, one example will be the Internet Explorer 10 browser, web pages that were opened in desktop mode will not appear when a browser is switched to the tile mode. Due to many popular programs that run only in desktop mode, it will make sense to do most of the work in desktop mode, however Windows 8 will always force a user into the tile mode when they start the machine. Thirdly, some of the settings are inaccessible such as the useful charms can be on the unseen right side of the screen, then users have to figure out how to access to them. It will be easier if using a touch screen monitor than using a mouse to control the views. Next, closing program has no clear way because there is no longer an "X" at any corner of a program. A user will require figuring out their own way to drag an application to the bottom of the screen and if they move too far to the left or right it will end up giving user multi-windows mode rather than closing the program. Lastly the multifaceted keyboard is making it easier for a touch screen but more difficult for mouse and keyboard commands.

The next issues will be the current security issues on Windows 8 as reviewed in the article by Phneah (2012), she warned about the security issues to be looked out for in Windows 8. Although a few promising features have

provided improved security within Windows 8 to decrease the likely chances of common attack, however in the article she quoted that Gerry Egan the senior director of product management for Symantec's Norton have pointed out that new features such as files scanning with Microsoft defender and Early Launch Anti-Malware (ELAM) making things more difficult, as malware is hard to prevent and if one way is blocked off, it can easily finds another way next easy way to counter the purpose (Phneah, 2012). The researchers Furtak, Bazhaniuk & Bulygin (2013) have proven that exploits that bypass Windows 8 secure boots where attacks are possible due to the Unified Extensible Firmware Interface specification's security was overlooked (Constantin, 2013). The researcher demonstrated two attacks that can bypass a secure boot in order to install a UEFI boot kit on affected computers. Next, threats from Windows 7 may alleviate to a Windows 8 system. Windows 8 has a backward compatibility with Windows 7 so some of the mutual legitimate and malicious programs can also run without any alteration on the Windows 8 devices (Phneah, 2012). As the users slowly move on to Windows 8 there are possibilities that malware designed for Windows 8 will eventually be noticeable. New cyber-attacks are targeting the Windows 8 platform with fake anti-virus and phishing attacks target at the current operating system. As reported in the article by Protalinski (2012), fake anti-virus has been created for Windows 8 that displayed a fake scanning result to threaten users to buy the fake anti-virus application label as a security tool made for Windows 8 (Protalinski, 2012). Another significant issue will be the phishing attack pretending to be from Windows 8 team offering free Windows 8 software through a website link requesting users to enter their login and password. Such social engineering issues with older versions of Windows Operating Systems are still not addressed in Windows 8 and have possibilities to be one of the biggest security issues where very little improvement has been made to protect users from such attacks. Especially in one of the security issues raised by Gupta (2012), who conduct an examination of identify any security issues related to Windows 8. He found out that is no official method to disable the Metro interface for Windows 8 and such screens have an important security risk when Metro takes over the entire screen space when the address bar becomes invisible. There are chances that users could

enter a phishing site by accident and could not tell the difference if the site is similar to the legitimate site (Gupta, 2012).

3.1.3. Review of Windows 8 Digital Forensic Issues And Problems

The Digital Forensic challenges in the Windows 8 operating system were impacted by the latest functions that were introduced to users. These new functions helped to improve a user experience in using windows, however there were possibilities that more consideration will be required during investigations in relation to these new technologies. The three possible Digital Forensic considerations consisted of the cloud Forensic issues related to SkyDrive, USB Forensic that related to Windows to Go and Anti-Forensic issues linking to the recovery options. Firstly the SkyDrive introduced by Microsoft as a file sharing host and was integrated into Windows 8 as a sync features making files available in the cloud but only for the files in the users SkyDrive folders (Bright, 2013b). SkyDrive automatically integrates across all Metro applications so that files can be opened and saved direct into SkyDrive making it more convenient for users to utilize the data without worrying about downloading the files or uploading the files. This can appear to be attractive options for users who rely mostly on a computer to store their files. The issues with cloud can impact the amount of potential evidences available to an investigator when collecting data in the system (Birk, 2012). A Digital Forensic investigator can lose control of the data stored in SkyDrive through the cloud environment and the evidential artifacts to support the investigation can be considered as not complete and not reliable. SkyDrive can pose unique Forensic challenges as supported by Lawton (2012) where he mention the need for better Forensic tools to extract evidence from cloud based environments. Cloud-based environments may include more evidences of the suspect activities and Digital Forensic investigation on cloud can be difficult because of the challenges with multi-tenant hosting, synchronization problems and techniques for choosing the right data in the log files. The challenges related to cloud computing consists of control of evidence and in the current situation law enforcement does not have enough physical control of the media and the network which the cloud services are based on.

The Windows 2 Go was included with Windows 8 Enterprise Version and provides the capability to boot off of a USB stick and allow users to have a full Windows 8 operating system running on their own computer. This technology boot on any kind of laptop for Windows, the benefits of this technology include a special boot disk that works like antivirus and computer Forensic. Users can run their corporate images on their home computer which can let them work from home. The technology introduces some risks as it allows mobile users to run Windows 8 on a different operating system without using up the disk space. Data security can be a threat because USB flash drive is portable and can carry so much data that it could be easily loss or stolen. The solution is to use a hardware encrypted flash drive that can be used to enhance better security, further authentication features and centralized device management. However, it can pose serious challenges in relation to the encrypted file system according to Bit Locker (Woodward, 2006) all the drive information is encrypted making the data unreadable. On the other hand, there are risks where potential data might not exist or be left behind on the suspect machine and once the USB is plugged off the session will expire after 60 seconds (O'Neill, 2013).

Lastly the recovery option introduces two new functions which are the reset and refresh artifacts. One of the main concerns will be that this function can be abused by the users easily as the refresh and resetting data takes about 24 minutes without BitLocker encryption and 6 minutes for a quick reset (Newman, 2012). Users utilizing this option will make it harder to recover any data without using more advanced tools or advanced methods to retrieve deleted data. This option can be ideal if the main purpose is to give away the computer system to a new user and having it clean just like what it was originally. In the past, most advanced users will consider the System Restore option to overwrite what they thought will be the damaged registry back to where it was. The step is to bring the system back to an earlier version so that the system could pretend the suspected changed that damaged the system has never occurred at all, however if all else failed, then the next step will be just reformatted the hard drive first and reinstalling windows in the system (Fulton, 2012a). The reason this function was introduced in Windows 8 did not consider the new issues and problems in the

Digital Forensic investigation. The impact is that it could clear up the important data that could help to solve a case. There are options such as doing a quick reset, full reset and refresh can change the original plan set out for the investigation where more steps were needed to recover the windows artifacts during an investigation.

3.1.4. Review of Windows 8 New Features Issues and Problems

The problem and issues for new features in windows 8 that can be identified will bring more consideration for investigator and challenges when conducting Digital Forensic investigation on a Windows 8 machine. The storage space features allow users to pool their system hard drive in a way they can be seen by the operating system as one large hard drive. The purpose of this is to keep track of free space across several disks so that users can automatically mirror their data to multiple disks as one thus keeping files safe in the event of hard drive failure (Cunningham, 2012). The changes in the RAID technologies can affect the data acquiring phase as multiple disks of different sizes and interface needs to be considered. There may be chances that files being duplicated across all of the drives to prevent data loss just to prevent data loss, however can reduce the amount of space available for data storage.

Another new feature is the hybrid boot the purpose was to improve the boot times as it does not usually shut down the computer but instead goes into a hibernate mode where it stores a state with the drivers, services and other software that were loaded into the memory. However this feature may cause issues where some drivers which are not compatible can refuse to hibernate properly and the corrupted boot data can prevent Windows 8 from booting as normally. The things to consider during Digital Forensic investigation will be the memory dump and handling the OS kernel on the hard drive when the OS kernel goes into hibernation. One of the problems related to hybrid boot can also be linked to the exploits that can bypass the secure boot which was overlooked because an attacker can gain code execution rights on the system by exploiting the vulnerability in the popular applications such as Adobe Flash or Microsoft Office (Constantin, 2013).

Windows 8 has introduced a new start and metro style modern user interface. A menu bar appears that is known as Charms Bar that provides a quick way to jump to the most commonly used tasks. In Windows 8.1 many new features will be offered as improvements from Windows 8 could have the possibility to change the way Forensic artifacts in the machine are being discovered during the investigation. The new addition included in the Charm Search will be “Search Everywhere” functions that will let users search for their files, settings, applications and the website at the same time. The new search feature will only be available in Windows 8.1 that will give an investigator another source of search charm data. The source of data contains the historical result from the search which a user conducted when using the search charm in Windows. In order to ensure that the LNK files linked with search charm history, it is required for tools for analysis to parse shall item ID list and beware that same keywords search on a later search will not change the file content or file system timestamps of the LNK file. This implies that LNK files will only be used to identify the first timestamp if a similar search was executed (Hale, 2013). This can be a problem during analysis on the LNK files history because when multiple searches are being conducted the history will not be recorded.

3.2 SELECTION OF RESEARCH PROBLEM

In this section the selection of research problems will follow the sub section where 3.2.1 will focus on the relevant analysis methods for Windows Artifact to conduct events and timeline analysis based on the evidence acquired from the suspect machine. The next sub section 3.2.2 will look into the security issues that are targeting Windows 8 machines and the trend for computer misuse cases occurred on a Windows 8 machine. The section follows the reasons of why Windows 8 can be infected by malware and can be targeted by attackers therefore the need to have a Digital Forensic professional being well trained to deal with computer misuse issues on the Windows 8 system. Sub section 3.2.3 will explored the possible new challenges that can impact a Digital Forensic investigation to look for a suitable research question based on one significant feature that can be

further explored. Sub section 3.2.4 will outline the challenges that were present in the key artifacts in Windows 8 new features. The purpose was to determine whether these key artifacts in Windows 7 are still available in Windows 8 and whether any new features pose new challenges to Digital Forensic investigation.

3.2.1. Relevance Past Windows Platform Issues And Problems

The relevant past issues and problem that would be the focus in this research will be on the Windows Artifact. This section will cover the relevant analysis method that was used in past research for Windows Artifacts and to conduct events and timeline analysis on a suspect machine. Rob lee (2012) and SAN DFIR faculty has created a poster to assist in answering analysis questions during the Windows Artifact Analysis. This poster was proposed to help investigators to remember where to discover key items to reconstruct activity for Microsoft Windows. This cheat sheet listed out the different interesting areas in Windows Artifacts that can relate event construction and also the interesting challenges to Digital Forensic investigator of Windows systems. This sheet was intended for Windows 7 operating systems, however the details in the list may not be the same for Windows 8 operating system artifact analysis and this may provide new challenges for an investigator to follow the key activities a suspect. The relevant windows artifact is picked out in the list below were meant to assist an investigator to minimize problems and issues that can occur when looking for potential evidences in windows systems. These series of artifacts can assist the investigators to determine whether the particular event has occurred before and if any related artifacts can produce similar events that can point to the same activity. These locations of the items can act as an important guide during analysis process and help the investigator to answer specific questions to reconstruct of the suspect activities.

Table 3.3: Windows Artifact Analysis Cheat Sheet (Adapted from “Digital Forensic and Incident Response Poster” (Lee, 2012))

| WINDOWS ARTIFACT ANALYSIS CHEAT SHEET | | |
|---------------------------------------|-----------------|----------------------|
| File | Download | - Opened/Saved Files |

| | |
|--|---|
| Evidence | <ul style="list-style-type: none"> - Email Attachments - Skype log chat session and files transfer - Index.dat for file downloaded |
| Program Execution | <ul style="list-style-type: none"> - User Assist to track program launched in desktop - Last executed files by an application - Run command executed - Application compatibility cache - Taskbar Jump List - Prefetch files and Services Events log files |
| Files Created and Opened Timeline | <ul style="list-style-type: none"> - Saved and Opened Files - Last executed files by applications - Recently files opened - Shall Bags - Shortcut files (LNK) - Taskbar Jump List - Prefetch files - IE history files |
| Deleted files | <ul style="list-style-type: none"> - Search Assistant search history - Keywords search from START menu - Last executed files by application - Hidden file in directory (Thumbs.db) - Recycle Bin - IE history files |
| Physical Location | <ul style="list-style-type: none"> - Current system Timezone - Network History - IE cookies - Website visited date and time |
| Drive Usage | <ul style="list-style-type: none"> - USB key identification - USB device plug and play times - GUID from a Mounted Devices - Volume Serial Number - Drive Letter and Volume Name |

| | |
|----------------------|---|
| | <ul style="list-style-type: none"> - Shortcut files (LNK) Files - Plug and Play Event Log |
| Account Usage | <ul style="list-style-type: none"> - Last password change on system - Last Login time on system - Successful and failed login on system - Login types for account - Remote desktop usage |
| Browser Usage | <ul style="list-style-type: none"> - IE History - IE Cookies - IE cache files for webpages contents - Automatic Crash Recovery in browser - Local stored object and flash applications |

3.2.2. Relevance Current Issues And Problems in Windows 8

The selected relevant current issues and problems in Windows 8 will focus on the security issues that are targeting the Windows 8 machine. Improvements in the Windows 8 helps to deliver software solutions that fight against cyber security threats and Windows 8 contains considerable security updates that enable users to stay ahead of the threat landscape and provided better malware prevention and data protection. The Microsoft Business (2013) website reported that there are still chances that Windows 8 can be infected by malware and with hackers currently targeting not only small and large organisation but also government sector and non-profit sectors. There is a growing trend of the black market selling of customer's personal data and credit card information and the hacker focus is now on information theft and taking control of a user's pc. The attacks target focus on specific targets, data theft such as user's private information or using a computer as a combine launch such as botnet to launch a denial of service attack. The hackers are now increasingly are well-funded professional, teams and nation states compared to the past where hackers were largely unfunded and unorganized individuals. In the past hacker attacking a system was for the purpose of fame and reaching out to the company's lack of security on their system, however

nowadays the cases for misusing of computers are mainly for the purpose of profit, stealing confidential information and disruption of services. This is due to the easily attainable incentive from the black market in the current times as compared to the past where there is no specific market place for a hacker to sell the data they obtained (Microsoft Business, 2013).

Nevertheless the Windows 8 operating system can be used by a hacker to commit crime and therefore law enforcement has to keep up with the changes to deal with Windows 8 machines. Computer misuse can also happen on Windows 8 and according to the Security Intelligence Report volume 15 by Microsoft Corporation, which analyses threat from more than 1 billion systems worldwide, the report found that in the first half of 2013, nearly 17% of computers were still vulnerable to malware despite running up to date real time security products from Microsoft. Windows 8 encounters the similar amount of malware as compared to the amount of malware from Windows XP and Microsoft has urged users to switch to Windows 8 for the sake of better security (Greene, 2013). With more users recommended moving up to Windows 8 that would mean that a Digital Forensic professional would have to be properly trained in dealing with computer misuse cases on the Windows 8 system.

3.2.3. Relevance Windows 8 Digital Forensic Issue And Problems

Since the release of Windows 8 operating system, research has started to explore the possibilities of the new challenges that can impact the Digital Forensic investigation. The consideration to select a suitable research question will look into one of most significant features. The recovery options in Windows 8 will still need to be further researched and explored. The recovery option consisted of reset, refresh, system restore and system image recovery. These options were there to provide users a certain level of comfort should there be security threats such as virus and malware accidentally installed on their computers that causes error to the system. Another situation will be when users decided to give away their computer to another person or dispose their computer, they will need to remove the already existing data so that it is not to be visible to other users.

Nevertheless the recovery function will be there to benefit most users of Windows 8 as it has the potential to be used to correct any errors caused by computer software issues with just one click on the reset or refresh depending on any decision any users want to do with their machine. The reason why reset and refresh function was being researched widely was due to the interesting challenges presented when such options are being abused by users with the intension to destroy potential data in the system. This is a new challenge for Digital Forensic investigators because important data could be deleted or altered.

3.2.4. Relevance Issues And Problems In Windows 8 New Features

The relevance problems and issues in Windows 8 new features will focus on the new Digital Forensic changes and challenges that were present in the key artifacts. The key artifacts which were present in the earlier version are still around in Windows 8 and the immersive experience from the Metro User Interface is something new to investigator as most of the applications in Windows 8 are associated with a Microsoft Account. The artifacts from the Metro User Interface that existed only on a Windows 8 machine provided different registry keys information, artifacts from the new Metro User Interface and the Immersive Web Browser. With windows 8.1 releases on 17 October 2013, the new changes were intend to improve the current Windows 8 but there are many new possibilities that can be explored on finding the potential data for confirmatory analysis on whether there is such data existing on a system based on the research and also event reconstruction analysis during the analysis phase of the data acquired. The focus will be on the some of the significant new features such as the new File Explorer, Metro User Interface and the new task managers. The purpose was to research how these new features can make a different when doing Windows Artifact analysis after Windows 7 is preceded by Windows 8.

3.3 RESEARCH QUESTION AND HYPOTHESIS

The developing of questions is based on the article by Lipowski (2008), where the author described using three steps to produce some great research questions. It is

recommend asking interesting questions, selected the appropriate question for the research which can turn into a testable hypothesis (Lipowski, 2008). The questions asked must address the problem areas in the research and provide new perspective to gain knowledge on something new. The next section will review the challenges for Digital Forensic that are impacted by the Windows 8 new features which will assist with the selection for the best research questions and testable hypothesis for this research.

3.3.1. Review of Challenges in Windows 8 New Features For Digital Forensic Investigation

The review of articles caught the attention of the new features in the Windows 8 operating system. In particular the recovery option that was introduced in the Windows 8 Operating system that will benefit users and system administrators that can provide technical support on the Windows 8 Operating System. The recovery option is recommended to be used to correct the error caused by any computer software issues by just selecting the reset or refresh options in the recovery option. When these options were used the question is how they can influence the Digital Forensic investigation on the machine and when new features were introduced in Windows 8 what are the new features that benefit the user's experience but end up causing issues for Digital Forensic investigation. Further attention will be the Digital Forensic process on the Windows 8 machine and how would existing Digital Forensic steps such as acquisition and analysis of Digital Forensic evidence on the Windows 8 machine change as compared with other versions of the operating system in Windows Forensic. Also when using tools to collect potential evidence how these tools can be compatible to a Windows 8 machine or whether more tools were required to conduct a better analysis to ensure better efficiency when doing confirmatory analysis on the evidence collected.

3.3.2. Research Question And Sub Questions

Based on the review of the selection of relevant issues and problems, the research will focus on Windows 8 New Features and challenges of Digital Forensic

investigation when dealing with the fast changing operating system platform. The selection of research questions is as follows:

MQ→What New Features in Windows 8 Operating System Poses new challenges to the Digital Forensic investigation?

The following sub-questions are connected to the main question:

SQ1→ How can we tell the differences on the data collected on the different recovery options from Windows 8 machine?

SQ2→ Which Digital Forensic tools can work effectively to extract and collect data from Windows 8 machine for confirmatory analysis

SQ3 →Where can potential evidence for event reconstruction analysis found on Windows 8 machine?

3.3.3. Hypothesis

The following testable hypothesis listed out below can lead to answers the sub-questions:

H1a→ The data found in different Recovery options is different.

H1b→ The data found in different Recovery options is similar.

H2a →Only one Digital Forensic tool is required to effectively extract and analyse data from Windows 8 machine for confirmatory analysis

H2b → More than one Digital Forensic tool is required to effectively extract and analyse data from Windows 8 machine for confirmatory analysis.

H3a →Using file analysis, registry analysis, timeline analysis and applications analysis allows a Digital Forensic Investigator to find potential evidence for event reconstruction analysis in a Windows 8 machine.

H3b →Using file analysis, registry analysis, timeline analysis and applications analysis does not allow a Digital Forensic Investigator to find potential evidence for event reconstruction analysis in Windows 8 machine.

3.4 RESEARCH DESIGN

The research design outlines Case Based Reasoning as the paradigm for this research to acquired specific knowledge based on previous experience from Windows Forensic. This section will discuss the Digital Forensic process chosen from the list of Digital Forensic models available. The forensic process chosen will be the hierarchical, objectives-based framework for Digital Forensic investigation by Beebe & Clark (2005), and this framework will be followed through the research as the standard guideline. The research phases will be covered in sub section 3.4.3 together with the data map in sub section 3.4.4. The pilot test is plotted out to ensure that the required data were collected for the research to ensure that everything works out as according to the plan. After that the section 3.5, 3.6, and 3.7 will list out the data requirements for the research, the intend method on how data were collected and the intend method to conduct analysis on the data collected with the final section ending with the limitations that were considered when conducting this research.

3.4.1. Case Based Reasoning

Case based reasoning will be the paradigm used in this research to gain specific knowledge based on the previous experience of an actual problem scenario (Aamodt & Plaza, 1994). In another introduction by Kolodner (1992), she describes that he case-based reasoning uses old experiences to understand and solve new problems. When using case-based reasoning, a participant remembers a previous situation that is similar to the current one and uses that to solve the new problems. Case-based reasoning is similar to adapting an old solution to encounter new questions where using old cases to explain a new situation and analyse new solutions. The Case-based reasoning that can be incorporated in this research that consists of the four-step process as shown in the table 3.4 below.

Table 3.4: Case-based Reasoning Process for This Research (Adapted from “Case-Based Reasoning: Foundational Issues, Methodological Variations, and System Approaches” (Aamodt & Plaza, 1994))

| Steps | Process |
|--------------|--|
| Retrieve | Given a research question, retrieved from the list of past problem and issues that is relevant to the questions. |
| Reuse | Map the solution from the past research question that is related to the target problem. |
| Revise | After mapping the past solution from the past research question to the target problem, test out the new solution in the real world and revise it |
| Retain | Once the solution was adapted into the target problem successfully, the resulting experience was stored as a new case in memory. |

Case-based reasoning is also used extensively in day-to-day common-sense reasoning and was supported by Leake (2002) as solving a new problem and construes a new situation by applying comparable previous incidents. The author described a case based reasoning is similar to retrieval, analogy, adaption and learning which is related to the development of the methodology for this research (Leake, 2002). For Digital Forensic investigation, case based reasoning can be linked to the research done by Horsman, Laing, & Vickers (2012), to improve the trustworthiness of results obtained from digital investigation by using the results from previous Digital Forensic examination and reused to audit the risks faced in the current Digital Forensic investigations. This according to the authors will overall improve the problem solving process and provide a higher potential accuracy on the Digital Forensic process (Horsman, Laing, & Vickers, 2012).

3.4.2. The Digital Forensic Process

The Digital Forensic process that will be used in this research will be based on the approach used by Beebe & Clark (2005), the methods they proposed is using a hierarchical, objectives-based framework for the Digital Forensic investigation

process. This framework has two tiers and the first tier consisted of six phases where the first phase will be the preparation of the suitable equipment for investigation. Second phase will be the incident response that is to identify a plan to respond to the incident. Third phase will be the data collection phase where collecting the relevant digital evidences to support the case. Forth phase will be data analysis phase that will further enhance to survey, extract and reconstruct the collect data for evidence. The survey part is used to describe the digital landscape by mapping the file system and locations where the files reside on. Followed by the Extract where the Extract data will be based on the objectives using techniques. For example, keyword searching and filtering of the data collected. Finally the examination of the extracted data for reconstruction and confirmation analysis to support the objectives is done. After the data analysis phase is completed, the fifth phase will be the presentation phase. This phase is often used as documentation where information is recorded during the investigation process to communicate the findings to the intended audiences. Incident Closure is the last phase critically reviews all the investigation process to identify and incorporate lesson learned that matches what is required in Case Based Reasoning.

3.4.3. Research Phases

The research phases will consist of six phases and each of their objectives are shown in the table 3.5 below.

Table 3.5: Windows 8 Research Phases Objectives (Adapted from “A Hierarchical, Objective-Based Framework for Digital Investigation Process” (Beebe & Clark, 2005))

| Phases | Objectives |
|-------------------|---|
| Preparation Phase | <ul style="list-style-type: none"> • Setup 2 Windows 8 machine in the laboratory in a way that can increase the availability in support of detection, response, investigation related to computer security incident • Look out for any risks, |

| | |
|--------------------------------|--|
| | <p>vulnerabilities and threats that may occurred during evidence acquisition on the Windows 8 machine</p> |
| Incident Response Phase | <ul style="list-style-type: none"> • Validate the incident occurs on Windows 8 machine • Formulate the investigation plan for data collection and analysis on Windows 8 machine • Formulate the tools used for investigation and analysis on Windows 8 machine |
| Data Collection Phase | <ul style="list-style-type: none"> • Conduct data acquisition and attempt recovery of any hidden data on the Windows 8 Machine • Ensure data integrity and authenticity of the digital evidence in Windows 8 Machine • Using Write Blocker to generate MD5 hashes on all digital evidence files |
| Data Analysis Phase | <ul style="list-style-type: none"> • Transform the data collected from Windows 8 machine to a more manageable size • Answer the sub questions by examine, analyse and reconstruct event based on data collected |
| Presentation of findings Phase | <ul style="list-style-type: none"> • Test Hypothesis for H1a against H1b and present findings |

| | |
|------------------------|--|
| | <ul style="list-style-type: none"> • Test Hypothesis for H2a against H2b and present findings • Test Hypothesis for H3a against H3b and present findings |
| Incident Closure Phase | <ul style="list-style-type: none"> • Preserve new knowledge gained during the investigation and use it to enhance future investigation • Critical Review on the entire process on any challenges involved during the investigation |

3.4.4. Data Map

The steps for all the data collection and management processes are summarised in figure 3.2 below.

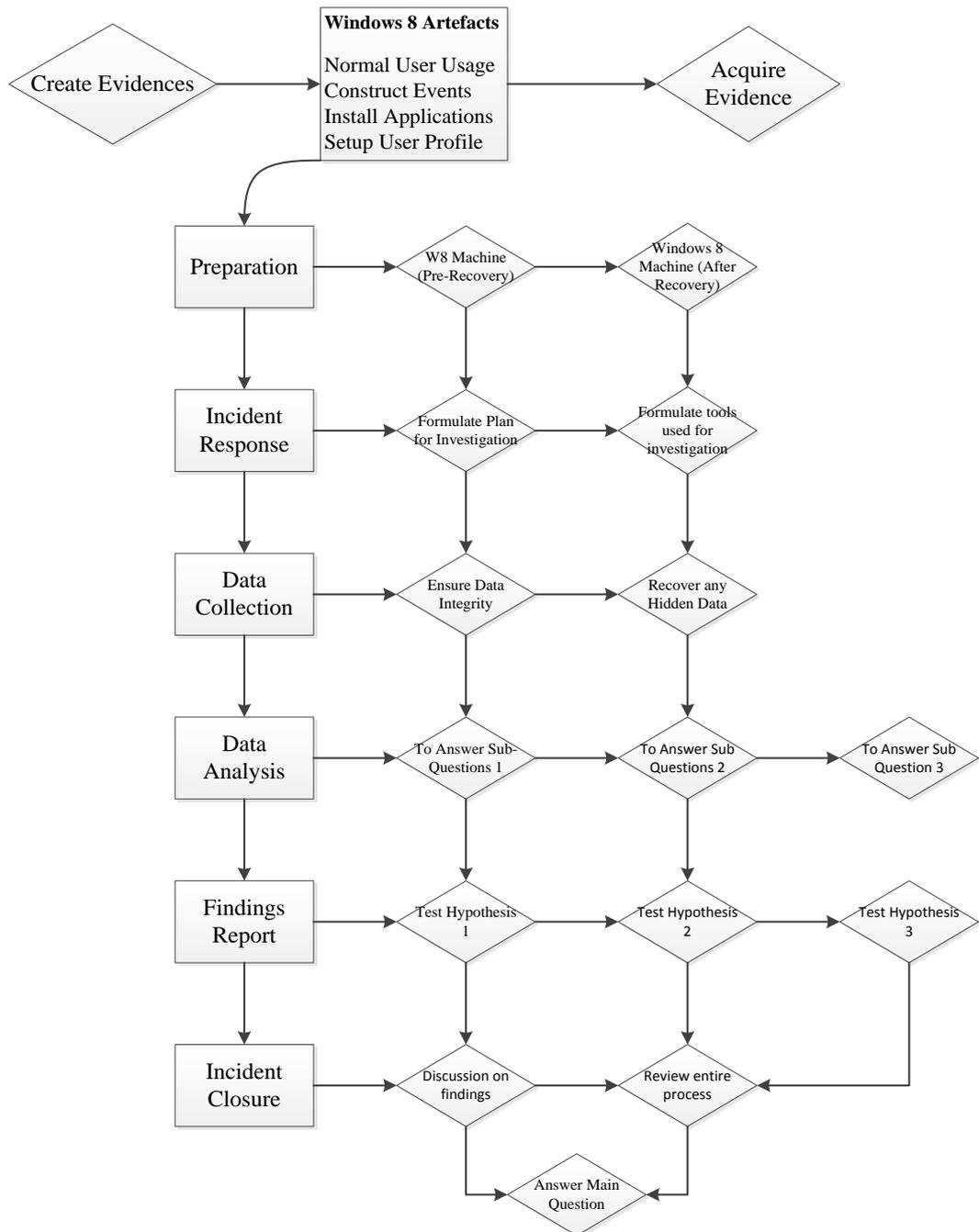


Figure3.2: Data Map for Windows 8 Research. (Adapted from “A Hierarchical, Objective-Based Framework for Digital Investigation Process” (Beebe & Clark, 2005))

3.4.5. Pilot Test

In order to ensure that the desired data were collected for the research and everything works out as planned a pilot run is required. A pilot test will be required on the pre-recovery machine and this is to make sure that the Windows 8

machine has the totality of all the data. The pre-recovery machine must meet the objectives set out to reconstruct the event analysis. This is also used as the preparation phase that was set out in the methodology in the case of any failure in this stage then the methodology will have to be reviewed again.

3.5 DATA REQUIREMENT

The testing will follow case based reasoning scenarios of the past related problems for files analysis, registry analysis, timeline analysis and applications analysis on a Windows 8 machines to be used in the lab environment. The scenario was setup based on the Windows artifact analysis poster created by Lee (2012) as the cheat sheet to help investigators remember the key items and the activities to look out for in Windows operating system. The Windows 8 machine will be setup to generate the intended data in order to provide answers to solve the sub-questions asked in the research. The preparation phase and incident response phase will be recorded so that during the presentation of the findings phase the process can be compared with the guideline recommended by Sommer (2012), on the risk scenario to identify the possible source of evidence and loaded into the laptop before any recovery options are being used. Encase V7.05 will be used to perform the data acquisition on the Windows 8 machine. The data acquisition will be first done on the laptop before any recovery options are being used and after that on the similar machine where data recovery options such as the reset and refresh PC are being executed. The data will be created on a control scenario with all details recorded. Each type of data created will be verified to ensure that all data entered in the Windows 8 machine are correct.

3.6 DATA COLLECTION

The testing variable will be collected based on the data collection phase in the Digital Forensic methodology proposed by Beebe & Clark (2005) with the goal to increase the availability of evidence acquire from the hard disk and to ensure the integrity of evidence during the Digital Forensic process. The Digital Forensic tools Encase will be used as the Forensic tools to collect the evidence and if required other Forensic tools will be enforced to further collect any other

evidence on the hard disk. Tools are used to collect any data found in the Windows 8 machine and review how much the data is created during the preparation phase that can be acquired by the existing tools. The variables for Windows artifact analysis will consist of a data the file created, the time the files were created, the path the file resides in, the time the file was modified and if files was attached in an email then further action will be required to look out for the time the email was sent and received. The variables for Internet Explorer will be the search history, the content of the file and the internet cache history. The MD5 values for each file found by the tools will be recorded to ensure the authenticity and data integrity. Before any recovery options were utilized all the data created must be the expected data to be found, if not further investigation will be required to find the missing or hidden data. The percentage of expected data can be justified by the total data found and total data created can be calculated as follows below:

Percentages of expected data found (X) = Total Data Found (Y) divided by Total Data Created (Z) times 100

This value will be the actual percentage of the expected data collected without any changes made. The values will then be used to determine the differences on the data collected for pre-recovery and after the recovery options been utilized in the Windows 8 machine. The percentage of the successful data collected after recovery options utilized can be justified by the total files found in the after recovery options utilized can be justified by the total files found in the after recovery machine as follows:

Percentages of successful number of file found (X) = Total Files Found (Y) divided by Total Files Created (Z) times 100

In the data collection phase, hypothesis can be used on the total data collected on the pre-recovery and after-recovery machine in order to answer the sub-question on what are the differences on the data collected on the different recovery options from Windows 8 machine. The hypothesis can be “H1a→ the data found in the pre-recovery machine and after-recovery is different. However if Hypothesis H1a is proven false, then hypothesis H2b will need to be tested for the argument on why the data collected is similar.

3.7 DATA ANALYSIS

The data collected will be transformed into a more manageable size for analysis. In this phase, it will be using confirmatory analysis to determine if the windows artifact is available in the data collected. At this stage, the sub questions will be asked to be answer upon the hypothesis and whether the hypothesis can be constructed at this stage to confirm or refute allegation of any suspicious activities (Beebe & Clark, 2005). This relates to Mandia & Prosis (2003) description where they state “Single data analysis can be divided into “Data Preparation” and “Data Analysis” Sub Phases. The data analysis approach will follow the Data Analysis Phase in figure 3.3 below.

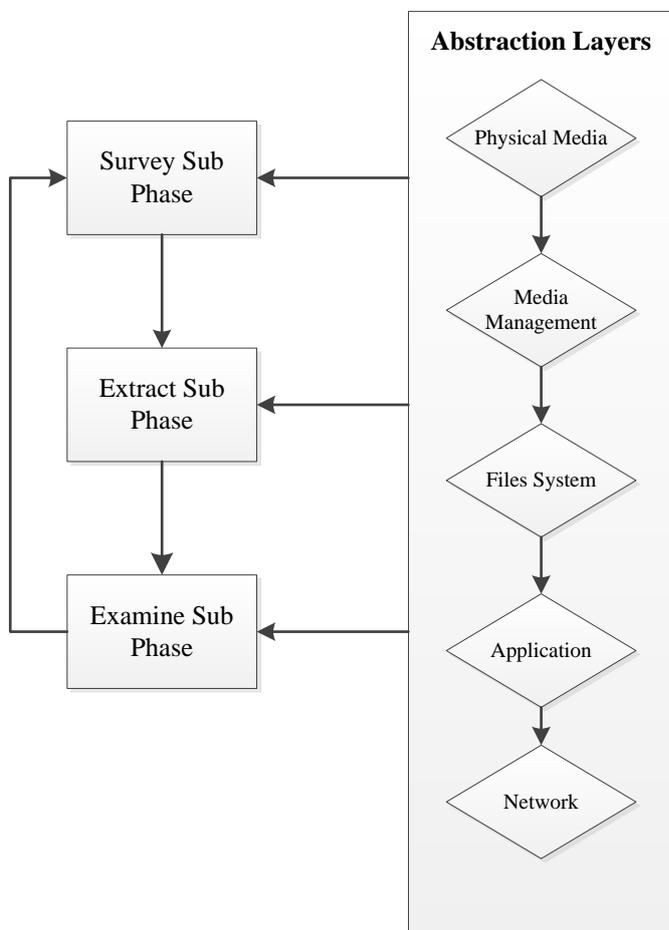


Figure 3.3: Data Analysis Guide for Windows 8 Research. (Adapted from “A Hierarchical, Objective-Based Framework for Digital Investigation Process” (Beebe & Clark, 2005))

In the data analysis stages, for the sub-questions to find how effective are the current Digital Forensic tool available for Windows 8 machine, the question “Which Digital Forensic tools can work effectively to extract and collect data Windows 8 machine for confirmatory analysis?” was asked and can be answered based on the existence or non-existence of digital evidences extract by the tools that is used. The hypothesis can be “H2a → Only one Digital Forensic tools is required to effectively extract and analyse data from Windows 8 Machine for confirmatory analysis.” Or “H2b → More than one Digital Forensic tool is required to effectively extract and analyse data from a Windows 8 machine for confirmatory analysis.” For the sub-question to analyse the new features in Windows 8, the question is asked is based on “Where can we find potential evidence for event reconstruction analysis on a Windows 8 machine?” The question can be answered based on the event reconstruction analysis done on the Windows 8 machine for the different recovery options by using Files Analysis, Registry Analysis, Timeline analysis and Application Analysis to look for potential evidence. This can lead to answer the questions with the hypothesis “H3a → Using file analysis, registry analysis, timeline analysis and applications analysis allowing a Digital Forensic Investigator to find potential evidence for event reconstruction analysis in a Windows 8 machine.” Or “H3b → Using file analysis, registry analysis, timeline analysis and applications analysis does not allow a Digital Forensic Investigator to find potential evidence for event reconstruction analysis in Windows 8 machine.”

3.8 LIMITATIONS OF RESEARCH

The research will focus on the challenges of new features and the impact of the new features that may affect Digital Forensic investigations. The first limitation of the research will be the Digital Forensic tools. There are many tools that were available to conduct the Digital Forensic investigation and because of time resource limitations not all the tools that were currently available will be used in the experiments. The second limitation of the research will be the Digital Forensic investigation method to conduct the experiment, as it was known to have at least

10 to 15 types of Digital Forensic models available that can follow as guidelines to conduct experiments. The Digital Forensic investigation models were narrowed down to three and finally only one model of the three reviewed on the literature will be a standardized method to follow for the experiments. Thirdly due to the time limitations not all the new features in Windows 8 can be tested in the research the selection will narrow down to test the recovery options and from there explore the Digital Forensic implications. Fourth not all the problems and issues discussed in the chapter will be explored. In the research the problems and issues will only be raised if there is an occurrence with Digital Forensic implications. Fifth will be the case scenario that is planned for the experiments, there can be many case scenarios available that can be selected to conduct the experiment but only one has to be chosen. The case scenario will not be able to focus on every aspect of a computer misuse case such as attacking a computer system or downloading a malware into the machine. The scenario will be based on normal user usage and the device use in the suspicion of a computer misuse case on a Windows 8 machine. Finally the last limitation will be the number of machines available to conduct the experiment, as only one Windows 8 machine is available for testing therefore the machine will have to be re-used, after each case scenario and the process will have to be repeated on the same machine again.

3.9 CONCLUSION

In this chapter previous problem and issues of similar studies were reviewed in section 3.1 that consisted of four sub sections to analyse at these two to three problems and issues related to Digital Forensic investigation. The review attempted to look at past Windows issues first related to data acquisition problems and then the data analysis problems that were noted by Digital Forensic researcher. The next review will be the current windows 8 issues and problems that follow the user's interface challenges and the security threats that could impact on the Windows 8 machine. The possible challenges to Digital Forensic investigation from SkyDrive, Windows 2 Go and Recovery Options were reviewed in sub section 3.1.3 and the possible problems and issues that are useful

for Digital Forensic investigator to consider for the Windows 8 new features such as RAID technologies, Hybrid boot and Charms Bar that were introduced in Windows 8. The section 3.3 describes the section of the research main questions, sub questions and the hypothesis. The research design was outlined in 3.4 for Case Based Reasoning to create a similar scenario based on the past research and the Digital Forensic process that describes the research phases, the data map that follows the phases of preparation, incident response, data collection, data analysis, findings report and incident closure. Pilot testing was planned to ensure that data on Windows 8 machine before any recovery options were utilized to make sure that methodology worked as expected. The Data Requirement aims to prepare the Windows 8 machine to generate intended data in orders to answer the sub questions in the research and finally the main question of the research. The data collection and data analysis discussed in the section 3.6 and 3.7 to ensure that testing is conducted to obtain results that are expected outcomes and correct in order to test the hypotheses formed in sub section 3.3.3 to answer the sub questions.

Chapter 4 will outline the details on how data were gathered using the methodology stated in this chapter. The findings of each phase based on the Hierarchical Objectives will be recorded and any variation made during the research experiment will be updated. The next chapters will also include the report of the data collected, analysis of the data collected and the findings presented in this research.

Chapter 4 – Research Findings

4.0 INTRODUCTION

In chapter 3 the methodology of the research was outlined and the research questions together with sub questions and hypothesis were defined. The methodology defined in chapter 3 has been used to deliver the results reported in this chapter 4. In this chapter, the findings from the experiments are reported. The chapter starts with first reporting alterations to the research phases that were caused by the limitations listed out in 3.8 of chapter 3. When preparing for the research some challenges were recognized and rectified to ensure that the experiment can be completed and met the objectives of the research. Section 4.1 outlines the changes of the data requirement, data collection and data analysis.

The second part of the chapter outlines the preparation phase of data for Windows 8 machines. This section details the types of equipment available in the laboratory. The Forensic techniques were recorded in sub section 4.2.2 on how data were acquired from the Windows 8 machines followed by the list of forensic tools chosen for the experiments. The Windows operating system data created as the potential evidence were recorded based on the types of data created, application used and the task conducted. The third part of the chapter reports the incident response phase for Windows 8 machines acquisition and in this part the scenario for Windows 8 machine acquisitions were described accordingly; on the before recovery machine, after refresh machine and after reset machine. The changes found on Windows 8.1 upgrade were also reported and also the recovery option to remove all files for the after reset machine were recorded. The fourth part of the chapter details the data collection phases by summarising the report from the acquisition tools which also includes the data verifying and processing of the images files collected using Encase 7. The final part is the analysis phase for Windows 8 machines acquisition. These parts will be grouped into three parts in order to answer the sub questions as plotted out in the methodology on chapter 3. The three parts included the data existence for different recovery options, the

tool's efficiency during analysis phases and the potential evidences found on machine with different recovery options.

4.1 ALTERATION IN RESEARCH PHASES

A number of challenges were uncovered when conducting the experiments which required more time and resources to successfully complete the experiment. Based on the Data Requirement, Data Collection and Data Analysis outlined in Chapter 3 there were some changes made to ensure the experiments can be carried as planned in the research methodology. The changes made creating the types of evidence feasible for the data requirements listed out in sub section 4.1.1 and sub section 4.1.2 and for data collection were altered to ensure the ability to increase the availability of evidence acquired from the hard drives of a Windows 8 machine by not removing the hard drive from the machine to prevent the risk of spoiling the hardware on the machine if multiple times were required to remove hard drive from machine. The data analysis phases in sub section 4.1.3 will focus on comparing the differences of the Windows artifact found on each of the images collected and using tools selected to analyse the data collected. Changes also made to pilot tests will be discussed in sub section 4.1.4 that attempt to test on before recovery, after refresh and after reset machine to determine the existence of data available.

4.1.1. Data Requirement

A few challenges were uncovered during the attempt to test the experiment and these challenges require more time and resources to successfully complete the experiment. Firstly the varieties of past related issues on operating system was very wide and it needed many configurations to create all the key items as proposed in the Windows artifact analysis poster cheat sheet created by Lee (2012). The keys items to be created as evidence were narrowed down. The types of evidences generated from users then had keywords search in Google and websites visited. Also the pictures created by users and text files images created by users in the Windows 8 machine. The Sky Drive images and document

uploaded by users. The emails sent and received by users. The calendar entries and the application installed in Windows Store. The messaging text sent and received by users via the messaging function for Microsoft account. The second challenge was the changes in Windows 8 which removed msn messenger and mail application and are merged to the new People feature in Windows 8. There may be difficulties in tracking the message and mail sent by the user from the machine. In order to successfully track the emails sent by users and messages sent using the immersive application, therefore thunderbird application and Skype application were installed so that the tools used in the experiment can successfully capture the data created.

Lastly the challenges of using the types of images created after utilizing the recovery options in the Windows 8 machine. The data requirement can be too huge if all types of images have to be collected after changes. To analyse the differences made to the machine for example in Windows 8 machine before the upgrade to Windows 8.1, the refresh before upgrade and after upgrade to Windows 8.1 was used. When using the reset features, there will be an option to either remove all the files from all drives or only one of the drives where Windows is installed. Another extra option to choose from will be removed files or fully clean up the drive. These can produce at least 5 to 6 images that will not be feasible for the experiment. The first set of images that were chosen to be used in this research had in the end be bought down to use only one benchmark image for pre-recovery Windows 8 machine. The second image for the after refresh where PC setting will be back to default and personal files will not change. The third image will be the after reset image to bring the machine back to default factory setting and fully clean the drives.

4.1.2. Data Collection

The data collections plan has also been altered to ensure the ability to increase the availability of evidence that can be acquired from the hard drive of the Windows 8 machine. Due to limited resources with only one machine used which has the Windows 8 installed. The initial plan of removing the hard drive from the experimental machine and attaching it to a write blocker before running the

acquisition has been forfeited. The removing of the hard drive from the machine might cause new damages to the machine especially when doing it multiple times after each change was made. This means after one image is collected then it needs to be attached to where it was originally and then run the system again in order to create the second image and so on. Doing this multiple times may cause a higher risk for the experiment so therefore another approach was proposed for the data collection steps. The alternate approach for data collection will be using one of the Digital Forensic toolkits available to run on the machine without tampering the target hard disk in order to collect the data for the experiment. For this research, DEFT8 ISO files were downloaded and installed into a pen drive so that the machine can boot the DEFT operating system to conduct data collection process. This method was conducted to reduce any risk from any accidental force that may destroy the experimental machine hardware during data collection phase. The method will also ensure data integrity and the authenticity of digital evidences collected from the Windows 8 machine.

4.1.3. Data Analysis

The data analysis phase will be altered from the original plan to focus on comparing the differences of the Windows artifact available between the three images that were collected. The confirmatory analysis will solely focus only on the files system discovered and applications installed on the window machine via the images collected so that further survey, extract and examine the existence and non-existence of the key items found between the three images. Using this method can effectively build the data collected into a more manageable size during data analysis. The steps will be first to survey the file created earlier on and determine their existence in the file system, followed by extracting the data from the Windows system registry keys files and then examine where such files were located in the file system. Doing these steps allows the available tools chosen for the experiment to determine the confirmatory analysis of the artifact found to answer the sub-questions. These can lead to potential evidences being discovered and the information found that can help as guidelines for an event reconstruction analysis based on the list of items found.

4.1.4. Pilot Test

The pilot test was initially planned for pre-recovery machine only but now will be included to test for the refresh and reset machine to determine the existence of the data available after refresh and reset has been done to the machine. The test will also include the Digital Forensic tools other than Encase V7.05 to conduct pilot testing to analyse data collected during the data collection phase. Doing this test can reduce the chance of any failure and ensure the availability of data. The selection of tools used in the experiment can also be finally brought down lesser numbers to be feasible for the research. The final selection of the tools used that will be further discussed in section 4.2.3 and the findings can be set out to answer the sub-questions on the effectiveness of digital tools to collect and extract data for Windows 8 machine.

4.2 Preparation Phase of Data for Windows 8 Machine

This section targets the preparation phases to setup the Windows 8 machine for the experiments. The sub section 4.2.1 recorded the equipment available for the experiments the laptop picked with Windows 8 installed will be Asus X201 laptop as the suspect machine, and DEFT 8 will be Digital Forensic tool kits used to acquire the hard disk image. Sub section 4.2.2 described the techniques and details each step that was done in order to obtain the data from the hard disk of the suspect machine. Next sub section 4.2.3 details the tools that will be used in the experiment with Guymager application deployed to handle data acquisition process. Encase 7, FTK imager, Bulk Extractor, Regripper and Registry Decoder to handle the analysis process. Lastly sub section 4.2.4 summaries the data prepared for the acquisition on the machine.

4.2.1. Equipment Available

The equipment used in the experiment consisted of one Asus X201 laptop, 2 x 500GB western digital portable hard disk drive and one bootable 8GB USB pen drive installed with DEFT 8. The DEFT 8 will be the Digital Forensic tool kit that was used to acquired all the data on the laptop without tampering any of the evidence created on the laptop. Windows 7 Enterprise desktop will be the the system

to analyse all the data acquired from the laptop hard disk drive. The table 4.1 displayed below summarises the equipment available for the experiment

Table 4.1: Equipment Available

| Equipments | Model | Serial No. | Size |
|-----------------------------------|------------------------------|-------------------------|-------|
| Asus X201 HDD | ATA ST320LT012- 9WS14C | W0V1ZPPZ | 320GB |
| Portable HDD 1 | My Passport 0748 | 57584731453832555843431 | 500GB |
| Portable HDD 2 | My Passport 0748 | 57583731413732532313132 | 500GB |
| Linux (DEFT8) | Linux Loop File Sytem | N/A | 1.6GB |
| Windows 7 Enterprise 64 Bit | WD- WCAYUEZ05122 | 88462 | 500GB |

Two Microsoft accounts were created to be used for communication purposes between emails and messaging. The main microsoft account will be the login to installed applications downloaded in the Microsoft Store and to transfer files from the local computer into SkyDrive. The laptop was setup with a login to the user local account first and then followed by signing in with a Microsoft Account online. The laptop will be running on Windows 8 operating system with 2GB of memory. The figure 4.1 below will displayed the actual setup with the equipmentavailable to acquire potential evidence on the laptop and the table 4.2 displays the details of the Two Microsoft Account Created for this experiment.

Table 4.2: Microsoft Account

| Username | First Name | Last Name | Email Address |
|----------------|------------|-----------|------------------------------|
| thesismfit2013 | Thesis | Mfit | thesismfit2013@hotmail.co.nz |
| thesismfit2 | Thesis2 | Mfit2 | thesismfit2@live.com |

4.2.2. Windows 8 Operating System Forensic Techniques

The Forensic techniques for this experiment will be first installed the DEFT 8 ISO on to the pen drive. To get it done, run the USB universal installer 1.9.3.1 program on a standalone machine to install a live version of DEFT 8 into the USB drive so that this can create the forensic toolkit into the bootable drive. The laptop must be able to boot from the pen drive successfully and load into DEFT 8 operating system directly without altering any data in the machine. In order to achieve this, the need to go into BIOS mode to change the setting so that it can boot directly to the USB to prevent it from loading to Windows 8 operating system directly. The method to this was to select the power off but instead of shutting down choosing restart the computer. While doing this method press and hold on the shift key will get to the advanced options screen. In the advanced options screen select the UEFI Firmware Setting will bring the up the boot menu to allow the change of boot setting by disabling secure boot, fast boot and enable launch CSM. Finally on the next boot up press the F12 key to allow system boot from USB pen drive. On the DEFT 8 operating system launch the Guymager application to conduct the acquisition process and remember to mount the hard disk drive where the image is needed to be stored into so that the image file acquired can be written onto the portable drive. The figure 4.1 below will displayed the actual Forensic techniques with the equipment available to acquire potential evidence on the laptop:

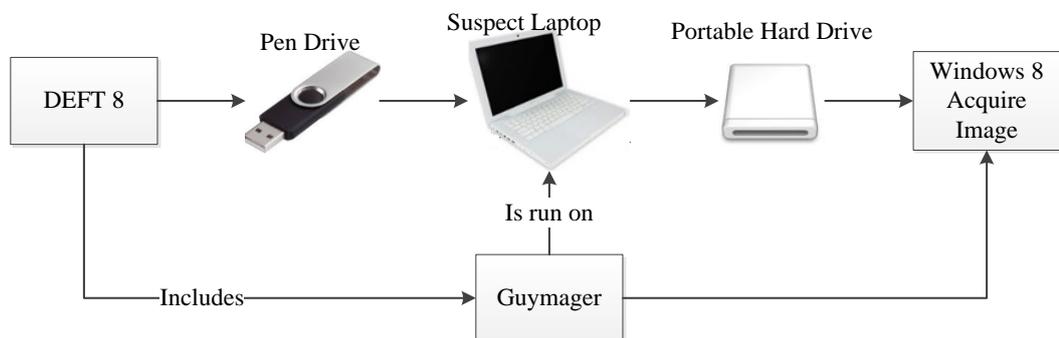


Figure 4.1: Forensic Techniques with Equipment Available to Acquire Potential Evidence on Laptop

4.2.3. Windows 8 Operating System Forensic Tools

The Digital Forensic tools that were used in the experiment consisted of DEFT 8 where Guymager application was deployed to handle the data acquisition processes on the Windows 8 machine. Once all the data needed for the experiment were acquired, the acquired image files were copied into the Windows 7 Enterprise standalone machine in the Forensic lab to conduct further analysis. Three different types of image files were acquired were saved into the portable hard drive and copied into the machine for analysis. The three different types of image files contained a before recovery, after refresh and after reset Windows 8 machine data. The Forensic tools to handle the data for analysis consisted of Encase 7, FTK Imager, Bulk Extractor, Regripper and Registry Decoder. The table 4.3 below shows the Forensic task for the research and the purpose of the tools in the research:

Table 4.3: Tools Chosen For Research

| Tools | Version | Forensic Task | Purpose of Tools |
|------------|------------|---------------|---|
| Guymager | 0.7.1 | Acquisition | To collect all the data from the suspect's machine |
| Encase 7 | 7.05 | Analysis | Validate the data collected from the suspect's machine and analyse the data found on the suspect machine |
| FTK Imager | 2,9.0.1385 | Analysis | Analyse all the file system of the suspect machine and check for unallocated space files in the suspect machine |

| | | | |
|------------------|-------|----------|--|
| Bulk Extractor | 1.4.1 | Analysis | Process the data obtain from the suspect machine to scan the disc image file for the specific email address and the keywords search on the suspect machine |
| Registry ripper | 2.8 | Analysis | Review the registry hive files and analyse the file path found on the registry keys of the suspect machine |
| Registry Decoder | R103 | Analysis | Review the registry hive files and analyse timeline found on the registry keys of the suspect machine |

4.2.4. Windows 8 Operating System Data

The operating system data created in the windows 8 machine for the experiment follows the regular tasks on what users are likely will do when using a computer. The action performed for this research to create data to prepare for the acquisition are summarised in the table 4.4 displayed below.

Table 4.4: Operating System Data Created

| Type of Data Created | Application Used | Task Conducted |
|---|--|--|
| Keywords Search | <ul style="list-style-type: none"> - Internet Explorer (Immersive and Desktop) - Charm Bar | 10 keywords search on google website and 10 keyword search on everything using Charm Bar |
| Website Visited | <ul style="list-style-type: none"> - Internet Explorer (Immersive and Desktop) | 10 Website visited |
| Emails sent and received | <ul style="list-style-type: none"> - Thunderbird - Mail (Immersive) | Sending/Receiving 10 emails from Immersive mail app using microsoft account and using Thunderbird application |
| Picture Files saved on My Documents Folder | <ul style="list-style-type: none"> - Windows Explorer | Uploaded 10 pictures on to the machine |
| Synconizing SkyDrive Documents | <ul style="list-style-type: none"> - SkyDrive | Upload 10 pictures/word documents to SkyDrive via a different machine and synconizing the files with Windows 8 Machine |
| Calendars Entries | <ul style="list-style-type: none"> - Calendars (Immersive) | 10 Test data added for calendar entries on machine |
| Text Document and RFT documents both saved on My Documents Folder | <ul style="list-style-type: none"> - Windows Explorer | 10 notepad text and 10 rich text format created |
| Messaging Text Sent and Received | <ul style="list-style-type: none"> - Messaging (Immersive) - Skype | Sending/Receiving 10 emails from Immersive messaging app using microsoft account |

| | | |
|-----------------------------|--|---|
| Installed Applications | <ul style="list-style-type: none"> - Skype - Avast anti-virus - Thunderbird email | Installed new application from installation file downloaded onto the machine |
| Micosoft Store Applications | <ul style="list-style-type: none"> - Micosoft Store (Immersive) | Review the applications already installed on machine and installed new applications selected from store |

4.3 Incident Response Phase For Windows 8 Machine Acquisition

This section will deal with the incident response phase for Windows 8 machine acquisition. The first part of this section will be the scenario for Windows 8 machine acquisition phases that describes each scenario based on the before recovery machine in sub sub section 4.3.1.1, after refresh machine in sub sub section 4.3.1.2 and after reset machine in sub sub section 4.3.1.3. The second part of this section in 4.3.2 describes the details of a Windows 8 machine that has been upgraded to the latest Windows 8.1 and any changes in this version were recorded for the incident response for the Windows 8 machine. The third part in the section 4.3.3 will be the recovery options that were recorded after each option was selected for after refresh and after reset.

4.3.1. Scenario for Windows 8 Machine Acquisition

The scenario planned for the experiment is a computer misuse case that has been reported and the investigation was carried out on the personal laptop which was owned by the suspect. In the three different scenarios the suspect has the administrator right for the laptop and can abuse the new features of the Windows 8 recovery option. The experiment was set out to determine the challenges for Digital Forensic investigation that were faced when investigating a Windows 8 machine. The three scenarios describe on the next sub-section also focus on issues

that may occur during the investigation of a computer misuse case and when potential evidence may be destroyed by a suspect.

4.3.1.1. Before Recovery Machine

The first scenario was a normal setup where no recovery option was being utilized. The pre-recovery machine was to capture all the data created for the experiment and work as the benchmark for the three images acquired. The potential evidences found can be helpful to answer the questions related to the analysing the existence of the data and to reconstruction of the event on the suspect laptop. The findings will be compared with data found on the second and third scenario to understand the traces of the missing data could have existed originally and the data that should be there but after changes made can no longer can be found anymore.

4.3.1.2. After-Refresh Machine

The second scenario was the after-refresh machine where a suspect attempts to remove the application manually installed on the laptop and revert the computer setting to default. The attempt in this investigation will using the same method for the investigation on the pre-recovery machine to find out whether any data created can still be detected and the compared to the differences of existence of potential evidence with the pre-recovery machine. The findings will help to understand whether when the setting were restored to the default and even when applications were removed there are still chances that traces of data left behind can still successfully reconstruct any other event left behind on the suspect laptop.

4.3.1.3. After-Reset Machine

The third scenario was the after-reset machine where a suspect attempts to remove all the files from the drive by resetting the machine to factory default. The responder to this investigation will be using the same method as the pre-recovery machine and after-refresh machine to find out if any traces or left over of the data created are still remaining in the machine or not. The findings will be compared with both the pre-recovery and the after-refresh machine to determine the existence of data remaining behind is still able to be successfully recovered and

whether the suspect has actually misused the system even after restoring machine back to where it was initially.

4.3.2. Windows 8 Machine Upgrade to Windows 8.1 Changes

This section describes the changes observed when the system was upgraded to the latest Windows 8.1. The Windows 8 machine was prepared for the experiment by following the current situation where a machine was upgraded to tie up with the release of Windows 8.1 that was released on 17th October 2013. This is to determine whether any data created on Windows 8 prior to the upgrade can still be detected on the analysis stage or it has produced a new challenge to the computer Forensic investigation. In Windows 8.1 SkyDrive was integrated with the machine as the setup to load on the machine and since windows 8.1 required the user to login to the machine using the Microsoft account so the images and files on the SkyDrive will be immediately synchronize to the machine. The messaging application that was initially used as the communication tools were removed in this version and got replaced by Skype application for messaging purpose.

4.3.3. Windows 8 Recovery Options

As described in the scenario for Windows 8 machine acquisition the first image will contain data that the pre-recovery with the data created as described in sub section 4.2.4 and the upgrade to Windows 8.1. This section will discuss the recovery options setup for the after-refresh image and the after-reset image. The Refresh your PC options choose in the experiment means the personal files will not change, the PC setting will be changed back to default meaning it may uninstall the Windows 8.1 and applications installed. When this option was selected the users will have to reinstall other applications from discs and websites. Users will also have to reinstall all updates. The after-reset option chosen in the experiments will totally remove all files from all drives and this also included full clean the drive instead of just removing files from the machine.

4.4 Data Collection Phase For Windows 8 Machine Acquisition

Guymager was the tool chosen to handle the Windows 8 machine Acquisition. This section details the time taken to acquire images from the Windows 8 machine of the three different scenarios. The sub section 4.4.1 represents the imaging for Windows 8 before recovery machine, sub section 4.4.2 represent the imaging for after refresh machine and sub section 4.4.3 represent the imaging for after reset machine. The details in the sub section covered the time that took to verify the files and the time taken to collect the files. Also recorded were the format of the files, the size of the files and the numbers of files generated. Sub section 4.4.4 discusses the data verifying and processing of the images collected on the Windows 8 machine.

4.4.1. Imaging Windows 8 Pre-Recovery Machine

The acquisition of Windows 8 pre-recovery machine was on 11/11/2013. The time the image acquired was 01:08:52 am and the verification of the data started on 03:03:26 am. The total time took to acquire the image took 2hour, 41 minutes and 23 seconds. The total time taken to verify the image acquire took 46 minutes and 49 seconds. Expert Witness Format was chosen as the format of the image and file extension is .Exx. The total of 25 files was generated in the acquisition and the size for all files generated will be 25 times 2GB calculate together to give 50GB.

4.4.2. Imaging Windows 8 After-Refresh Machine

The acquisition of Windows 8 after-refresh machine was on 17/11/2013. The time the image acquired was 11:00:41 am and the verification of the data started at 13:00:45 pm. The total time took to acquire the image took 2 hours, 51 minutes and 50 seconds. The time required in order to process the collection was 2 hours and 3 second to acquire the image and 51 minutes and 47 seconds to verify the image. Similarly Expert Witness Format was chosen as the format of the image with .Exx as the file extension. All together there were 28 files generated for the acquisition and the total file size generated was 56GB.

4.4.3. Imaging Windows 8 After-Reset Machine

The acquisition of Windows 8 after-reset machine was on 20/11/2013. The time the image acquired was 00:31:17 am and the verification of the image started at 05:12:41 am. The total time took to complete the collection process took 5 hours, 50 minutes and 33 seconds. The time for acquisition took 4 hours, 41 minutes and 23 seconds. The time for verification took 1 hour, 9 minutes and 9 seconds. Same as the previous two images collected, the format chosen was Expert Witness Format and the file extension was .Exx. The total number of files generated is 140 for the acquisition and file size for all the files generated was 280GB.

4.4.4. Data Verifying and Processing for Windows 8 Machine

Once hard disk image were acquired on the Windows 8 machine, the images stored in the hard disk were moved into the standalone computer that had the Encase 7 installed for further analysis. The images were put into the Encase 7 program for verifying to ensure the data integrity of each file. This is the standard procedure for Encase where after evidence files were added it will require the data verifying step before anything could be done. In the stage the time to verify each of the images were different, the time taken to verify the before recovery machine and after refresh machine took about an hour. However the time taken to verify the after reset machine took two and a half hours to complete which means at least 2.5 times longer. All three machine used the same way for processing with all the option were de-selected to process all the option individually in order to complete the processing of all the image acquired. The after reset image has taken longer than to process than the other images and similar for the bulk extractor it took at least 8 hours to complete the whole scanning of the image files as compared with the other two image files which were before recovery and after refresh took total of 4 hours to complete the scanning process.

4.5 Analysis Phase For Windows 8 Machine Acquisition

This section covered the findings from the analysis phase for Windows 8 machine acquisition. The findings were grouped into three parts in order to answer the sub questions listed out in chapter 3. The first part is the data existence for different

recovery options on Windows 8 machine in sub section 4.5.1 and this part will compare the data on the findings from the three images collected that were based on before recovery, after refresh and after reset. The second part of the section for sub section 4.5.2 will be the tools effectiveness for confirmatory analysis on Windows 8 machine which will report the result of the five tools chosen to analyse the acquired images content. The third part sub section 4.5.3 described the results from the evidence created for the operating system data to determine whether potential evidence for event reconstruction were found on the different recovery options.

4.5.1. Data Existence For Different Recovery Options on Windows 8 Machine

There are 7 partitions and 1 un-partitioned space (GPT) found in the Windows 8 system evidence trees in all the three types of evidence collected were listed in table 4.5 below.

Table 4.5: Partition Type

| Partition Type | Windows 8 Before Recovery System partition size | Windows 8 After Refresh System partition size | Windows 8 After Reset System partition size |
|----------------------------------|---|---|---|
| EFI System Partition (1) | 300MB | 300MB | 300MB |
| Recovery Partition (2) | 900MB | 900MB | 900MB |
| Microsoft Reserved Partition (3) | 128MB | 128MB | 128MB |
| Operating System Partition (4) | 121748MB | 121748MB | 121748MB |
| NTFS Partition (5) | 350MB | 350MB | 350MB |
| Data | 161328MB | 161328MB | 161328MB |

| | | | |
|---------------------------|---|---|---|
| Partition (6) | | | |
| Restore Partition (7) | 20490MB | 20490MB | 20490MB |
| Unpartitioned Space (GPT) | - Unallocated Space Root Folder - File System Metadata | - Unallocated Space Root Folder - File System Metadata | - Unallocated Space Root Folder - File System Metada |

The items of artifacts found on each system partition for different recovery options were listed on table 4.6 below.

Table 4.6: Items of Artifacts

| Partition | Before Recovery | After Refresh | After Reset |
|-----------|-----------------|---------------|-------------|
| C (1) | 330 | 335 | 342 |
| D (2) | 210 | 213 | 216 |
| E (3) | 1 | 1 | 1 |
| F (4) | 578101 | 758119 | 370564 |
| G (5) | 50 | 55 | 55 |
| H (6) | 123 | 123 | 49 |
| I (7) | 55 | 55 | 55 |

4.5.1.1. EFI System Partition

The EFI system partition was the first partition displayed on FTK imager and displayed as C drive in Encase. It worked as partition for data storage device to adhere to the UEFI aka Unified Extensible Firmware Interface. The FEI system partition is formatted using the FAT32 file system as seen in the evidence acquired in all the three images collected. The data existence for different recovery options on the Windows machine were similar the only differences were the date where the file was modified was files associated with the boot sector and boot configuration data, these indicated when the computer boot up to windows

operating system the new date will be recorded. The table 4.7 below displays the findings for the EFI system partition.

Table 4.7: EFI system partition

| Evidence Tree | Before Recovery | After Refresh | After Reset |
|-----------------|---|---|--|
| SYSTEM (FAT32) | Displayed the following files: root directory, Unallocated space folder, FAT1, FAT2, reserved sectors and VBR | Displayed the following files: root directory, Unallocated space folder, FAT1, FAT2, reserved sectors and VBR | Displayed the following files: root directory, Unallocated space folder, FAT1, FAT2, reserved sectors and VBR |
| Root | Boot Sector Backup file Date Modified 10/11/2013 at 3:29:28 p.m. | Boot Sector Backup file Date Modified 15/11/2013 at 7:24:16 p.m. | Boot Sector Backup file Date Modified 15/11/2013 at 7:24:16 p.m. |
| EFI (Microsoft) | BCD (Boot Configuration Data) Date Modified was 11/11/2013 at 12:36:30 p.m. BOOTSTAT.DAT Date Modified was 10/11/2013 3:39:14 p.m. | BCD (Boot Configuration Data) Date Modified was 17/11/2013 at 10:49:26 p.m. BOOTSTAT.DAT Date Modified was 15/11/2013 7:24:16 p.m. | BCD (Boot Configuration Data) Date Modified was 18/11/2013 at 7:17:26 p.m. BOOTSTAT.DAT Date Modified was 15/11/2013 7:24:16 p.m. |
| EFI (Boot) | Similar for all 3 evidences acquired | Similar for all 3 evidences acquired | Similar for all 3 evidences acquired |
| EFI (ASUS) | BCD (Boot Configuration Data) Date Modified was 25/10/2013 at | BCD (Boot Configuration Data) Date Modified was 15/11/2013 at | BCD (Boot Configuration Data) Date Modified Was |

| | | | |
|----------------------|--------------|--------------|--------------------------------|
| | 9:48:40 p.m. | 8:55:44 p.m. | 17/11/2013 at 11:03:50 a.m. |
| Unallocated Space | 6 files | 14 files | 15 files |

4.5.1.2. The Recovery Partition

The recovery partition was the second partition displayed on FTK imager and displayed as D drive in Encase. It worked as a partition which stored the Windows installation file locally and worked as the partition that allow to create the recovery drive to refresh or reset the computer to troubleshoot problems. The installation exists in all the three different images acquired however there are some differences such as on the After Reset's image it can be seen from the root folder that recovery.txt is marked for deletion and logs folder that does not exist for both After Refresh and Before Recovery options. The ReAgent.xml was modified according to when the after refresh and after reset was utilized and the findings are displayed on the table 4.8 below.

Table 4.8: Recovery Partition

| Evidence Tree | Before Recovery | After Refresh | After Reset |
|-----------------------|---|---|---|
| Root Folder | No file marked for deletion | No file marked for deletion | Recovery.txt is displayed at marked for deletion |
| Root Recovery Folders | Displayed Windows RE folder OS Build version path leads to Windows 8 OS | Displayed Windows RE folder OS Build version path leads to Windows 8.1 OS | Displayed Windows RE Folder and Logs folder OS Build version path leads to Windows 8 OS, additional Reload.xml leads to Windows 8.1 |

| | | | |
|------------------------------|---|--|--|
| | | | OS |
| Windows RE | Winre.win, boot.sdi & ReAgent.xml is found The date modified for ReAgent.xml was 26/10/2013 at 4:48:46a.m. | Winre.Win, boot.sdi & ReAgent.xml is found The date modified for ReAgent.xml was 15/11/2013 at 7:55:51 a.m. | Winre.Win, boot.sdi & ReAgent.Xml is found The date modified for ReAgent.xml was 17/11/2013 at 7:03:54 p.m. |
| System Volume Information | Displayed tacking log file Date Modified was 07/04/2013 at 09:57:53a.m. | Displayed tracking log file Date Modified was 07/04/2013 at 09:57:53 a.m. | Displayed Tracking log file Date modified was 07/04/2013 at 09:57:53a.m. |
| Unallocated Space | 11 files | 10 files | 13 files |

4.5.1.3. Microsoft Reserved Partition

The Microsoft reserved partition was the third partition displayed on FTK imager and E partition displayed on Encase. This partition size is 128MB and it worked to make sure that all Windows features were working correctly. This partition cannot be deleted after it was created, the main functions were to store boot manager code and boot configuration database. There were no data found in all the three images acquired in this partition. The findings displayed only unallocated space and the size for unallocated space is about 128MB which is the same size as the partition size. The table 4.9 below displayed the findings from the Microsoft reserved partition.

Table 4.9: Microsoft Reserved Partition

| | | | |
|-------------------|--------------------------------|--------------------------------|--------------------------------|
| Evidence Tree | Before Recovery | After Refresh | After Reset |
| Unallocated Space | 131,072KB unallocated space | 131,072KB unallocated space | 131,072KB unallocated space |

4.5.1.4. Operating System Partition

The operating system partition was the fourth partition displayed on FTK imager and displayed as drive E in Encase. This partition contained all the data files from the system such as programs files, windows files and user's files. It was also seen as the main drive of the computer where the important evidences related to the case were stored in this partition. The items found on this partition was different with the total of 578101 items were discovered the before recovery system, 758119 items were discovered on the after refresh system and 370564 items were discovered on the after reset system. The data existences of the items discovered were reported in table 4.10 below.

Table 4.10: Operating System Partition

| Evidence Tree | Before Recovery | After Refresh | After Reset |
|---------------------|---|---|-----------------------------|
| Root folders | 2 recycle bin folders | 1 recycle bin folders | 1 recycle bin folders |
| \$Windows.~BT | Has a boot folder, drivers download folder and EFI folder More Folders seen on source folder Work folder NTFS Index file size is 4KB | Inside New OS has root folder, EFI and Driver download folder not found Lesser folders seen on Sources folder compare to before recovery Work Folder NTFS index file size is 8KB | Not available |
| Program Files | AVAST Software Existed | AVAST Software Missing | AVAST Software Missing |
| Program Files (x86) | Mozilla Thunderbird Existed Windows PowerShell | Mozilla Thunderbird Missing Windows PowerShell | Mozilla Thunderbird Missing |

| | | | |
|-----------------|--|--|---|
| | Existed | Missing | Windows Power Shell Missing |
| Program Data | AVAST Software Program Data Existed Default Program Data Available | AVAST Software Program Data Missing Default Program Data Available | AVAST Software Program Data Missing Default Program Data Available |
| Recovery | Recovery Folder seen | Recovery Folder Seen | Recovery Folder Missing |
| Sources | Sources Folder displayed under \$Windows~BT | Source Folder displayed under \$Windows~BT | Source Folder not available |
| Rollback Folder | QuarantineLog.TXT, FolderMoveLog.TXT & LogRestored.TXT displayed | QuarantineLog.TXT, FolderMoveLog.TXT & LogRestored.TXT displayed | Not available |
| \$\$SysReset | \$\$SysReset Not available | \$\$SysReset displayed | \$\$SysReset Not available |
| Lost Files | 10297 items displayed | 93471 items displayed | 585 items displayed |
| Users | Admin2013 folder displayed All Users, Default, Default User and Public folders displayed Default migrated folder displayed | Admin2013 folder displayed All Users, Default, Default User and Public folders displayed Default migrated folder missing | Administrator2013 displayed All Users, Default, Default User and Public folders displayed Default migrated folder missing |
| Windows.old | Existed with all default files displayed | Existed with all default files however Adobe, NIS, another | Not Available |

| | | | |
|-----------------------|-------------------------------|---|-----------|
| | Total = 30265 items displayed | Windows.old and source displayed as marked for delete Total = 193786 items displayed | |
| Unallocated Spaces | 10 folders | 18 folders | 3 folders |
| Total Items Displayed | 578101 items | 758119 | 370564 |

4.5.1.5. NTFS Partition

The NTFS partition was the fifth partition displayed on the FTK imager and was displayed as drive F in Encase. The data displayed on the evidence tree was similar to the recovery partition however the files were being marked for deletion for the after refresh and after reset machine. The findings were recorded in the table 4.11 below.

Table 4.11: NTFS Partition

| Evidence Tree | Before Recovery | After Refresh | After Reset |
|--------------------|--|--|--|
| Recovery | Boot.sdi, ReAgent.xml and Winre.win existed and no changes been made | Boot.sdi, ReAgent.xml and Winre.win maked for delete | Boot.sdi, ReAgent.xml and Winre.win maked for delete Boot folder also marked for delete |
| Unallocated spaces | 4 files | 8 files | 8 files |

4.5.1.6. Data Partition

The Data Partition was the sixth partition displayed on FTK imager and was displayed as drive G in Encase. This partition was the data partition that was known as the D drive on the machine. This partition can be access by users on

their machine to store other files in the drive, however in this experiment the drive was untouched and the findings on the data existence for this partition was displayed in table 4.12 below.

Table 4.12: Data Partition

| Evidence Tree | Before Recovery | After Refresh | After Reset |
|-------------------|---|---|---|
| Root | MSI244b2.tmp displayed as marked for delete | MSI244b2.tmp displayed as marked for delete | 4014a83b56d0cd71dd displayed as marked for delete |
| Recycle Bin | 2 Recycle bin folder exists | 2 Recycle bin folder exists | 1 Recycle bin folder exists |
| Lost Files | Displayed 25 items | Displayed 25 items | Not Available |
| \$TxfLog | Modified on 10/11/13 08:12:30 p.m. | Modified on 15/11/13 09:10:14 p.m. | Modified on 18/11/2013 05:59:58 a.m. |
| Unallocated Space | 1617 files | 1617 files | 1617 files |

4.5.1.7. Restore Partition

The restore partition that allows the system to restore to its original states the files existences was similar for the three machine acquired. The three machines contain the installation files, the disk layout data files and the partition data files however the differences that were seen is the unallocated space files. In the unallocated space the before recovery machine contains the most files followed by after refresh and after reset. The lesser number of files remains in the unallocated space which means that the clusters inside the partition have been written therefore the unallocated space in the partition become lesser. The findings on the restore partition are displayed in the table 4.13 below.

Table 4.13: Restore Partition

| Evidence Tree | Before Recovery | After Refresh | After Reset |
|-----------------|--------------------|--------------------|-------------|
| \$Extend Folder | \$RmMetada, \$Txf, | \$RmMetada, \$Txf, | \$RmMetada, |

| | & \$TxfLog displayed | & \$TxfLog displayed | \$Txf, & \$TxfLog displayed |
|---|--|--|--|
| \$RmMetadata | \$TxfLogContainer modified date was 10/11/2013 at 08:12:30 p.m. \$TxfLog.blf modified date was 10/11/2013 at 08:12:30 p.m. | \$TxfLogContainer modified date was 15/11/2013 at 09:10:15 p.m. \$TxfLog.blf modified date was 15/11/2013 at 09:10:15 p.m. | \$TxfLogContainer modified date is 18/11/2013 at 06:59:59 p.m. \$TxfLog.blf modified date is 18/11/2013 at 06:59:59 p.m. |
| RecoveryBoot, RecoveryImage & System Volume | Contains the following files: AsDiskLayout.dat Boot.Win AsPartition.dat Install.win Tracking.log | Contains the following files: AsDiskLayout.dat Boot.Win AsPartition.dat Install.win Tracking.log | Contains the following files: AsDiskLayout.dat Boot.Win AsPartition.dat Install.win Tracking.log |
| Unallocated Space | 1617 files | 90 files | 89 files |

4.5.2. Tools Effectiveness For Confirmatory Analysis on Windows 8 Machine

The tools effectiveness for confirmatory analysis on Windows 8 machine were summarise in the sub section 4.5.2.1 for FTK Imager, sub section 4.5.2.2 for Encase V7, sub section 4.5.2.3 for Bulk Extractor, sub section 4.5.2.4 for Registry Ripper and sub section 4.5.2.5 for registry decoder. The results of the finding compared the tools based on their efficiency of findings potential evidence in the experiments and what was lacking in the tools that requires the help of other tools to find the potential evidence.

4.5.2.1. FTK Imager

The FTK Imager tools used in this research allows the viewing of the different types of partition collected from the image. The images collected from the acquire

machine were added as evidence items so that the files inside the images collected can be further analysed for the confirmatory of the data. The advantages for using this tool were that the evidence tree displayed the size of each partition and displayed the name of the partition that were label accordingly to each of their file system type. The root folder will contain all the files related to the file system including the unallocated space folder and orphan folder. The next advantages for using this tool will be the export of file hash list into csv file to view the file path for only the select files available in the partition folder on excel. Another function was the export of file hash also generates the MD5 hash and SHA1 values for the file of interest to ensure the integrity of the file. Depending on the size of the file system and unallocated space the time to generate the file can take longer for bigger file size but shorter time for smaller file size.

4.5.2.2. Encase V7

Encase was the main tool that use to process the data collected from the machine, the images collected were added as evidence in the case. The image file added will have to be verified before the entries can be viewed. The evidence processor can search for the relevant artifacts in the image such as the emails, link file parser and the internet artifacts on the data collected from the machine. Encase allows the selection of the type of evidence to process and then view on it as records. The selections have to be carefully picked to ensure that it does not take too long to process the image file. This can be break down by first selecting the relevant type of evidences related to the case follow by other type of evidences on the list. Similar to FTK imager all the items in the evidence can be hash into MD5 and SHA1 values to ensure the file integrity. Another similarity with FTK imager will be the way to view the folder and directory of the files of the evidence on the tree table however the differences are the partitions were named as drives alphabetically rather than partitioned with names. The sizes of all the partitions were not viewable and no unallocated space folder was seen on the evidence tree. The good thing about the entries was all the items on the evidence can be selected and de-selected and the total number of items found on the three different images

can be compared to determine the data existence for different recovery option on the Windows 8 machine.

4.5.2.3. Bulk Extractor

The bulk extractor was chosen as another tool to scan the images files acquired for the experiment to extract for potential evidence. The images files were input into the scanner and the output files will produce the data chosen to scan in the scanner options. At the end of the scanning the data were exported into the report. The tool includes bulk extractor viewer to allow the viewing of the report to find potential information on a disk images. The benefits of this tool will be the results from the disk images can be parsed with automated tools. Another benefit will be the lesser time to examine a disk image acquired for a variety of information that may be missed out by other tools. For this experiment the URLs visited on the and machine keywords search done on the machine acquired rely on the results from Bulk Extractor to determine whether potential evidence existed on the machine.

4.5.2.4. Registry Ripper

The Registry Ripper was chosen to parse the information from the registry files acquired from the 3 machines. The selected registry files are NTUSER.dat, SOFTWARE, SECURITY, SYSTEM, SAM and DEFAULT. The advantages for Registry Ripper was to search for the registry keys on the files to produce the path of where the related path the file was written, the log file folder, User identity associated with the file and provided the last written time. The results produce in the report allows the analysis of where the related files such as internet history, shell folders and last created documents history were located in the Encase evidence folder so that it allows the search that can lead directly to the folder to look for relevant evidences. The last written time provided was UTC therefore in order to reconstruct the event the time will need to covert in to the correct time on where the city was located at. The data generated out will be based on plugin available on the registry ripper tools. There is more data being parsed out as compare to Registry Decoder but Registry Ripper can only read one registry files

at one time and the data parsed out the files can only be generated out in one text files.

4.5.2.5. Registry Decoder

The Registry Decoder chosen to process the registry files that were copied from the Encase and Registry Decoder handle the selected registry files together at one time rather than one file at a time. The plugins were not as many compared to the Registry Ripper and errors occurred when attempting to run the system plugin but the Registry Decoder has the file view version that allows browsing of all contents inside registry files inside the case file. The advantage is that there is a search function that can lead to the registry key data from a keyword to find further information on another related path. Followed by the viewing of all the content on the registry files and only limited to the files that can be processed by Registry Decoder. The registry files that were not recognized by the Registry Decoder will be rejected and this lowers the chances of finding potential data. In Registry Ripper timeline were generated according to the data being parsed out from the plug in this means sorting have to be done manually if wanting to capture the timeline of registry keys that were written on the machine and on the other hand Registry Decoder has the functions that allows the generation of report that contains all the timeline each keys which were modified into a .CSV files for further timeline analysis.

4.5.3. Potential Evidence For Event Reconstruction on Windows 8 Machine

This sub section 4.5.3 focused on the potential evidence for event reconstruction on Windows 8 machine. The potential evidence will follow the list created for the operating system data for event reconstruction based on the findings in the different types of evidence created. From the first evidence created will be the keywords search in sub section 4.5.3.1 to the application installed on Microsoft Store applications at 4.5.3.10.

4.5.3.1. Keywords Search

The keyword search evidences were found in the path as shown below on the before recovery machine:

F:\Users\admin2013\AppData\Local\Microsoft\Windows\INetCache\IE folders.

However it was not found on the after refresh and after reset machine. The Bulk Extractor was run to analyse the data in url_search.txt to determine if the data still existed in the after refresh machine and after reset. In the after refresh machine the traces of data were still available and looking further into Encase it was found in the path as shown below F:\Windows.old\Users\admin2013\AppData\Local\Microsoft\Windows\INetCache\IE

There were 2 old windows folders discovered in the after refresh machine and the evidence were found in the folders that was not on the marked for deletion. The files related to keywords search from the suspect machine were displayed as search.html [1] and suggestions [1].html. During analysis all the 10 keywords search were found in both before recovery and after refresh machine but not in the after reset machine.

4.5.3.2. Website Visited

The website visited were processed in all the three evidence acquire using encase. The findings produce the result as Typed URL but the result was not the evidence that was created. The Typed URL produced the results that were typed on the address bar on the Internet Explorer. The results produced in the record shows that for before recovery machine there were nine URLs, for after the refresh machine there were eleven URLs and for after refresh machine there was only one URL. The URLs produced in the after reset machine was the default URL. The findings in the registry files generated a different result where five URLs were found in both before recovery and after refresh machine. On the other hand the similar result as Encase were detected on the after reset registry files for the Typed URL. The bulk extractor was also used to further analyse the website visited. The search on the URL.txt, domain.txt, and url_histogram.txt could find the details of the list of the website visited. Both the before recovery machine and

after refresh were able to find the matches related to the website visited on the evidence that were created on the machine. There were no matches found in after reset machine and the URLs that were seen on the list belong to the factory setting defaults.

4.5.3.3. Emails Sent and Received

The potential evidences for email histories were able to find on the before recovery machine and after refresh machine by following the path as shown below:

F\Users\admin2013\AppData\Local\Packages\microsoft.windowscommunicationsapps_8wekyb3d8bbwe\LocalState\Indexed\LiveComm\

There is a different number in the folder layout when analysed in encase there were two LiveComm folders. The analysis confirmed that all the data of email there were sent and received were stored in the log files. The master log livecomm.edb contains the evidence of the email sent and received by the user on the machine. In the after reset machine LiveComm folders did not exist and the Livecomm.edb file was missing.

On the other hand, emails sent and received were using Thunderbird application were able to be processed in encase successfully and results generated are able to provide the details information of all the emails sent and received in both before recovery and after refresh machine. The file path for emails in the before recovery machine were stored on the following path below:

F\Users\admin2013\AppData\Roaming\Thunderbird\Profiles\

The file path for email in the after refresh machine were stored on the following path below:

F\Windows.old\Users\admin2013\AppData\Roaming\Thunderbird\Profiles

4.5.3.4. Pictures Saved On My Document Folders

The pictures were filtered out from all the three types of evidence acquired using Encase. The before recovery machine managed to filter out 37538 image files, after reset machine managed to filter out a total of 147222 image files and 147222 image files were filter out from the after reset machine The image files created for

the experiment were found on both before recovery machine, after refresh machine however all the images files created were missing on the after reset machine. The analysis showed that the images files that were created were stored on the local machine was found on the path: F:\Users\admin2013\Pictures\

4.5.3.5. SkyDrive's Documents Synchronizing

The documents and picture saved on SkyDrive were able to be located in the file paths as shown below:

F:\Users\admin2013\SkyDrive\Documents

\F:\Users\admin2013\SkyDrive\Pictures\

The folders were found in both before recovery and after refresh machine. The data found in the document folders displayed not only the original file and also the properties of the files. For the picture folder, the data displayed contains the original files, the thumbnail and the properties of the image files. The SkyDrive that were synchronize with the Microsoft account on both the before and after refresh machine were successfully found. On the other hand there was no trace of SkyDrive folder that was found on the after reset machine. The attempt to look at all the items acquired in the after reset machine also does show any of the SkyDrive files existence.

4.5.3.6. Calendars Entries

The calendar entries can be found in the master log files called edbtmp.log under the LiveComm folder for Windows communication apps. The file path for the master log on before recovery machine as shown below:

F:\Users\admin2013\AppData\Local\Packages\microsoft.windowscommunicationsapps_8wekyb3d8bbwe\LocalState\LiveComm\08737a0bd7d7e5f4\120712-0049\DBStore\livecomm.edb

The file path for the master log on after reset machine as shown below:

F:\Windows.old\Users\admin2013\AppData\Local\Packages\microsoft.windowscommunicationsapps_8wekyb3d8bbwe\LocalState\LiveComm\08737a0bd7d7e5f4\120712-0049\DBStore\livecomm.edb

The data displayed were not very obvious as the master log files also contains a lot of data from the other communication applications such as the email sent and

received and the messaging text sent and received. The log files were not found in the after reset machine. The calendar can be recognized by the title of the events but the content inside the calendar entries could not be found. After searching the data acquired in the three machines there were no trace of the file WLCalendarStore.edb that can provide enough details of the calendar entries.

4.5.3.7. Word Documents Saved In My Documents Folder

The word documents created in the before recovery machine were able to parse out from the before recovery machine NTUSER.dat files. The attempt to parse out similar information from the after refresh and after reset machine were not successful as the result shows there is no sub-key for the recent document created. With the information collected in Encase using the EnScript to filter documents from entries from all the three types of evidence were acquired, and the result displayed and the documents that were saved on the My Documents Folder. The finding shows that the word documents existed in both the before recovery machine and after refresh machine on the path displayed below:
F:\Users\admin2013\Documents\Thesis Experiment Documents\

4.5.3.8. Messaging Text Sent And Received

The messaging text sent and received using the immersive metro functions were stored on the master log. Under the people folder the information of the contacts details were found that means in order to send and receive text the other party will have to be added into the contact list. Unfortunately there is no data to determine when this contact was added into the contact list. The path for the sent and received message in the before recovery machine can be located below:

F:\Users\admin2013\AppData\Local\Packages\microsoft.windowscommunicationsapps_8wekyb3d8bbwe\LocalState\LiveComm\08737a0bd7d7e5f4\120712-0049\DBStore\livecomm.edb

The path for the sent and received messages in the after refresh machine can be located below:

F:\Windows.old\Users\admin2013\AppData\Local\Packages\microsoft.windowscommunicationsapps_8wekyb3d8bbwe\LocalState\LiveComm\08737a0bd7d7e5f4\120712-0049\DBStore\livecomm.edb

In Windows 8.1 version the messaging function in the immersive view was no longer available. Skype application has replaced the messaging function. If the machine acquired was already on Windows 8.1 then the file path to located the data from the sent and received message will be the main.db files. In the before recovery machine the file can be found in the following path below:

F:\Users\admin2013\AppData\Local\Packages\Microsoft.SkypeApp_kzf8qxf38zg5c\LocalState\live#3athesismfit2013\main.db

In the after refresh machine the data of the messaging function were stored in the old windows folders and the location of the main.db files can be found in the following path below:

F:\Windows.old\Users\admin2013\AppData\Local\Packages\Microsoft.SkypeApp_kzf8qxf38zg5c\LocalState\live#3athesismfit2013\main.db

4.5.3.9. Installed Applications

The installed applications that were installed in the before recovery machine consisted of Thunderbird mail, Skype and the Avast Anti-Virus program. Initially Skype was included as one of the data required to be discovered in the install applications but due to Skype already been integrated as one of the Microsoft application therefore the installed applications were reduced to two applications of interest. The evidences of the two applications were found in the roaming data under the file path listed below on the before recovery machine:

F:\Users\admin2013\AppData\Roaming

In the after refresh and after reset machine displayed only the default installed applications the traces of the installed applications can still be found in the old windows folder for the after refresh machine but no traces of the installed applications on the before recovery machine were found in the after reset machine as the old windows folders does not exist anymore in the after reset machine. Similar results of the installed applications were parsed out from the registry keys NTUSER.dat files. The findings in registry keys files were also compared with the findings on Encase shows that the user software consisted of the Avast software and Mozilla was the Thunderbird application name in the before recovery machine registry files.

4.5.3.10. Microsoft Store Applications

The Microsoft Store Applications in the machine acquired were analysed. The findings were also compared with the registry keys that were reviewed on the registry viewer under the registered applications to determine the Microsoft store applications installed on the three machines. The evidences where all the Microsoft store application in the machine were found in the path in Encase:

F\Users\admin2013\AppData\Local\Packages

Other potential evidences will be using the Registry Decoder to generate information from the user assistant values for the link files to see how many times the Microsoft store applications has been run on the machines. The findings shows that all the three user assistant values result generated from the registry keys were different. When a machine was refreshed or reset the values were re-recorded again. The findings proved that data that was captured in the before recovery machine were deleted when changes have been made on the machine. The table 4.14 below shows the findings of the Microsoft store applications that were installed on the machine:

Table 4.14: Microsoft Store Applications

| Store Applications | Before Recovery | After Refresh | After Reset |
|-------------------------|-----------------|---------------|-------------|
| ASUS Tutor | O | O | O |
| The World Clock | O | O | O |
| File Manager | O | X | X |
| Juniper Network | O | X | X |
| Adera | O | O | O |
| Bing Finance | O | O | O |
| Bing Food And Drink | O | X | X |
| Bing Health And Fitness | O | X | X |
| Bing Maps | O | O | O |
| Bing News | O | O | O |

| | | | |
|------------------------|---|---|---|
| Bing Sports | O | O | O |
| Bing Travel | O | O | O |
| Bing Weather | O | O | O |
| Fresh Paint | O | O | O |
| Microsoft Solitaire | O | O | O |
| Mo Camera | O | X | X |
| Microsoft Reader | O | O | O |
| Skype App | O | O | O |
| Studio Pinball | O | O | O |
| Tap tiles | O | O | O |
| Windows Alarms | O | X | X |
| Windows Calculator | O | X | X |
| Communications App | O | O | O |
| Windows Reading List | O | X | X |
| Windows Scan | O | X | X |
| Windows Sound Recorder | O | X | X |
| Xbox Live Games | O | O | O |
| Zune Music | O | O | O |
| Zune Video | O | O | O |
| Windows Photos | X | O | O |
| Microsoft Camera | X | X | O |

4.6 CONCLUSION

This chapter reports the changes and alterations made in the methodology defined in chapter 3 due to the limitations discovered during the preparation phases. In this chapter each phase was taken from the preparation of the equipment to tool analysis and the results were recorded. The incident response phases to build each

scenario were noted and there were three scenarios in the findings that included any changes for example upgrading the machine to Windows 8.1 and types of recovery options chosen. The data collection phases were details out based on the time taken to complete the data acquisition task, the amount of files generated and the size of each files. The data extracted from the machine was reported in the findings after data analysis were conducted based on the amount of data found on each partition to determine the data existence. Tools efficiency was displayed on the findings based on how each tool had functionality in order to analyse data collected for potential evidence and lastly the result reported where the path/locations of potential evidence were found on the machine. The findings were presented for potential evidence found in order to construct event analysis. They were positive on the before recovery and after refresh machine but negative for after reset machine. Chapter 5 is to evaluate the findings based on the result from experiments in this chapter and what was expected from chapter 2. The results will be used to answer the sub questions based on the hypotheses tested and finally the research main question on what new features in Windows 8 Operating System poses new challenges to Digital Forensic investigation.

Chapter 5 – Research Discussions

5.0 INTRODUCTION

In chapter 4 each phases of the experiments were recorded and any alteration made in the methodology from chapter 3 reported. This chapter will look at the results derived from the findings in chapters 4 by evaluating the sub questions and hypothesis first to answer the research sub-questions. The section will review the hypothesis in a table format with the argument for accepting the first hypothesis (a) proposed and argument against to attempt to accept the second hypothesis (b) proposed and finally the result for the hypothesis will be either rejected or accepted. The answers from the research sub questions will be discussed in the next section in 5.2 and the new feature challenges will be re-construct as the hypothesis to answer the main research questions on the new features in Windows 8 Operating System that pose new challenges to Digital Forensic investigation.

The new features challenges are discussed in section 5.2.4 before giving an answer to the answer to main questions in section 5.2.5. The findings will be discussed in sub section 5.3 based on the data existence, tools capability and the event reconstruction method from the analysing the potential evidence. The chapter will ends with the recommended steps as guideline to provide some solution to the problems areas that were discovered and lastly with a conclusion given in section 5.5.

5.1 Answering Of Research Sub Questions

This section will attempt to answer the research questions based on the findings from chapter 4. Sub section 5.1.1 will answers the first research sub question on the data existence, sub section 5.1.2 will answers the sub questions based on tools efficiency and section 5.1.3 will answer sub questions regarding the event reconstruction. The table structure in this section first put up the hypotheses that were listed in chapter 3.3.3 follow by the argument for and the argument against. The argument supports the hypothesis A and the argument against supports the

hypothesis B. The table will displayed the test results on whether the hypothesis were accepted or rejected and the bottom part of the table will summarise the results from the test.

5.1.1. Data Existence And Hypothesis Test

In chapter 3 the first sub questions were put as the research sub question. The question asked was “How can we tell the differences in the data collected on the different recovery options from Windows 8 machine?”

In order to answer the first sub question the hypothesis listed under chapter 3.3.3 were described in the table 5.1 below were tested according to the experiment findings in chapter 4.5.1.

Table 5.1: Data Existence And Hypothesis Test

| | |
|---|---|
| <p>Hypothesis H1a: The data found in different recovery options are different.</p> <p>Hypothesis H1b: The data found in different recovery options are similar.</p> | |
| <p>ARGUMENT FOR: According to the result in 4.5.1 after analysing the data of each of the images acquired the files existence found in the three images acquired are different.</p> <p>The total items found in each recovery option consisted of 578870 items found on the before recovery machine, 758901 found on the after refresh machine and 371282 found on the after reset machine.</p> <p>Comparing the folders in the user profile folder from the operating system partition the data existence for the three</p> | <p>ARGUMENT AGAINST: From the results of the finding in chapter 4.5.1, all the three images acquired have the similar file system partition.</p> <p>The system partition size for each recovery options were similar in all the three images acquired.</p> <p>The non-partitioned space also contains unallocated space root folder and file system metadata. EFI, Recovery and Restore Partition contain similar files for all three images acquired.</p> |

| | |
|---|---|
| <p>different types of recovery options were different.</p> <p>In the refresh machine some files were marked for deletion and in the reset machine some of the files does not existed at all.</p> <p>The modified date and last written date for the files found in the different recovery options are different.</p> | <p>Although similar there is no way to tell or proved that all the data found in different recovery option are similar.</p> |
| <p>Test Result: Hypothesis H1a is accepted and Hypothesis H1b is rejected</p> | |
| <p>Summary: The test result was based according to the findings that were described on chapter 4.5.1. The result determines the data existence on the three different images acquired with different recovery options. The total files found on each recovery options were counted for each partition. The Microsoft reserved partition and Restored partition have the same amount of items for the three images acquired with different recovery. For the data partition, before recovery and after refresh have the same amount of items artifacts found on the data partition. For the NTFS partition after refresh and after reset have the same amount of items of artifacts were found. The amount items of artifacts found on after refresh and after reset does not matches the amount on the before recovery options. The huge differences of the items existed in the operating system partition confirmed that the data found in different recovery options were different and therefore the hypothesis where data found in different recovery options are similar was rejected as there is no way to prove the data displayed in the evidence folder were similar.</p> | |

5.1.2. Tools Efficiency And Hypothesis Test

In chapter 3 the second sub question asked was “Which Digital Forensic tools can work effectively to extract and analyse data from Windows 8 machine for a confirmatory analysis?”

In order to answer the second sub questions the hypothesis listed under chapter 3.3.3 were describe in the table 5.2 below were tested according to the experiment findings in chapter 4.5.2:

Table 5.2: Tools Efficiency And Hypothesis Test

| | |
|--|---|
| <p>Hypothesis H2a: Only one Digital Forensic tools is required to effectively extract and analyse data for confirmatory analysis</p> <p>Hypothesis H2b: More than one Digital Forensic tools are required to effectively extract and analyse data for confirmatory analysis</p> | |
| <p>ARGUMENT FOR: Encase 7 was the tool chosen to test for the hypothesis H2a to search for potential evidence on the Windows 8 machine. The system partitions were displayed correctly and can be seen clearly on the evidence tree. The search filter was able to filter out the different file type such as email files, pictures files and document files to conduct file analysis. Encase 7 was able to review the timeline of the files created and was</p> | <p>ARGUMENT AGAINST: More tools have to be chosen to conduct further analysis on the potential evidence created earlier for the experiment that was not found by Encase 7. Encase 7 could not directly parse out the information in the registry files and the registry files have to be extract out. The registry files were parsed by using registry ripper and registry decoder tools for timeline analysis based on the time and date the files was written on the registry files.</p> |

| | |
|--|--|
| <p>able to review the applications that was installed on the machine on the three image acquired.</p> <p>Registry files can be review and extract out successfully for further analysis.</p> | <p>The website visited and keywords search have to rely on the bulk extractor for extra processing of the data in the image acquired in order to match the evidence the created for the experiments</p> <p>The files systems rely on the FTK imager to review unallocated and the confirmed the names of the each partition found.</p> |
| <p>Test Result:</p> <p>Hypothesis H2a is rejected and Hypothesis H2b is accepted</p> | |
| <p>Summary:</p> <p>Although Encase 7 can extract and analyse data from the machine acquired in experiment there is still the need to require other tools to extract further information such as the keyword search done on the machine and the website visited that was not found when using Encase 7. The requirement for the help of other tools to determine the existence of the data and their path location. Once the locations are found it can be refer back to Encase 7 to re-look for the data of the file again to continue the analysis the confirmatory on whether such even has took place on the machine. Such example will be using the Bulk Extractor to conduct keywords search on the website that were visited and also using the data extracted out from the registry key to further analyse the data. This also means the Encase were not capable to parse out data directly from the registry keys to conduct registry analysis individually. The FTK imager can review unallocated files that enable the acknowledgement of files were actually written differently on each partition for different recovery options. However still even if one tools from the list were chosen it still could not give the describable result and still required two tools to work together to produce better result. As the result the use of more than one tools was required to effectively extract and analyse data for confirmatory analysis therefore the Hypothesis H2a where only one tools can</p> | |

effectively extract and analyse data for confirmatory analysis was rejected.

5.1.3. Event Reconstruction And Hypothesis Test

In chapter 3 the third sub question asked was “Where can potential evidence for event reconstruction analysis found on Windows 8 machine?”

To answer the third sub question the hypothesis listed under chapter 3.3.3 were described in the table 5.3 below were tested according to the experiment findings in chapter 4.5.3:

Table 5.3: Event Reconstruction and Hypothesis Test

| | |
|--|--|
| <p>Hypothesis H3a: Using files analysis, registry analysis, timeline analysis and application analysis allows Digital Forensic investigator to find potential evidence for event reconstruction analysis in Windows 8 machine</p> | |
| <p>Hypothesis H3b: Using files analysis, registry analysis, timeline analysis and application analysis does not allow Digital Forensic investigator to find potential evidence for event reconstruction analysis in Windows 8 machine.</p> | |
| <p>ARGUMENT FOR: Documents, pictures and emails created earlier on were searched on the before recovery, after refresh and after reset machine to conduct files analysis in order to do event reconstruction on the Windows 8 machine. Based on the findings potential evidence can be found on the before recovery and after refresh machine based on files analysis. The registry files from the before recovery, after refresh and after reset machine were copied out from the registry hive to conduct registry</p> | <p>ARGUMENT AGAINST: Documents, picture and emails created earlier on were searched but was not found on the after reset machine thus potential evidence for event reconstruction analysis could not be established on the after reset machine. The registry files from the after reset were analysis but the data stored in the file shows that the keys were back to factory settings. The last files access and applications launched were changed. Previous data on the before recovery and after refresh were not</p> |

| | |
|--|--|
| <p>analysis enable the review of last file access and the applications were launched on the machine.</p> <p>Timeline changes were detected based on the date and time where registry keys were written on the machines and also when changes occurred to the registry keys was captured. Timeline analysis enable the reconstruction for events from the most recent date and time the process were last updated.</p> <p>Application analyses were done on the applications installed from the Windows store and the selected software installed on to the machine. The log files associated with the applications were found and the data stored in the applications provided potential evidences to reconstruct event from Windows 8 machine.,</p> | <p>capture on the after reset machine registry keys.</p> <p>Timeline analysis for after reset machine shows that the registry keys of certain applications in the after reset machine were revert back to default time. Default times were retained for registry keys that were not changed.</p> <p>Log files or items related to applications does not exists anymore on the after reset machine. The data from the application installed and downloaded from Windows Store were missing thus no traces of data left from the applications before the system was reset is available to provide any event reconstruction analysis.</p> |
| <p>Test Result: Both Hypothesis H3a and Hypothesis H3b is accepted</p> | |
| <p>Summary: There is a fair share for the Hypothesis H3a and Hypothesis H3b test result where conducting files analysis, registry analysis, timeline analysis and application analysis does allows Digital Forensic investigator to find potential evidence for event reconstruction analysis in windows 8 machine. The hypothesis H3a was tested positive for evidence image acquired on the before recovery machine and after refresh machine. The result from the findings presented in chapter 4.5.3</p> | |

shows that evidence still existed in the before machine and the path were given on where to look for the potential evidence and for after refresh machine the evidence still existed on the old.windows folders working similar like a backup copy for the before recovery machine. On the other hand, the evidence image acquired from the after reset machine was suitable for the Hypothesis H3b test result where using file analysis, registry analysis, timeline analysis and application analysis does not allow the information to reconstruct an event analysis due to the experiment results where no trace of data was found related to the evidence created and therefore could not reconstruct the event on the after reset machine.

5.2 Discussion of Research Main Question

The results from the sub questions were further discussed in this section according to the data existence on different recovery option in sub section 5.2.1, tool efficiency for Windows 8 investigation in sub section 5.2.2 and event reconstruction from potential evidence acquired in 5.2.3. This section will construct the new feature challenges in sub section 5.2.4 that were derived from the answer and the discussion of the sub questions that were asked in the research.

5.2.1. Data Existence On Different Recovery Options

The questions for data existence on different recovery options were answered in the sub-section 5.1.1 and the answer leads the fact that data found in different recovery options were different. The result has determined that when using different recovery options it can provide some risks to the Digital Forensic investigation because the data found on each recovery option was different. The actual amount of data and the last modify time for each recovery option will never be the same for all system images acquired as it changed on each recovery option therefore there is no unique way to tell which recovery option were utilized by looking at the amount of data that were available. Forensic investigators will have to locate the files based on whether such files existed in the roots folders and where these files reside under the root folders when reviewing the evidence tree.

Following the result of the experiments the data existence can be based on the amount of files detected in the non-allocated spaces and the confirmatory of old.windows folders in the image files acquired. The characteristics where the recovery function as stated by Microsoft where if refresh function is used, the operating system setting will go back to the default but the files will still be kept therefore files are still existed in the machine and with the old.windows folders that still kept the backup copied of the old files. The old.windows folder also kept the details of the settings even after the refresh was conducted which means the refresh recovery option does not pose new challenges for the Digital Forensic investigation since data was still there.

5.2.2. Tools Efficiency For Windows 8 Investigation

The questions for tool efficiency focus on the numbers of tools used to find out which Forensic tools can effectively extract and analyse data from a Windows 8 machine were answered in the sub-section 5.1.2. The results from the tested hypothesis where only one tool is needed to effectively extract and analyse data from Windows 8 was not accepted due to the fact that more tools were required complete the extraction and analysis of the evidence acquired in the experiment. The reason could be due to the limitation where using one standard tool was not able to parse out information for registry analysis and also because the evidence created for the experiment was still not found easily after processing the evidence.

The search conducted by the standalone tools could not provide enough information for confirmatory analysis to locate where the potential evidence are hiding in the list of the folders under the evidence tree. Therefore the need for the other few tools came in to enable the effectively to search for evidence for confirmatory analysis for example all the website visited on the machine were not captured by Encase and the registry key. It turn out only bulk extractor were able to detect the website visited but the results after the processing also contains other default website that already existed on the machine. This can lead to new challenges when using tools to conduct analysis for Windows 8 machine like having to refer back to issues where findings potential evidence on one tool but does not find similar data on another tools and how can they be combined

together to make it to a case and successfully using the information found to reconstruct the event details of the suspect.

5.2.3. Event Reconstruction From Potential Evidence Acquired

The questions asked on where the potential evidence for event reconstruction analysis found on Windows 8 machine were answered in the sub-section 5.1.3. The result tested that gave the two answers, one of the answers will be that both before recovery and after refresh machine allows Digital Forensic investigator to find potential evidence to reconstruct event of the suspect. The next answers will be after reset machine does not allow the Digital Forensic investigator to find potential evidence because there are no traces of data left behind to reconstruct event of the suspect.

The answers to the test results were backed up by the findings in chapter 4.5.3 where all the data created for the experiment listed on 4.2.4 were found on the before recovery machine and after reset machine. The findings provide the path of where the potential evidence can be found on the machine. On the other hand, the similar method and analysis used for before recovery and after refresh machine does not produce any findings on where those data created for the experiment and further search on the after reset image file does not produces any related keywords, picture, documents and emails that even existed in the machine before. The result proved that data were wiped off completely and new installation of windows operating system then overwrites the disk to bring the machine to factory setting. The outcome will produce bigger challenges to Digital Forensic investigation especially when dealing with after reset machine as this will not be very easily to detect and more steps have to be taken to recover the actual data that could be hidden on the machine.

5.2.4. New Features Challenges

The new features challenges were reconstructed from the answers in the sub questions so that hypotheses can be formed to answer the research main questions. The total of three new features were discovered to pose new challenges to the Digital Forensic investigation. The new features will be discussed in sub

sub section 5.2.4.1 for secure boot, 5.2.4.2 for reset functions and 5.2.4.3 for communication applications.

5.2.4.1. Secure Boot

The secure boot features in a Windows 8 machine actually restrict the computer to boot directly to disk unless it was directly setup beforehand that would mean that if that machine were taken by an investigator without knowing whether the secure boot was already configured before or not then booting up the machine will end up starting the operating system rather than the boot to a Digital Forensic boot disk. This was found during the experiment when attempting to acquire data from the machine. The step taken first ends up as being having to login to the computer then choosing to restart but bring it to the boot configuration page to change the setting before being able to boot to the Digital Forensic disk then ran the desirable acquisition software to acquire the disk image from the machine. The normal method on the older version of computer system will be able to press the function keys where it could force the computer to boot to a disk does not work anymore for Windows 8 machine anymore. Due to this the secure boot new features that was intended to prevent malicious application to load during boot process could bring challenges to maintain the integrity of the data which were collected from the machine especially when a machine was turned off and when having to switch it on again to check the boot configuration end up changing original date where the last boot was run which could also alter the data that were initially stored on the machine.

5.2.4.2. Reset Functions

The rest function on the recovery option consider the biggest impact to the Digital Forensic investigation especially with the risks of deleting all the user data on the Windows 8 machine by just selecting the fully clean the drive can wipe all the data in the drive with just a click. When the hard drive was cleaned up then windows will be reinstall to bring the computer back to the factory setting. The benefit will be there is no need to install any software to conduct such a task which means it will be easy for the person who intends to misuse the computer to abuse such a function. After committing a crime, the user could just restore the

machine to default leaving no trace behind for investigator to find potential evidence that could detect the actual event before the reset was done. The suspect might re-create new events to mislead the investigator into believing that there was nothing unusual happening on the machine. In the experiment scenario the reset take at least 2 hours to fully reset to factory settings and users can rename the machine and re-setup a local machine with a new identity. During the analysis of the after reset machine only the new identify was detected and the identify setup before the reset could not be account for anymore. Another impact of the reset functions was it took much longer to acquire the image of the hard drive and the file size of the image was also largest as compared with the before recovery and after refresh. The reason where it took a longer time was because the speed to copy the data into a new drive decreased by 3 times when reading the drive after the reset machine therefore it took longer than to acquired data if the machine was reset. However when compared the numbers of items available in the hard drive and after reset hard drive contains the least number of items available.

5.2.4.3. Communications Applications

In Windows 8 and Windows 8.1 the communication application have a different way of storing information. Communication applications now merge with the immersive user interface. The immersive features allow users to sign in or merge with an online account that integrate with other social media platforms. The new integration could mean that potential evidence of communication history now might not be easily find the internet history or in the application history which was where an investigator could trace a communication between two parties in the past operating system Digital Forensic methodology. The Digital Forensic challenge was discovered when attempting to search for messages send and received that was created for the experiment. The communication history log was stored as the database files for the immersive applications which could be deleted by user when the file become too big and have taken up much space of the user hard disk. One of the risks noticed in the experiment will be the calendar entries that was created and it was found that the data were to be stored in the temporary log files however the data stored inside were encrypted and I could not tell the

actual text of the entries in the log file. The entries could only be read by the title that was added into the calendar and could only be recognized based on the public holiday that were already on log file by default. There was not information to tell which date the entries were added on for appointment in the calendar since the data found were unreadable. Other risks will be with many accounts that could merge together into one local system that could bring challenges to Digital Forensic investigation when having to look at huge data stored on log files to find important evidence related to the case and as mention earlier where the chances of it could produces larger log files that may in the end either be deleted by users to clear up spaces in their hard drive. Another possibility will be with all the relevant communication data stored in the log files this can promote the suspect to completely remove all the logs files or attempt to edit the logs files if they have the suitable tools to open up the logs files manually and changed the information. Such action could lead to misleading the investigation process and bring more challenges to prosecute the suspect in worst case may lead to the wrong person being prosecuted.

5.2.5. Answers To Main Research Question

In chapter 3 the main question asked was “What new features in Windows 8 Operating System poses new challenges to Digital Forensic investigation?”

To answer the main question the hypothesis were plotted based on the answers from the sub-question and the findings as reported in chapter 4. The answers to the main question are given in the table 5.4 below.

Table 5.4: New Features Challenges and Hypothesis Test

| |
|--|
| Research Question: What new features in Windows 8 Operating System poses new challenges to Digital Forensic investigation? |
| Hypothesis Main Question 1a: Secure Boot, Reset Functions and Communication Applications were found to poses new challenges to Digital Forensic investigation |
| Hypothesis Main Question 1b: Secure Boot , Reset Functions and Communication Application were not found to poses new challenges to Digital Forensic investigation |

| ARGUMENT FOR: | ARGUMENT AGAINST: |
|--|--|
| <p>Secure boot do not allow machine to boot directly to an external device thus investigator doing acquisition cannot press the function key to make the machine boot to the desirable Digital Forensic toolkit that was operating on different operating system. The only method to conduct the task affects the integrity of the data since computer has to be switch on to access the UEFI specification.</p> <p>Reset function removed existing data in the machine which prevent Digital Forensic investigator to find potential evidence to reconstruct any event analysis. After the reset function were executed on the machine previous user profile were removed and users can re-setup a new profile that may confused the investigation process. There could be more steps to be done to determine whether machine was reset intentionally by the suspect. Furthermore the data collected might be manipulated by suspect to make changes to the user profile and making it seem like nothing unusual was done on the machine that may end up poses new challenges to the Digital Forensic investigator.</p> | <p>Investigator can follow an alternate method to go to the BIOS setting to disable secure boot first then allow the machine to boot directly into an external device this can enable them to acquire the data on the machine without having to open up the machine to take out the hard drive when doing acquisition. However doing this method may alter the data on the machine that end up become a potential risk for data integrity.</p> <p>Even after the reset function were executed on the machine Digital Forensic investigator were still able to acquire the data from the after reset machine that enable them to collect data for analysis purpose. Unfortunately the process to acquired data from after reset machine such as acquired, processing and verifying seem to take longer time to read as compared to other types of machine. Despite of taking longer time to acquired, processing and verifying the data found in the after reset machine was much lesser as compared to the other machine therefore after reset could end up poses new challenges to Digital Forensic investigation for being</p> |

| | |
|--|--|
| <p>Communications applications logs were combined together and stored in a single database files. The database files contains the all the communication history of the user account. The file size will get huge and at some point user might attempt to shrink the file size that might end up deleting the data in the log. The logs files can be easily source out by suspect and can be edited since some of the data does not provide any timeline that could determine when the conversation were made. The event could be recreated without any difficulties that could have misled the investigator when conducting analysis on the log files.</p> | <p>more time consuming and more steps have to be taken to attempt to recover data still in the unallocated space.</p> <p>The logs history for communication applications were stored in a single database files that could save time to search around for potential evidence around the machine since the log contains all the communications between two parties. The accounts for all social media were combined together in one file making it easier to retrieve information on one location that means as long as investigators know were those files are stored in the machine they would be able to source out for the right evidence to further analysis the data on the single log file. On the other hand this can be a very easy way for suspect to purposely editing the logs file on the machine which still ends up posing great challenges to Digital Forensic investigation.</p> |
| <p>Test Result: Hypothesis Main question 1a was tested positive therefore Hypothesis Main question 1b was rejected</p> | |
| <p>Summary: The hypothesis were tested based on the findings and answering of the sub-questions where the hypothesis main question 1a were tested positive because these three new features indeed poses new challenges to Digital Forensic investigation. The first challenges will be for secure boot feature that can impact</p> | |

to the data integrity of the evidence acquired from the Windows 8 machine. If the investigation have to be conducted without removing the hard disk from the machine and required to boot a forensic tool kit software then the only method will have to start up the machine and let the machine access to UEFI option then disable the secure boot option to let the machine boot to BIOS or directly to Forensic tool kit operating system to conduct acquisition on the machine. The second challenges listed for after reset machine can affect the way Digital Forensic investigator method of analysing the data on a machine. If not being able to tell the difference of the after reset machine it may means that nothing unusual happened on the machine as new profile can be setup to complicate the investigation process. The process to collect data and analysing data on the after reset machine may consume a much longer time and if no potential evidence was found it would turn out more steps have to be taken to recover data on the machine. The third challenges will be the communication applications where database file actually contains all data of the communication history under the users account and the log files has possibilities of being manipulated or edited by suspect to mislead the investigation. If this were done that could complicated the analysis process for the case and more time will be needed to trace where have been changed on the log files thus causes more problems to Digital Forensic investigator having to track where is different from the original content. With the conditions discussed in the summary matches the hypothesis main question 1a and there were no way to rebuke that the three features in Windows 8 poses no new challenges to Digital Forensic investigation therefore hypothesis main question 1b was rejected.

5.3 Discussion Of Findings

The discussion of findings will be the extension of the findings from chapter 4 and this section explains in detail how the findings were tested on each of the hypothesis to obtain the final answers of the sub question. Sub sub section 5.3.1 compared the items found on each types of the partition using before recovery option as the benchmark to compare the differences of the amount of items found

on after refresh and after reset machine. The tools capabilities were being summarised based on the Forensic tasks, the tools can be used for in sub section 5.3.2 and the event reconstruction methods were discussed in 5.3.3 based on the Digital Forensic task done on the types of potential evidences.

5.3.1. Data Existence

The data existence relevant to the findings were compared using the before recovery data collected as the benchmarking. Looking at the table 5.5 below, for EFI system partition there were more items found in after reset machine than after refresh machine where after reset has 3.6% more items as compared to the before recovery options. Similarly for after reset machine the recovery partition also has 2.8% more files than before recovery's machine recovery partition. The characteristic when after reset were utilized data existence can be determine by the increase of items produced for the EFI system and Recovery partition. The Microsoft reserved partition contains a similar amount of items for all the different types of the recovery options and was expected because the partition was just to check that the installation were correctly installed and when reviewing the items in the partition there were no files found, this also indicates that nothing was written on the partition. The restored partition displayed similar amount of items found in all the machine with different recovery options which retained the installation, as disk partition and as disk layout files even after changes were made on the operating system. The operating system partition produced results with a significant differences where the after refresh machine it was found to have 31.1% more items than the before recovery option items which means that data old data were not actually removed on the system and were still existed on the computer. On the other hand, as compared with the before recovery option, it was found that the after reset have 35.9% lesser items. The characteristics were similar as the data partition which shows that 60.2% lesser items were found as compared to the before recovery option and this could match the scenario when both the drive with operating system partition and data partition was fully formatted on the after reset machine.

Table 5.5: Comparison of Data in Partitions

| Types of Partitions | Before Recovery | After Refresh | After Reset |
|------------------------------------|------------------------|----------------------|--------------------|
| EFI System Partition (1) C | 100 | 1.5% more | 3.6% more |
| Recovery Partition (2) D | 100 | 1.4% more | 2.8% more |
| Microsoft Reserved Partition (3) E | 100 | Similar | Similar |
| Operating System Partition (4) F | 100 | 31.1% more | 35.9% lesser |
| NTFS Partition (5) G | 100 | 10% more | 10% more |
| Data Partition (6) H | 100 | Similar | 60.2% lesser |
| Restore Partition (7) I | 100 | Similar | Similar |
| Totals% for all Partitions | 100 | 31.1% more | 35.9% lesser |

5.3.2. Tools Capability

The tools capabilities were selected to analyse the content of data of the machine. Table 5.6 below displayed the result of the forensic tasks that were used by the tools and how well they fared in the Digital Forensic investigation when searching for potential evidence. The results were summarise and recorded down based on the forensic tasks that each tool can conducted. The main tool which was Encase 7 could do most of the analysis such as file analysis, timeline analysis and applications analysis however only allowing to extract relevant registry files out that could only be used another registry decoder tools to analysis the content on the registry keys. The next tool FTK Imager allows only files analysis and applications analysis because during the analysis it allows the viewing of files information and any application installed on the machine but that would have view it manually by choosing the right path to view details of the files. Based on

the summaries not all tools can be perfect to conduct all the four Digital Forensic tasks listed which were file analysis, registry analysis, timeline analysis and applications analysis. The Forensic tasks that produced the best result for all the tools chosen for the experiment will be the applications analysis as all the tools were able to conduct application analysis on the evidence acquired. The Forensic tasks that fared the worst will be the registry analysis where only the registry ripper and registry decoder can read details for the registry keys by parsing out relevant information.

Table 5.6: Tools Capability Summary

| Tools | <i>Files Analysis</i> | <i>Registry Analysis</i> | <i>Timeline Analysis</i> | <i>Applications Analysis</i> |
|-------------------------|-----------------------|--------------------------|--------------------------|------------------------------|
| Encase 7 | O | X | O | O |
| FTK Imager | O | X | X | O |
| Bulk Extractor | O | X | X | O |
| Registry ripper | X | O | O | O |
| Registry Decoder | X | O | O | O |

5.3.3. Event Reconstruction

Event reconstruction can be conducted as long as potential evidence was found on the images acquired. The table 5.7 below will summarise the discussion about how the types of potential evidence and the event reconstruction methods that were attempt in order to reconstruct the event happened on the machine.

Table 5.7: Event Reconstruction Method for Potential Evidence

| Types Of Potential | Event Reconstruction Methods |
|---------------------------|-------------------------------------|
|---------------------------|-------------------------------------|

| Evidence | |
|--------------------------|---|
| Keywords Search | <p>Files Analysis → Internet cache files in Encase and bulk extractor url_search</p> <p>Timeline Analysis → Last modified date and time for the suggestion.htm and history.htm</p> <p>Registry Analysis → NTUSER.dat keyword search</p> <p>Application Analysis → Website browsing applications</p> |
| Website Visited | <p>File Analysis → Bulk Extractor url_search</p> <p>Registry Analysis → NTUSER.dat for typed URL</p> <p>Timeline Analysis → Timeline displayed on the typed URL</p> <p>Application Analysis → Charm search bar for search everything</p> |
| Emails sent and received | <p>Files Analysis → LiveCommunication Logs, bulk extractor email_txt and rfc822.txt</p> <p>Timeline Analysis → The content in the email for the sent and received date and time</p> <p>Registry Analysis → NTUSER.dat, SOFTWARE</p> <p>Application Analysis → Thunderbird Email application</p> |
| Picture Files | <p>Files Analysis → filter all jpeg files and review the content of the file</p> |

| | |
|----------------------------------|---|
| | <p>Timeline Analysis → Created date and modify date of the jpeg file</p> <p>Registry Analysis: NTUSER.dat for last file opened</p> <p>Application Analysis: Photo viewer applications</p> |
| SkyDrive | <p>File Analysis → document and picture folders that store the skydrive files for information of the document and picture files</p> <p>Timeline Analysis → Documents and picture created date and modify date</p> <p>Registry Analysis → SYSTEM and SOFTWARE to review the system changes and software files installed on the machine</p> <p>Application Analysis → Reviewing installed SkyDrive applications</p> |
| Calendar Entries | <p>Files Analysis → LiveCommunication Logs</p> <p>Timeline Analysis → Last modified date of log files or time displayed on the log content.</p> <p>Registry Analysis → Not available</p> <p>Application Analysis → Windows Calendar application</p> |
| Text documents and RFT documents | <p>Files Analysis → Text documents and RFT documents saved on the folder by reviewing the content inside the file</p> |

| | |
|----------------------------------|---|
| | <p>Timeline Analysis → Time document create and modified date</p> <p>Registry Analysis → NTUSER.dat for last file opened</p> <p>Applications Analysis → Word document reader that were required to read text file</p> |
| Messaging text sent and received | <p>Files Analysis → livecomm.edb and main.db for Skype</p> <p>Timeline Analysis → Last modified date for the .db files</p> <p>Registry Analysis → NTUSER.dat and SOFTWARE</p> <p>Application Analysis → Skype and communication applications installed on Windows 8</p> |
| Installed Applications | <p>File Analysis → Setup files stored on folders for installation of the applications</p> <p>Timeline Analysis → Last time the files was run on machine and the created date for the time applications were installed on the machine</p> <p>Registry Analysis → SYSTEM and SOFTWARE</p> <p>Applications Analysis → Application log files for installed applications</p> |
| Microsoft Store Applications | <p>Files Analysis → Application data of the user account for the packages to review the files from internet</p> |

| | |
|--|---|
| | <p>history, cache files and cookies installed</p> <p>Timeline Analysis → Last Accessed date of the files</p> <p>Registry Analysis → NTUSER.dat and SOFTWARE for list of installed store applications</p> <p>Application Analysis → Windows store applications settings logs</p> |
|--|---|

5.3.4. Digital Forensic Challenges

The three new features that were listed indeed pose new challenges to Digital Forensic investigation. Secure boot was to safe guard the machine from booting into malicious software that delivers a security experience to user to prevent the computer to be affected by malware. Although it was meant to protect the computer from getting affected by malicious software however when attempting to boot a Forensic toolkit as reported in findings in chapter 4.2.2 which stated that certain steps have to be taken to enable the computer to boot from USB disk as the function keys to allow the computer to boot directly to disk do not work anymore on a Windows 8 machine. Doing that method will end up affecting the integrity of the data acquired from the hard drive because it would be required to login to the Windows machine and navigate to the UEFI setting to allow the computer to boot to BIOS and change the setting to disable secure boot. Such a situation would happened especially if the specific machine have never been changed before to enable secure boot and thus poses new challenges to Digital Forensic investigation since the step could not be avoided.

The next new feature will be the after reset machine and it could poses new challenges to Digital Forensic investigation as described in the findings in chapter 4.4.4. The after reset machine takes a longer time to verified and process the data acquired. Other than this the data existence findings shows that data displayed in the after reset machine as compared with before recovery and after

refresh were different where the most of the folder on the other machine could no longer be found. The findings on chapter 4.5.3 also proved that most of potential evidence that could be found on before recovery and after refresh machine were missing on the after reset machine. In theory after reset machine was meant for users who intend to remove the data on the machine the option will reformat the hard drive data first by formatting all the drive partition where windows and personal data reside then reinstalled a fresh copy of Windows. By doing this method the computer will restart with a fresh copy of Windows which means data inside the data could be overwritten when such things happened it actually destroyed the potential evidence stored on the machine bringing challenges to the Digital Forensic investigation process and it was not known how much data can actually be recovered on the machine. In the worst scenario, after the reset the suspect could create new profiles and use the machine like normal to create new information that could misguide the investigation process during the analysis stage.

Communication applications in Windows 8 allow users to combine their social media account into one login which benefit users having to log on to multiple accounts to check their social media feeds. In this research most of the communication log were tested on the via sending and receiving message using the Windows application on the metro users interface and most of evidence created were successfully capture by the .edb files on the Windows applications cache. The features can be a benefit for Digital Forensic investigation since data could be stored on the same location or path which has the log histories of the communication between the users and their point of contact. Moreover it allows the consolidate of information on a specific method where information can be stored on meaning it would not be complicated or take many steps just to find the piece of information that contains the conversation of the communication. However due to the simplicity it could also bring challenges to the Digital Forensic investigation and as noted raise that the log files could become bigger and thus causing issues that users might end up deleting the log files regularly to save their hard disk space. Another problem with huge files size would mean that it would take more time processing the information found especially if the users

have a lot of contact in the list and that would mean taking a longer method to narrow down the possible people involved in the case. The worst case would be because the logs files may be easily located since users will be curious to find which files was the cause of adding up spaces on their hard disk which mean that could be a good opportunity if a suspect trying to cover their track would attempt to change the logs details with a fake timeline or fake communication to further complicate the investigation process which could add new challenges for Digital Forensic investigation.

5.4 Recommendations

The problems areas uncovered and discussed in the research, in this section recommendation were proposed to provide some solution to the problems areas that were discovered. Section 5.4.1 discussed about recommendations for secure boot and complication can be avoided during an unsure situation. The second recommendation in 5.4.2 describes why it is important to have more than one tool to produce better analysis results. Lastly the third recommendation covers the issues on Forensic readiness for after reset machine in 5.4.3.

5.4.1. Bypass Secure Boot Technique For Better Integrity

The experiment enabled the discovery of how the data integrity can be affected if attempts to acquired evidence when using a Digital Forensic boot disk or USB drive to boot a different operating system which has the tools that can enable the Digital Forensic investigator to copy the image of the hard drive without directly opening up the machine to take out the hard disk drive. Although in this experiment the steps do not require to take out the hard drive and to conduct the investigation by booting from a USB stick and the reason was because during the pilot test the issues was uncovered that it required more than a few steps to enable the machine to boot from a USB pen drive. However in the real situation it will be uncertain whether the machine will be able to boot from USB pen drive or not and if there is any mistake the machine will end up booting up the usual Windows 8 operating system and this could alter the last shut down time of the machine which means details will not be admissible in a court of law should a case was

logged for this incident. The recommendation will be it would be useful to directly take out the hard drive especially when there is uncertainty whether the secure boot has already been enabling or not on the machine; using the method of taking hard drive out from a machine and put write blocker to prevent any data from being written when acquiring the data from the hard drive on Windows 8 machine. The recommendation is that it would be useful to directly take out the hard drive if unsure whether the secure boot has already been enabling or not on the machine.

5.4.2. Combining Different Tools For Better Analysis Results

The second recommendation will be encouraging the execution of different types of tools to produce better analysis results. During the analysing stage it was found that using one tool or two tools is not enough to obtain a result compared with using at least more than two tools. That would depend on the types of the files that the investigation was interested in. One of the examples to describe why it would be encouraged to pick more tools would be the method to get more information from the registry files. When using file caver to extract all the registry files out from the Forensic images that would mean that the tools used in the experiments would not be suitable since it will exhaust the registry parser as the tools selected in the research were not created to process too many registry files. The next example would be some of the not common registry files such as BBI and Amcache.hve found in F:\Windows\AppCompat\Programs\Amcache.hve and F:\Windows\System32\config\BBI would not be able to be parsed by the tools if there were no plugin available to parse specific information therefore it would be recommended to put the registry files on tools that have registry viewer to view and browse the content of the registry file and to provide better analysis results.

5.4.3. Forensic Readiness For After Reset Machine

Based on the things that were discussed above, after reset function can make investigations more complicated that would be it would be an important to be aware that of the impact caused by the after machine. The impact caused by after

reset machine will mean that important data stored on the machine will be restored to factory settings and in this research the results has proved that the data does not existed and new users account setup can be setup to overwrite the previous user's information. The steps recommended would be prevention is better than cure, and it will be important to prevent that after reset machine from being utilized by users easily. Although for personal users it will be hard to stop the users from using this function but if the machine is a company's property then the policy should be setup carefully to prevent their normal users from being able to go to the recovery options and conduct the reset function on the system. Proper procedures can be considered should an IT administrator before they decided to reset the machine to solve any difficult machine issues, for example doing a backup or create a Forensic image of the machine before it was reset and retained it for a certain time should any incident occur during the timeframe after the machine was reset. Doing this procedure could also counter the issues related to the communication applications which may be erased during reset the machine to factory settings by capturing the history of communication logs related to the metro applications should a hard disk run out of space and if any changes being made to reduce the disk space due to reducing the size of the logs file then a necessary backup procedure should be enforced before any changes are made.

5.5 CONCLUSION

In this chapter findings were discussed based on the experimental results and different types of phases recorded in chapter 4. The hypothesis for sub questions that were defined in chapter 3 were tested and used to answer the sub questions. The answers for the sub questions were used to construct the hypothesis in order to answer the research main question. The test results have proven that the data found in each recovery options were different as there were more data in the after refresh machine and less data on the after reset machine. More than one tool was required to successfully analyse the evidence in the machine as Encase still required other tools to further extract information such as a keyword search done on the machine and the website visited on the machine. The result of the third sub question has both hypothesis accepted because both test positive. The before

recovery and after refresh machine still allow Digital Forensic investigators to find potential evidence to reconstruct an event but after reset machine does not allow Digital Forensic investigators to find potential evidence to reconstruct an event. The new features in Windows 8 that found new challenges for Digital Forensic investigation were secure boot, reset function and communication applications affected evidential recovery. The recommendations proposed in this chapter are to bypass secure boot techniques for better integrity during an uncertain situation. It recommends to remove the hard disk to conduct acquisition and do not attempt to boot from a USB drive. Forensic readiness steps were also recommended in this chapter to deal with the after reset machine. The chapter 6 concludes the research with a summary of findings, limitations of research, recommendation summary and future research suggestions.

Chapter 6 – Conclusion

6.0 INTRODUCTION

The research focused on the problem areas as described in chapter 1 section 1.1 and with the motivation of exploring the new features that could pose challenges to Digital Forensic investigation on a Windows 8 machine. The significant gap in the Digital Forensic research related to Windows 8 new features were also noted in chapter 1. The problems areas were identified during the course of the experiments done on the Windows 8 machine. The literature were reviewed in chapter 2 by including the history of the Windows platform, the review of Windows 7 platform with new features, the Forensic benefits areas in Windows 7 and Forensic problems areas in Windows 7. The reasons to review Windows 7 were to review the research completed on Windows 7 and to compare the unique new features to Windows 8. Windows 8 research were reviewed in chapter 2 based on the Windows 8 consumer review, Windows 8 consumer review advantages, Windows 8 consumer review disadvantages and the differences between Windows 7 and Windows 8. The main purpose was to review and establish the changes made to Windows 8 as compared to Windows 7 and how the differences could affect the current Digital Forensic investigation process. Eighteen of the Windows 8 new features were also reviewed in chapter 2 to allow the understanding of what was added into the operating system in order to protect against security threats and improve user experience. Past Digital Forensic research was outlined in a Windows 8 Forensic review as Forensic professional review, Windows 8 Digital Forensic investigation process, Windows 8 Forensic tools and techniques; in order to have a better overview of the Digital Forensic process to data acquisition from digital devices and their challenges. The review chapters end with the review of three existing Digital Forensic models available and one of the models is chosen as the methodology in chapter 3. The latest development in the Windows 8 operating system were reviewed to keep up with the times during the research for any upgrade or changes that may have happened

during the course of the research. In chapter 3 the past research were reviewed based on the problems areas found in terms of past Digital Forensic investigation, Windows 8 platform problems areas from the user perspective, new features and the Digital Forensic investigation perspective. The problems and issues raised in the past research were narrowed down to one of the major problems that could be looked at in the research and was further discussed on section 3.2. The research questions and hypothesis were developed in section 3.3 to address the challenges in Windows 8 new features for Digital Forensic investigation. The research design was established to conduct the experiment in order to look for the challenges of the new features based on the sub questions asked so that the hypotheses can be tested and used to answer the sub questions in order to identified the challenges to the news features. Any alterations in the research design, including each research phase were recorded and together with the ten types of potential evidence as findings which were from the experiment were recorded in chapter 4. The data recorded on each phase and findings from the chapter 4 were used to answer the sub questions and were further discussed in chapter 5 to establish an answer to the main question on the new features in the Windows 8 Operating System that could pose new challenges to the Digital Forensic investigation.

In this chapter the conclusion of the research will present the summary of findings in Section 6.2. The limitations of research that occurred during the investigation phases are also discussed in chapter 6.3. The recommendations that were raised in chapter 5 will be summarised in section 6.4 followed by the possible future research that could extend the current research in section 6.5. Finally section 6.6 is the conclusion to chapter 6.

6.1 SUMMARY OF FINDINGS

In chapter 5 the main questions and sub questions were answered based on the findings recorded in chapter 4. The first sub questions asked was “How could we tell the differences in the data collected on different recovery options from a Windows 8 machine?” The hypothesis was tested and the test results shows that

the data found in different recovery options are different. The result tested positive because most the data found in the operating system partition; where the total items found for the after refresh drive was 31.1% more than before the recovery option. The items found in the after reset option was 35.9% less in the drive as compared to the before recovery drive. For the second sub question “Which Digital Forensic tools can work effectively to extract and analyse data from Windows 8 machine for a confirmatory analysis?” The hypothesis was tested and the test results proved that more than one tool was required to effectively conduct the four Forensic analysis tasks that consisted of files analysis, timeline analysis, registry analysis and applications analysis. Another reason to support more than one Digital Forensic tool is because when an attempt to search for potential evidence another tool may be used to determine the existence of the data and their path location. The third sub question asked: “Where can potential evidence for event reconstruction analysis found on Windows 8 machine?” The result from the hypothesis test was neutral because both the hypotheses proposed were accepted by doing the files analysis, timeline analysis, registry analysis and applications analysis potential evidences were able to be discovered on the before recovery machine and after refresh machine.

Although the potential evidence for after refresh evidence were found in the different path using the same investigation method; the data were found and were similar to the before recovery options. However when using the same investigation method nothing was found on the after reset machine therefore the result proved that after reset tested positive for not allowing a Digital Forensic investigator to find potential evidence for event reconstruction.

The answer to the main questions was based on the new feature challenges that were uncovered in the experiments which included the secure boot features, reset functions and communication applications that were established based on the Digital Forensic phases and findings recorded from chapter 4. The first challenges for secure boot features can impact the data integrity of evidence acquired from the Windows 8 machine. The second challenges will be the after reset machine can impact the Digital Forensic investigation if the machine was reset and was not able to notice anything unusual if new profiles were setup. The

investigation process can be more complicated if the hard drive was fully cleaned and Windows 8 were reinstalled. The third challenges will be the communication applications in Windows 8 where the log histories of communication between the user and their contact were stored on the .edb files in the same location and the size of the log files could become bigger taking up a lot of spaces in the hard disk. In order to reduce spaces users might delete or shrink the file and in the very worst case the files could be easily edited by a suspect to mislead the investigator with a fake timeline or communication in order to complicate investigation process.

6.2 LIMITATIONS OF THE RESEARCH

The limitations of the research were discussed in chapter 3 with the focus on the challenges of the new features and the impact of the new features that may affect Digital Forensic investigation. There were a total of six limitations discovered before the experiment. The first limitation discussed the number of tools to be used in the experiments and not all tools can be tested. The second limitation will be the research will not be testing more than one Digital Forensic investigation model to find a suitable model as a standard. The third limitation expressed that not all the new features will be tested due to the time constrain and the scope of the research. The fourth limitation will be not all the problems and issues discussed in chapter 3 could be explored in the research. The fifth limitation described the case scenario will not be able to focus on all the aspects of the computer misuse case. The sixth limitation talked about the limited number of machines available as there was only one Windows 8 machine available for testing and therefore the machine was re-used.

During the experiments there were a few limitations that were also recognized and will be described in this section. The first limitation during the processing the evidence was that not all the options in the processor were selected as it will cause the processing time to be longer than expected. The second limitation was because Windows Forensic have a very wide scope and during the experiments quite a huge amount of data can be found but not all the data found

can end up being covered in the thesis for example; the Windows Artifact Parser that parsed Link files and File Carver that search for unallocated space or file slack. Finally the third limitation was the registry files data, in the research only the main registry files found were put into the registry ripper and registry decoder for analysis. The final results generate quite an amount of information about the system but only the information related to the evidence that were created to conduct the experiments is reported.

6.3 RECOMMENDATION SUMMARY

The recommendation outline in chapter 5 will be summarised in this section. A total of three different areas were discussed. The first area recommended that it would be helpful to directly take out the hard drive if anyone was unsure whether the machine has a secure boot enabled because there may be chance that the machine will boot up to the usual Windows 8 operating system that could alter the shutdown time. The second area for recommendation will be combining different tools for better analysis of results, as some of the tools only have certain functionality that only allow to analyse certain types of data hence combining different tools may produce a better result. The third recommendation focuses on the prevention is better than cure logic by preventing the after reset machine from being utilized by the users easily. Forensic readiness for after reset machine can be enforced in company properties that prevent normal users from wiping out any data on the machine. Proper procedures can be considered by doing backup before a machine was reset so that the data can be retained for a certain time and referred to if any incident was discovered during that timeframe that may require Digital Forensic investigation to be conducted.

6.4 FUTURE RESEARCH

The objectives to look for new features in Windows 8 that poses challenges for Digital Forensic investigation for this research were achieved. However there are further research that can be undertaken to further understand whether there will be

any solutions that could be achieved for the problem areas. The three areas recommended for further research will be based on the challenges of new features that were uncovered during this research. The first area will be the secure boot features the recommendation in this research strongly recommends that it would be safer to remove the hard disk drive directly from the machine if one was unsure about if the secure boot was already disabled on the machine. However there could be situations where the hard drive was not allowed to be removed from the machine. The future research could investigate about how much the integrity of data will be affected if investigators have to boot the machine directly as compared to the acquisition via the direct access to a hard drive with write blocker. The next area is the after reset machine since the disk is wipe off by tools there might be a chance for data recovery, the future research could focus on whether any of the data can be recovered and how much of the data can be recovered. It would be recommended to look at the unallocated spaces to see whether any remains were hidden in the space and how much data can be left behind. Lastly the next area for communication applications should be further explored on the potential data stored on the logs files, when such files were manually edited and if there is any way to tell the differences of the original and the edited file.

6.5 CONCLUSION

The research focuses on the problems areas on the recovery option and after the options were utilized by users the kind of challenges that it could bring to Digital Forensic investigation processes. In the experiment the after refresh and after reset function were researched based on the existence of data in the machine, the tools that were used to analyse the data in the machine and the potential evidence found in the machine for event reconstruction. The results obtained allow the hypotheses to be tested and to answer the sub questions asked in the research. The experiments also helped to achieve the main question being answered by listing out the three new features such as secure boot, after reset function and communication applications that could pose challenges to a Digital Forensic

investigation process. This chapter concludes the research to find out about the new features in Windows 8 that could pose challenges to the Digital Forensic investigation.

References

- Aamodt, A., & Plaza, E. (1994). Case-Based Reasoning: Foundational Issues, Methodological Variations, and System Approaches. *AI Communications. IOS Press, Vol. 7: 1*, 39-59.
- Abrams, L. (2006, November 15). *How to determine what services are running under a SVCHOST.EXE process*. Retrieved from <http://www.bleepingcomputer.com/tutorials/list-services-running-under-svchostexe-process/>
- Abrams, L. (2012a, December 21). *How to use a PIN to login to Windows 8*. Retrieved from <http://www.bleepingcomputer.com/tutorials/use-pin-to-login-to-windows-8/>
- Abrams, L. (2012b, December 18). *How to use a picture password in Windows 8*. Retrieved from <http://www.bleepingcomputer.com/tutorials/use-picture-password-in-windows-8/>
- Aggarwal, G., Burzstein, E., Jackson, C., & Boneh, D. (2010). *An Analysis of Private Browsing Modes in Modern Browsers*. California: Usenix Security .
- Alazab, M., Venkatraman, S., & Watters, P. (2009). *EFFECTIVE DIGITAL FORENSIC ANALYSIS OF THE NTFS DISK IMAGE*. University of Ballarat, Australia: Special Issue on ICIT 2009 Conference - Applied Computing.
- Amorosi, D. (2012, December 19). *In Windows We Trust*. Retrieved from <http://www.infosecurity-magazine.com/view/29913/in-windows-we-trust/>
- Ariffin, K. A., Mahmood, A. K., Jaafar, J., & Shamsuddin, S. (2012). Hybrid Approach for Memory Analysis in Windows System. *World Academy of Science, Engineering and Technology 70 2012*, 996-1004.
- Ashcroft, J. (2001). *Electronic Crime Scene Investigation A Guide For First Responders*. Washington: National Institute of Justice.
- Babu, M., & Parishat, M. G. (2004, October 11). *What Is Cybercrime?* . Retrieved from <http://www.crime-research.org/analytics/702/>
- Barnett, A. G. (2011). *The Forensic Value of the Windows 7 Jump List*. Purdue: Purdue University.

- Beebe, N. L., & Clark, J. G. (2005). A Hierarchical, Objectives-Based Framework for the Digital Investigations Process. *Digital Investigations Process Framework*, 146-166.
- Belkasoft. (2013, January 01). *Computer Forensic Investigations: Tools and Techniques*. Retrieved from <http://forensic.belkasoft.com/en/computer-forensic-investigation-tool>
- Berkeley Law. (2003, August 04). *Introduction to Computer Technology, Network Economics, and Intellectual Property Law*. Retrieved from <http://www.law.berkeley.edu/files/chp1.pdf>
- Bertolucci, J. (2010, September 21). *PC Users Happier with Windows 7, Survey Says*. Retrieved from PCWorld: http://www.pcworld.com/article/205905/PC_Users_Happier_with_Windows_7_Survey_Says.html
- Birk, D. (2011). *Technical Challenges of Forensic Investigations in Cloud*. Zurich: IBM.
- Bowers, T. (2012, August 06). *Windows 8 infographic: Pros and cons at a glance*. Retrieved from <http://www.techrepublic.com/blog/tech-manager/windows-8-infographic-pros-and-cons-at-a-glance/7911>
- Bradley, T. (2012, December 30). *Why Windows To Go is perfect for BYOD*. Retrieved from <http://www.pcworld.com/article/2023542/why-windows-to-go-is-perfect-for-byod.html>
- Bradley, T. (2013, January 03). *10 reasons why Windows 8 makes sense for business*. Retrieved from <http://www.pcworld.com/article/2022317/10-reasons-why-windows-8-makes-sense-for-business.html>
- Bright, P. (2013a, May 07). *Windows 8 six months in: 100 million licenses sold, 250 million app downloads*. Retrieved from <http://arstechnica.com/information-technology/2013/05/windows-8-six-months-in-100-million-licenses-sold-250-million-app-downloads/>
- Bright, P. (2013b, July 03). *SkyDrive in Windows 8.1: Cloud storage the way it's meant to be*. Retrieved from <http://arstechnica.com/information-technology/2013/07/skydrive-in-windows-8-1-cloud-storage-the-way-its-meant-to-be/>
- Brinkmann, M. (2011, September 09). *Windows 8 Fast Startup, Faster Boot Times*. Retrieved from <http://www.ghacks.net/2011/09/09/windows-8-fast-startup-faster-boot-times/>

- Brunty, J. (2012, September 27). *Microsoft Windows 8: A Forensic First Look*. Retrieved from <http://www.dfinews.com/articles/2012/09/microsoft-windows-8-forensic-first-look>
- Bruzzese, P. J. (2013, October 23). *Windows 8.1: The key security improvements*. Retrieved from <http://www.infoworld.com/d/microsoft-windows/windows-81-the-key-security-improvements-229263>
- Bulygin, Y., Furtak, A., & Bazhaniuk, O. (2013). A Tale of One Software Bypass of Windows 8 Secure Boot . *Black Hat USA 2013*. Las Vegas: UBM Tech.
- Callahan, J. (2012, February 21). *Windows 8 blog reveals improved language support*. Retrieved from <http://www.neowin.net/news/windows-8-blog-reveals-improved-language-support>
- Camm-Jones, B. (2010, July 04). *a timeline of Microsoft's OS*. Retrieved from <http://www.webuser.co.uk/news/in-depth/427212/windows-a-timeline-of-microsoft-s-os>
- Carvey, H. (2011). *Windows Registry Forensic: Advanced Digital Forensic Analysis of the Windows Registry*. Northern Virginia: Syngress Publishing, Inc.
- Carvey, H. A. (2012). *Windows Forensic Analysis Toolkit : Advanced Analysis Techniques for Windows 7*. Waltham, MA 02451, USA: Syngress.
- Casey, E., & Rose, C. W. (2010). Chapter 2: Forensic Analysis. In E. Casey, *Handbook of Digital Forensic and Investigation* (pp. 21-63). California: Elsevier Academic.
- Casey, E., & Stellatos, G. (2008). *The Impact of Full Disk Encryption on Digital Forensic*. Washington, DC: Stroz Friedberg.
- Chacos, B. (2012, December 14). *How to activate Windows Defender in Windows 8*. Retrieved from <http://www.pcworld.com/article/2020260/how-to-activate-windows-defender-in-windows-8.html>
- Constantin, L. (2013, August 02). Retrieved from Researchers demo exploits that bypass Windows 8 Secure Boot: <http://www.pcworld.com/article/2045793/researchers-demo-exploits-that-bypass-windows-8-secure-boot.html>
- Crenshaw, A. (2009, August 13). *Forensically interesting spots in the Windows 7, Vista and XP file system and registry*. Retrieved from <http://www.irongeek.com/i.php?page=security/windows-Forensic-registry-and-file-system-spots>

- Cunningham, A., Smith, R., Vatto, K., & Walton, J. (2012, March 09). *In-Depth with the Windows 8 Consumer Preview*. Retrieved from <http://www.anandtech.com/show/5630/indepth-with-the-windows-8-consumer-preview/7>
- Curtis , J. (2012, March 15). *A Brief History of the Windows Operating System*. Retrieved from <http://windows-operating-system-reviews.toptenreviews.com/a-brief-history-of-the-windows-operating-system.html>
- Daubert v. (1993). *MERRELL DOW PHARMACEUTICALS*. 509 U.S. 579: SUPREME COURT OF THE UNITED STATES.
- Ellis-Christensen, T. (2006, April 10). *What is the Computer Misuse Act of 1990?* Retrieved from <http://www.wisegeek.org/what-is-the-computer-misuse-act-of-1990.htm>
- Emigh, J. (2011, September 19). *10 Key Features in Windows 8: Tablets, Touch and More*. Retrieved from <http://www.notebookreview.com/default.asp?newsID=6268>
- Feng, X. (2005). *Towards RealTime*. Redmond, WA 98052: Microsoft Corporation.
- Fernandes, J. (2012, July 09). *Windows 8 Features And Release Date*. Retrieved from <http://www.thetechlabs.com/tech-news/windows-8-features/>
- Fieber, J. (2012, February 21). *Three Cool Ways You'll Benefit from SkyDrive in Windows 8*. Retrieved from http://www.pcworld.com/article/250383/three_cool_ways_youll_benefit_from_skydrive_in_windows_8.html
- Fikar, M. (2013, January 17). *Advantages and Disadvantages of Windows 8* . Retrieved from <http://thekasiaproject.com/?p=152>
- Fleisher, E. (2012, March 26). *Windows 8 Forensic*. Retrieved from <http://computerForensic.champlain.edu/blog/windows-8-Forensic>
- Forensic KB. (2011, January 11). *Forensic Review of Windows 7 - Part V - Bitlocker* . Retrieved from Computer Forensic, Malware analysis and Digital Investigations: <http://www.forensickb.com/2010/01/forensic-review-of-windows-7-part-v.html>
- Fulton, S. M. (2012a, March 16). *If Windows 7 "Simplifies" the PC, What Does Windows 8 Do to It?* Retrieved from <http://readwrite.com/2012/03/16/if-windows-7-simplifies-the-pc>

- Fulton, S. M. (2012b, May 08). *Top 10 Windows 8 Features #7: Client-side Hyper-V*. Retrieved from <http://www.readwriteweb.com/cloud/2012/05/top-10-windows-8-features-7-client-side-hyper-v.php>
- Gaddam, K. (2012, February 10). *Part 3: Introduction to WinRT, the new 'Windows Runtime' in Windows 8*. Retrieved from <http://www.codeproject.com/Articles/328551/Part-3-Introduction-to-WinRT-the-new-Windows-Runti>
- Geier, E. (2012, July 30). *12 new network features in Windows 8*. Retrieved from <http://www.networkworld.com/slideshow/58311/12-new-network-features-in-windows-8.html>
- Geier, E. (2013, July 16). *Windows 8.1 steps up security with biometrics, encryption, and more*. Retrieved from <http://www.pcworld.com/article/2044422/windows-8-1-steps-up-security-with-biometrics-encryption-and-more.html>
- Gibb, T. (2012a, November 12). *How to Do a Full Shutdown in Windows 8 Without Disabling Hybrid Boot*. Retrieved from <http://www.howtogeek.com/129021/how-to-do-a-full-shutdown-in-windows-8-without-disabling-hybrid-boot/>
- Gordon, W. (2012, August 11). *How to Use Windows 8's New File History Backup (aka Time Machine for Windows)*. Retrieved from <http://lifehacker.com/5958865/how-to-use-windows-8s-new-file-history-backup-aka-time-machine-for-windows>
- Grabham, D. (2012, October 25). *Windows 8 vs Windows 7: 8 ways it's different*. Retrieved from <http://www.techradar.com/news/software/operating-systems/windows-8-vs-windows-7-8-ways-it-s-different-1025285>
- Graham-Smith, D. (2013, January 22). *Windows 8 Storage Spaces: a how-to guide*. Retrieved from <http://www.pcpro.co.uk/features/379408/windows-8-storage-spaces-a-how-to-guide>
- Gralla, P. (2011, May 17). *New survey shows users love Microsoft software. But where's the money?* Retrieved from http://blogs.computerworld.com/18303/new_survey_shows_users_love_microsoft_software_but_wheres_the_money
- Gupta, P. (2012, June 29). *Windows 8 Metro Brings New Security Risks*. Retrieved from <http://blogs.mcafee.com/mcafee-labs/windows-8-metro-brings-new-security-risks>

- Hale, J. (2013, March 08). *Windows 8: Tracking Opened Photos* . Retrieved from <http://dfstream.blogspot.co.nz/2013/03/windows-8-tracking-opened-photos.html>
- Hargreaves, C., & Chivers, H. (2007). *Potential Impacts of Windows Vista on Digital Investigations*. United Kingdom: Cranfield University, Defence Academy of the United Kingdom.
- Harms, K. (2006). Forensic analysis of System Restore points in Microsoft Windows XP. *Digital Investigation Volume 3, Issue 3, September*, 151–158.
- Hayes, D., Reddy, V., & Qureshi, S. (2010). The Impact of Microsoft's Windows 7 on Computer Forensic Examinations. *Applications and Technology Conference (LISAT), 2010 Long Island Systems*, 1-6.
- Hicks, J. (2012, September 12). *Windows 8 Client Hyper-V : Installation and Configuration*. Retrieved from <http://www.petri.co.il/using-windows-8-client-hyper-v-part-1.htm#>
- Horsman, G., Laing, C., & Vickers, P. (2012). *Improving the Trustworthiness of Digital Forensic Investigations*. Newcastle Upon Tyne, United Kingdom: Department of Computing, Engineering and Information Sciences, Northumbria University.
- IBN Live Tech. (2012, October 26). *MS-DOS to Windows 8: The history of Microsoft operating systems from 1981 to 2012*. Retrieved October 26, 2012, from <http://ibnlive.in.com/news/msdos-to-windows-8-the-history-of-microsoft-operating-systems-from-1981-to-2012/302308-11.html>
- InfoSecurity. (2012, November 12). *Windows 8 security useless against 15% of malware*. Retrieved from <http://www.infosecurity-magazine.com/view/29260/windows-8-security-useless-against-15-of-malware>
- Javaid, U. (2012a, March 03). *The Complete Guide To Windows 8 Task Manager; New Features And Options*. Retrieved from <http://www.addictivetips.com/windows-tips/windows-8-task-manager/>
- Johnson, K. W. (2012a, June 28). *WINDOWS 8 RECOVERY FORENSIC*. Retrieved from Understanding the Three R's: <http://computer-Forensic.sans.org/summit-archives/2012/windows-8-recovery-Forensic-understanding-the-three-rs.pdf>

- Johnson, K. W. (2012b). *WINDOWS 8 RECOVERY FORENSIC*. Iowa: SANS DFIR SUMMIT 2012.
- Kent, K., Chevalier, S., Grance, T., & Dang, H. (2006). *Guide to Integrating Forensic Techniques into Incident Response*. Gaithersburg: National Institute of Standards and Technology.
- Kooten , M. v. (2011, August 23). *Global Software Top 100 - Edition 2011* . Retrieved from <http://www.softwaretop100.org/global-software-top-100-edition-2011>
- Lallie, H. S., & Briggs, P. J. (2011). Windows 7 registry forensic evidence created by three BitTorrent clients. *Digital Investigation, Volume 7*(Issue 3–4), 127–134.
- Larkin, R. (2013, February 01). *The Pro's and Cons of Windows 8 in the Enterprise*. Retrieved from <http://www.techscratched.com/2013/02/the-pros-and-cons-of-windows-8-in.html>
- Lawton, G. (2011, June 10). *Cloud computing crime poses unique Forensic challenges*. Retrieved from <http://searchcloudcomputing.techtarget.com/feature/Cloud-computing-crime-poses-unique-Forensic-challenges>
- Leake, D. (2002, May 05). *CBR in Context: The Present and Future*. Retrieved from http://www.cs.indiana.edu/~leake/papers/p-96-01_dir.html/paper.html
- LeBlanc, B. (2011a, January 27). *Windows 7: 300 Million Licenses Sold*. Retrieved from <http://windowsteamblog.com/windows/b/bloggingwindows/archive/2011/01/27/windows-7-300-million-licenses-sold.aspx>
- LeBlanc, B. (2011b, July 11). *400 Million Windows 7 Licenses Sold*. Retrieved from <http://windowsteamblog.com/windows/b/bloggingwindows/archive/2011/07/11/400-million-windows-7-licenses-sold.aspx>
- Lee, R. (2012, September 05). *Windows Artifact Analysis: Evidence Acquisition*. Retrieved from <https://blogs.sans.org/computer-Forensic/files/2012/06/SANS-Digital-Forensic-and-Incident-Response-Poster-2012.pdf>
- Leibrock, L. (2003). *Forensic Tools and Processes for Windows XP*. Texas: Blackhat Windows Security.

- Lim, H. (2010, May 11). *Evolution of Microsoft Windows: 1985 – 2009*. Retrieved from <http://www.hongkiat.com/blog/evolution-of-microsoft-windows-1985-2009/>
- Limer, E. (2013, October 17). *Windows 8.1 Review: Little Changes Make a Big Difference*. Retrieved from <http://gizmodo.com/windows-8-1-review-little-changes-make-a-big-differenc-1446625571>
- Lipowski, E. (2008). Developing great research questions. *Am J Health-Syst Pharm—Vol 65 Sep 1,* 1667-1670.
- Mandia, K., & Prorise, C. (2003). *Incident response and computer Forensic (Second ed.)*. Emeryville: McGraw-Hill/Osborne.
- Manik, S. (2012, October 15). *Windows 8: The Key Advancements*. Retrieved from <http://www.techopedia.com/2/28850/software/operating-systems/warm-welcome-windows-8>
- Microsoft Case Studies. (2013, April 12). *Visual Computing Company Boosts Staff Mobility by Adopting New Operating System* . Retrieved from <http://www.microsoft.com/casestudies/Windows-8-Enterprise/NVIDIA/Visual-Computing-Company-Boosts-Staff-Mobility-by-Adopting-New-Operating-System/710000003591>
- Microsoft US. (2009, October 27). *Explore Windows 7 features*. Retrieved from <http://windows.microsoft.com/en-NZ/windows7/products/features>
- Microsoft US. (2012a, December 01). *Windows 8 system requirements*. Retrieved from <http://windows.microsoft.com/en-NZ/windows-8/system-requirements>
- Microsoft US. (2012b, December 01). *Windows 7 system requirements*. Retrieved from <http://windows.microsoft.com/en-NZ/windows7/products/system-requirements>
- Microsoft US. (2013, January 01). *A History of Windows*. Retrieved October 21, 2012, from <http://windows.microsoft.com/is-IS/windows/history>
- Moorhead, P. (2012, August 17). *Why Windows 8 is Microsoft's Biggest Risk Ever*. Retrieved from <http://www.forbes.com/sites/patrickmoorhead/2012/08/17/why-windows-8-is-microsofts-biggest-risk-ever/>
- MSDN. (2011a, September 09). *Delivering fast boot times in Windows 8*. Retrieved from

<http://blogs.msdn.com/b/b8/archive/2011/09/08/delivering-fast-boot-times-in-windows-8.aspx>

- MSDN. (2012a, November 29). *What's new for Windows 8 display drivers (WDDM 1.2)*. Retrieved from [http://msdn.microsoft.com/en-us/library/windows/hardware/jj583805\(v=vs.85\).aspx](http://msdn.microsoft.com/en-us/library/windows/hardware/jj583805(v=vs.85).aspx)
- MSDN. (2013a, March 11). *What's a Windows Store app?* Retrieved from <http://msdn.microsoft.com/en-us/library/windows/apps/hh974576.aspx>
- Muchmore, M. (2012, October 26). *5 Reasons You Should Upgrade to Windows 8*. Retrieved from <http://www.pcmag.com/article2/0,2817,2411451,00.asp>
- Muchmore, M. (2012, June 01). *Top 6 New Features of Windows 8 Release Preview*. Retrieved from <http://www.pcmag.com/article2/0,2817,2405176,00.asp>
- National Institute of Standards And Technology. (2012a). *Computer Forensic Tools Testing Handbook*. Washington: NIST & NIJ.
- Niehus , O. (2013a, April 05). *Windows 8: Recovery and Troubleshooting*. Retrieved from <http://blogs.msdn.com/b/olivnie/archive/2013/04/05/recovery-and-troubleshooting.aspx>
- O'Brien, T. (2012, October 21). *Skype 6.0 lands with Microsoft and Facebook account integration, Retina support*. Retrieved from <http://www.engadget.com/2012/10/24/skype-6-0-for-mac-and-windows/>
- Okolica, J., & Peterson, G. L. (2011). Extracting the windows clipboard from physical memory. *Digital Investigation, Volume 8*, 118–124.
- O'Mahony, J. (2012, November 28). *Windows 8 outsells Windows 7*. Retrieved from <http://www.telegraph.co.uk/technology/microsoft/9707731/Windows-8-outsells-Windows-7.html>
- O'Neill, S. (2012, June 13). *Windows To Go: The Do's and Don'ts*. Retrieved from http://www.cio.com/article/708391/Windows_To_Go_The_Do_s_and_Don_ts?page=2&taxonomyId=3081
- Otnes, K. (2011). Getting Around Quickly. In *Windows 7 Made Simple* (pp. 3-37). New York: Apress. doi:10.1007/978-1-4302-3651-1_1

- Palmer, G. (2001). *A Road Map for Digital Forensic Research*. New York: Report From the First Digital Forensic Research Workshop.
- PC Plus. (2009, July 13). *Windows compared: Windows 7 vs Vista vs XP*. Retrieved from <http://www.techradar.com/news/software/operating-systems/windows-compared-windows-7-vs-vista-vs-xp-615167>
- Perez, J. C. (2012, February 21). *Microsoft to Tightly Integrate Windows 8 and SkyDrive*. Retrieved from http://www.pcworld.com/article/250359/microsoft_to_tightly_integrate_windows_8_and_skydrive.html
- Phneah, E. (2012, November 09). *5 security issues to watch in Win 8*. Retrieved from <http://www.zdnet.com/5-security-issues-to-watch-in-win-8-7000007148/>
- Pinola, M. (2013, April 02). *Automatically back up your files with Windows 8's File History feature*. Retrieved from <http://www.itworld.com/consumerization-it/350739/automatically-back-your-files-windows-8s-file-history-feature>
- Plugable. (2012, October 25). *New USB 3.0 Support Built-In to Windows 8*. Retrieved from <http://plugable.com/2012/10/25/usb-3-0-support-on-windows-8>
- Protalinski, E. (2012, October 31). *Malware authors quickly create fake antivirus just for Windows 8*. Retrieved from <http://thenextweb.com/microsoft/2012/10/31/malware-authors-quickly-create-fake-antivirus-just-for-windows-8/>
- Raghavan, S., Clark, A., & Mohay, G. (2009). *FIA: An Open Forensic Integration Architecture for Composing Digital Evidence*. Brisbane, Australia: Queensland University of Technology.
- Ray, D., & Bradford, P. (2007). *Models of Models: Digital Forensic and Domain-Specific Languages*. Tuscaloosa, AL: The University of Alabama, Department of Computer Science.
- Rey, D. (2012, July 05). *8 things about windows 8: microsoft account integration*. Retrieved from <http://blogs.technet.com/b/drey/archive/2012/07/05/8-things-about-windows-8-microsoft-account-integration.aspx>
- Rhee, E. (2012, June 26). *Check your PC for Windows 8 readiness with upgrade assistant*. Retrieved from http://howto.cnet.com/8301-11310_39-

57455768-285/check-your-pc-for-windows-8-readiness-with-upgrade-assistant/

- Rivera, R. (2012, May 30). *Windows 8 Secrets: A Peek at Internet Explorer "Flip Ahead"*. Retrieved from <http://withinwindows.com/within-windows/2012/05/31/windows-8-secrets-a-peek-at-internet-explorer-flip-ahead>
- Rosenblatt , S. (2012, August 15). *Windows 8 Release to Manufacturing* . Retrieved from CNET: <http://reviews.cnet.com/windows-8-review/>
- Rouse , M. (2007, February 01). *computer Forensic (cyberForensic)*. Retrieved from <http://searchsecurity.techtarget.com/definition/computer-Forensic>
- Saran, C. (2013, April 11). *PC market crashes*. Retrieved from <http://www.computerweekly.com/news/2240181282/PC-market-crashes>
- Schauland, D. (2012, October 17). *I'll take my Windows 8 To Go, please*. Retrieved from <http://www.techrepublic.com/blog/networking/ill-take-my-windows-8-to-go-please/6084>
- Shultz, G. (2013, January 03). *Windows 8: New File Explorer features*. Retrieved from <http://www.techrepublic.com/blog/window-on-windows/windows-8-new-file-explorer-features/7070>
- Shultz, G. (2013a, April 15). *Quick Tip: Make Windows 8 File Explorer launch in Computer view*. Retrieved from <http://www.techrepublic.com/blog/window-on-windows/quick-tip-make-windows-8-file-explorer-launch-in-computer-view/7550>
- Shultz, G. (2013c, March 27). *Restore Windows 8 with System Image Recovery*. Retrieved from <http://www.techrepublic.com/blog/window-on-windows/restore-windows-8-with-system-image-recovery/7464>
- Shultz, G. (2013d, March 01). *An explanation of the Windows 8 Automatic Repair feature*. Retrieved from <http://www.techrepublic.com/photos/an-explanation-of-the-windows-8-automatic-repair-feature/6407251>
- Sinchak, S. (2012, September 02). *How to Create a Windows To Go USB Drive*. Retrieved from <http://tweaks.com/windows/52279/how-to-create-a-windows-to-go-usb-drive/>
- Sinofsky, S. (2012, January 05). *Refresh and reset your PC*. Retrieved from <http://blogs.msdn.com/b/b8/archive/2012/01/04/refresh-and-reset-your-pc.aspx>

- Snyder, K. (2013, March 07). *Disadvantages of Upgrading to Windows 8*. Retrieved from <http://www.iprovit.com/2013/03/disadvantages-of-upgrading-to-windows-8/>
- Sommer, P. (2012). *Digital Evidence, Digital Investigations and E-Disclosure: A Guide to Forensic Readiness for Organisations, Security Advisers and Lawyers*. United Kingdom: Information Assurance Advisory Council (IAAC).
- Stewart, B. (2007, September 01). *Forensic Implications of Windows Vista*. Retrieved from <http://whereismydata.files.wordpress.com/2009/09/forensic-implications-of-windows-vista.pdf>
- Strickland, J. (2011, June 23). *How Computer Forensic Works*. Retrieved from <http://computer.howstuffworks.com/computer-forensic.htm>
- Swider, M. (2013, February 05). *Windows 8 sales are 'on par' with Windows 7 in 90 days*. Retrieved from <http://www.techradar.com/news/software/operating-systems/windows-8-sales-are-on-par-with-windows-7-90-days-in-1129313>
- The Times of India. (2013, May 11). *5 common Windows 8 problems with solutions*. Retrieved from <http://timesofindia.indiatimes.com/tech/windows8problems/5-common-Windows-8-problems-with-solutions/itslideshow/20003075.cms>
- Thomson, A. C. (2012). *Windows 8 Forensic Guide*. Washington, D.C.: The George Washington University.
- Thurrott, P. (2013, April 30). *Skype + Outlook.com*. Retrieved from <http://winsupersite.com/outlookcom/skype-outlookcom>
- Tushabe, F. (2004). *Computer Forensic For Cyberspace Crimes*. Uganda: University of Colombo.
- Valjarevic, A., & Venter, H. S. (2012). *Harmonised Digital Forensic Investigation Process*. Pretoria, South Africa: University of Pretoria.
- Valjarevic, A., & Venter, H. S. (2012). Harmonised Digital Forensic Investigation Process. *Information Security for South Africa (ISSA)* (pp. 01-10). Johannesburg, Gauteng: IEEE. doi:10.1109/ISSA.2012.6320441
- Virtue, E. (2003). *Computer Forensic: Implications for Litigation and Dispute Resolution*. Canberra: University of Canberra.

- Vogel, D. (2012a, January 11). *Hitting Windows 8 reset button: Security bonus saves time and money.* Retrieved from <http://www.techrepublic.com/blog/security/hitting-windows-8-reset-button-security-bonus-saves-time-and-money/7236>
- Vogel, S. (2012b, May 16). *Faster data transfer as standard with Windows 8.* Retrieved from <http://www.pcadvisor.co.uk/features/windows/3357932/windows-8-native-usb-30-support/>
- Wang, L., Xu, L., & Zhang, S. (2011). Network Connections Information Extraction of 64-Bit Windows 7 Memory Images. *Forensic in Telecommunications, Information, and Multimedia, Volume 56*, 90-98 .
- Warren, T. (2012, July 09). *Windows 7 hits 630 million licenses sold, now running on 50 percent of enterprise desktops.* Retrieved from <http://www.theverge.com/2012/7/9/3146777/windows-7-630-million-licenses-sold-enterprise-adoption>
- Warren, T. (2014, January 30). *Microsoft testing Windows 8.1 update that hides tile interface by default.* Retrieved from <http://www.theverge.com/2014/1/30/5362156/windows-8-1-update-1-boot-to-desktop-by-default>
- Whitney, L. (2012, March 28). *IE10 in Windows 8: Metro style vs. desktop style.* Retrieved from http://news.cnet.com/8301-10805_3-57405765-75/ie10-in-windows-8-metro-style-vs-desktop-style/
- Whitwam, R. (2013, June 27). *Windows 8.1: A complete list of changes and new features.* Retrieved from <http://www.extremetech.com/computing/159803-windows-8-1-a-complete-list-of-changes-and-new-features>
- Wilhelm, A. (2012, July 07). *Windows 8 boots 55.26% faster than Windows 7, and that's important for tablet devices.* Retrieved from <http://thenextweb.com/microsoft/2012/07/07/windows-8-boots-55-26-faster-than-windows-7-and-thats-important-for-tablet-devices/>
- Wright, N., & Judd, B. (2004, June 01). *Using USB as a Data Acquisition Interface.* Retrieved from <http://www.evaluationengineering.com/articles/200406/using-usb-as-a-data-acquisition-interface.php>
- Yegulalp, S. (2012, December 05). *5 excellent uses of Windows 8 Hyper-V.* Retrieved from <http://www.infoworld.com/d/virtualization/5-excellent-uses-of-windows-8-hyper-v-208436>

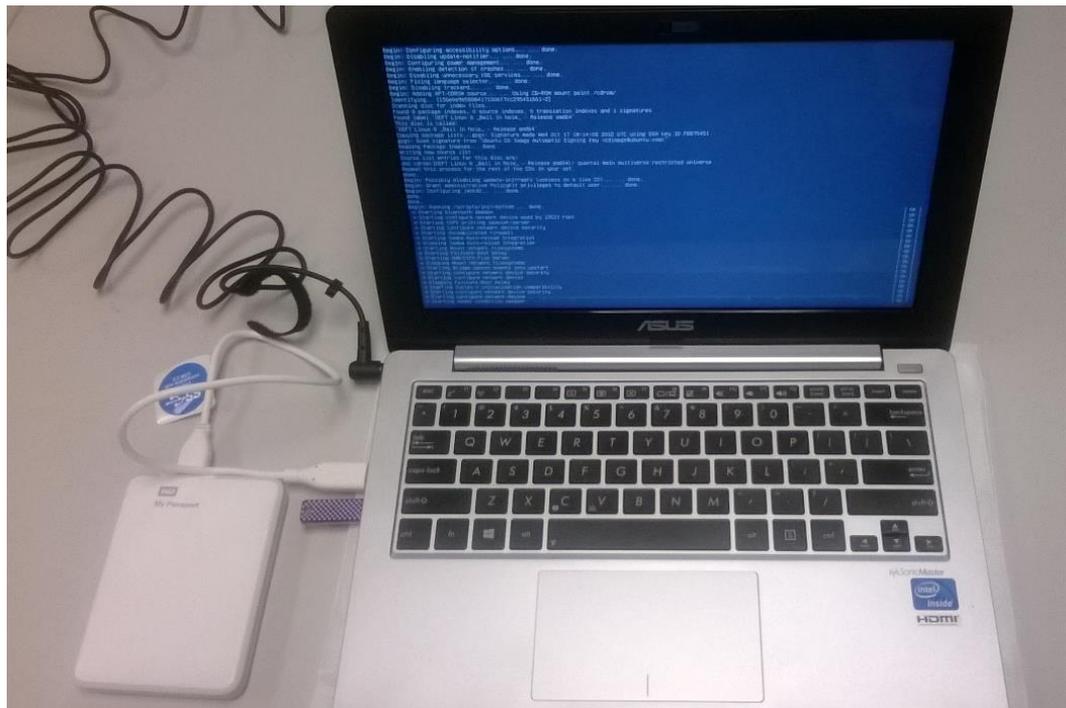
Zhang, S., Wang, L., Zhang, R., & Guo, Q. (2010). Exploratory Study on Memory Analysis of Windows 7 Operating System. *2010 3rd International Conference on Advanced Computer Theory and Engineering(ICACTE), Volume 6*, 373-377.

Zukerman, E. (2013, March 01). *The Windows 8 Task Manager: A Gem Hidden In Plain Sight*. Retrieved from <http://www.makeuseof.com/tag/the-windows-8-task-manager-a-gem-hidden-in-plain-sight/>

Appendices

APPENDIX A: EQUIPMENT SETUP ENVIRONMENT

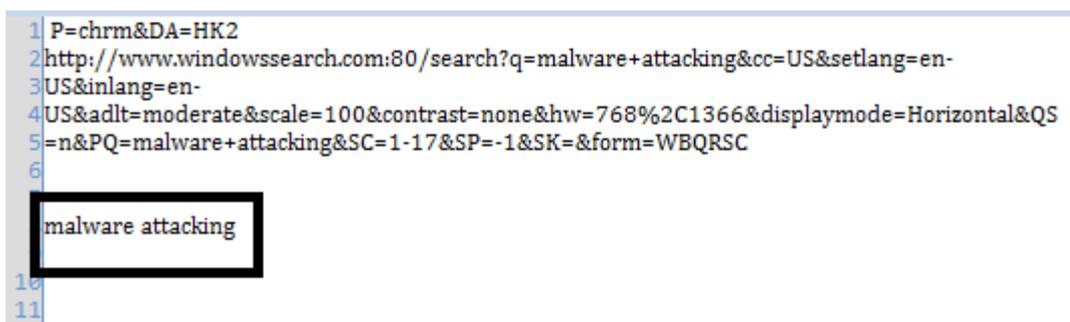
Lab Setup for Data Acquisition



FigureA.1: Data Acquisition

APPENDIX B: FINDINGS SCREENSHOT

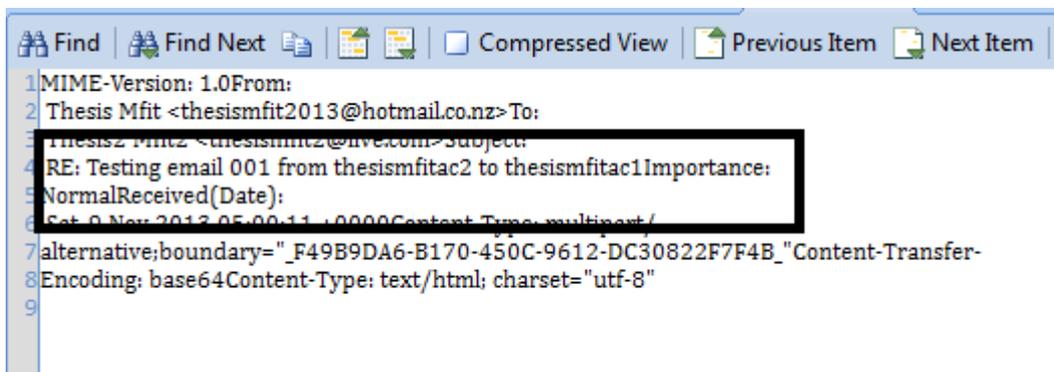
i. Keyword search



| | |
|------------|---|
| 5624513432 | http://www.burgerfuel.com/ |
| 5624516522 | http://www.burgerfuel.com/nz/ |
| 5624517560 | http://uae.burgerfuel.com/ |
| 5624518630 | http://www.burgerfuel.com/nz/au/menu |
| 5624519669 | http://www.burgerfuel.com/nz/radio-burgerfuel |
| 5624520817 | http://www.burgerfuel.com/nz/stores |
| 5624521864 | http://www.burgerfuel.com/nz/au/ |
| 5624523844 | http://www.burgerfuel.com/ |
| 5624526905 | http://www.burgerfuel.com/ |
| 5624529958 | http://www.burgerfuel.com/ |
| 5624532061 | https://twitter.com/BurgerFuel |

FigureB.5: Website Visited From Bulk Extractor

iii. Email sent and received



FigureB.6: Email Sent and Received

iv. Pictures

| | | |
|----|---------------|-----|
| 1 | desktop.ini | ini |
| 2 | Thesis001.jpg | jpg |
| 3 | Thesis002.jpg | jpg |
| 4 | Thesis003.jpg | jpg |
| 5 | Thesis004.jpg | jpg |
| 6 | Thesis005.jpg | jpg |
| 7 | Thesis006.jpg | jpg |
| 8 | Thesis007.jpg | jpg |
| 9 | Thesis008.jpg | jpg |
| 10 | Thesis009.jpg | jpg |
| 11 | Thesis010.jpg | jpg |

FigureB.7: Pictures Found

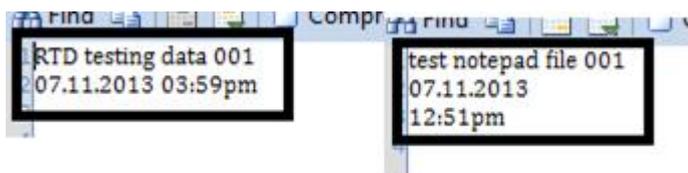
vii. Text documents

| | Ext |
|-------------------|-----|
| RTD test 001.rtf | rtf |
| RTD test 002.rtf | rtf |
| RTD test 003.rtf | rtf |
| RTD test 004.rtf | rtf |
| RTD test 005.rtf | rtf |
| RTD test 006.rtf | rtf |
| RTD test 007.rtf | rtf |
| RTD test 008.rtf | rtf |
| RTD test 009.rtf | rtf |
| RTD test 010.rtf | rtf |
| Test file 001.txt | txt |
| Test file 002.txt | txt |
| Test file 003.txt | txt |
| Test file 004.txt | txt |
| Test file 005.txt | txt |
| Test file 006.txt | txt |
| Test file 007.txt | txt |
| Test file 008.txt | txt |
| Test file 009.txt | txt |
| Test file 010.txt | txt |

FigureB.10: Text Documents

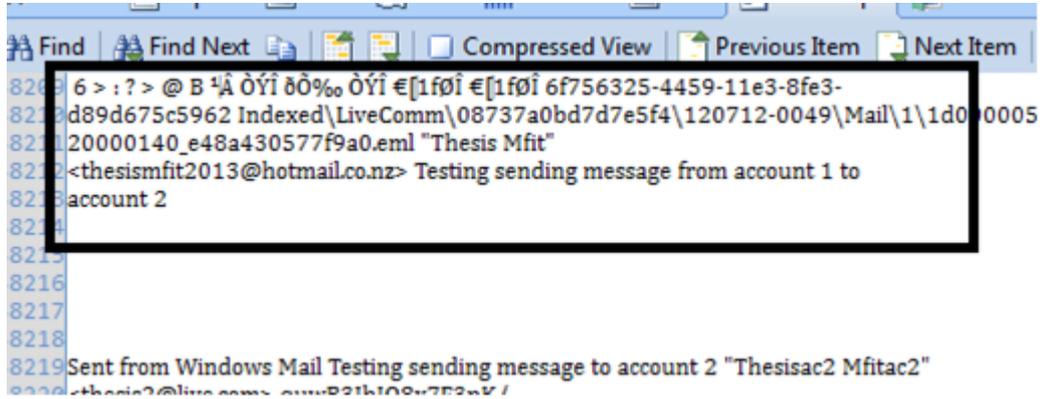
| | | |
|----|-----------|---|
| 1 | MRUListEx | |
| 2 | 0 | PDP?PFN=Microsoft.SkypeApp_kzf8qxf38zg5c&sessionId=9480e6ad2cb64649b3424b6e0a847391&form=WEBPDP |
| 3 | 2 | Thesis Documents |
| 4 | 5 | Test file 002.txt |
| 5 | 6 | Test file 003.txt |
| 6 | 7 | Test file 004.txt |
| 7 | 9 | Test file 005.txt |
| 8 | 10 | Test file 006.txt |
| 9 | 12 | Test file 008.txt |
| 10 | 13 | Test file 009.txt |
| 11 | 14 | Test file 010.txt |
| 12 | 4 | RTD test 001.rtf |
| 13 | 15 | RTD test 003.rtf |
| 14 | 8 | RTD test 002.rtf |
| 15 | 16 | RTD test 004.rtf |
| 16 | 17 | RTD test 005.rtf |
| 17 | 18 | RTD test 006.rtf |
| 18 | 11 | Test file 007.txt |
| 19 | 19 | RTD test 007.rtf |
| 20 | 20 | RTD test 008.rtf |
| 21 | 21 | RTD test 009.rtf |
| 22 | 22 | RTD test 010.rtf |
| 23 | 1 | Test file 001.txt |
| 24 | 3 | Thesis Experiment Documents |
| 25 | 23 | mail.live.com/ |

FigureB.11: Last Opened Files



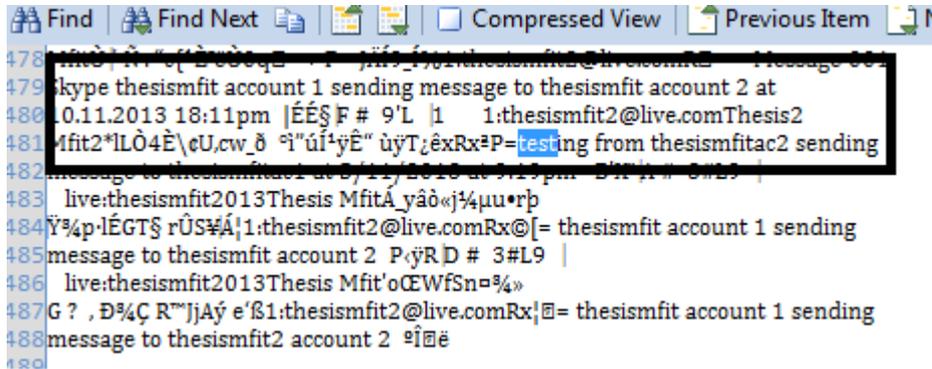
FigureB.12: Text Document Content

i. Message Text Sent and Received



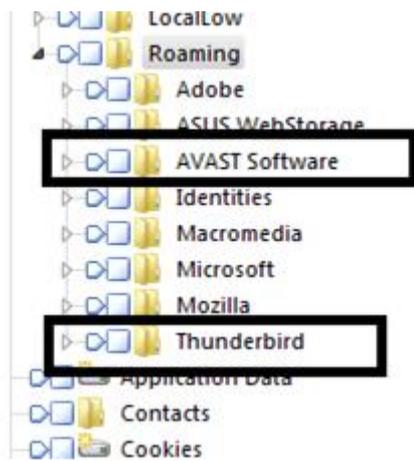
FigureB.13: Messaging Text Sent & Received

ii. Skype

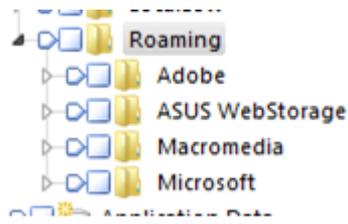


FigureB.14: Skype Message Text Sent and Received

iii. Installed Applications

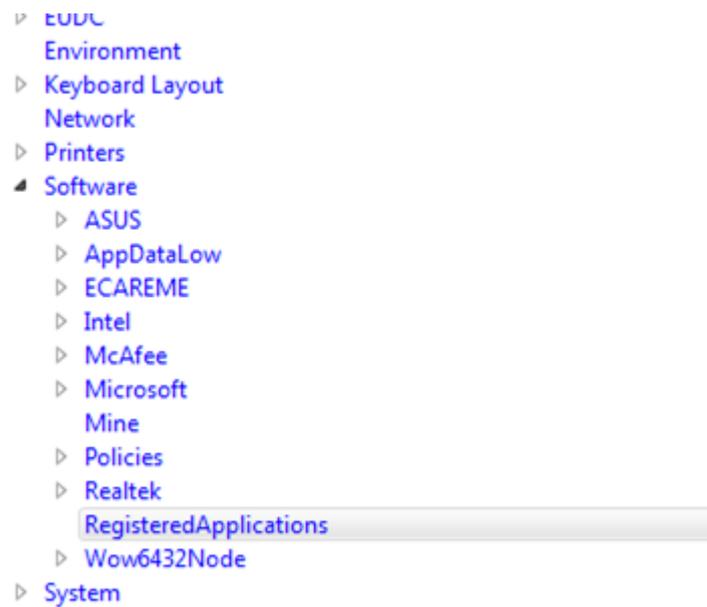


FigureB.15: Installed Applications

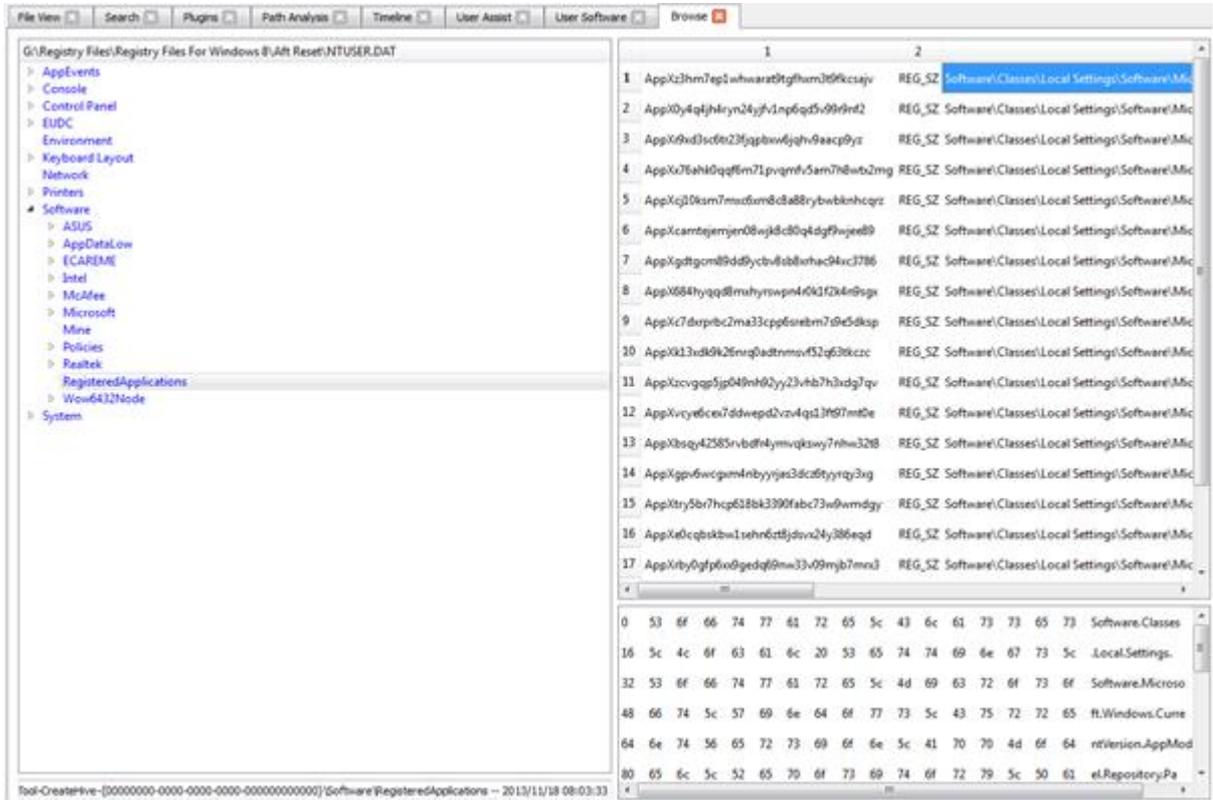


FigureB.16: Installed Application in After Reset Machine

iv. Microsoft Store Applications



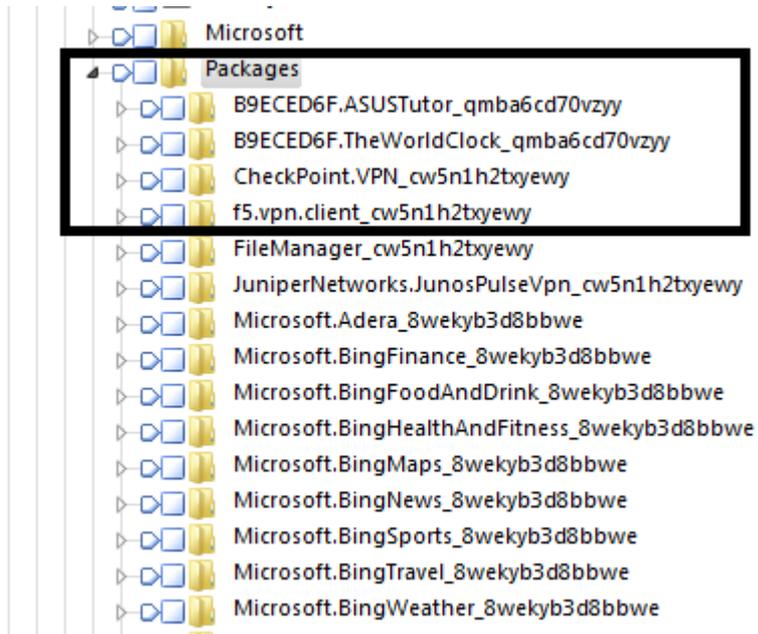
FigureB.17: Microsoft Store Applications in Registry View



FigureB.18: Microsoft Store Applications in Registry View B

| | | | |
|----|--------------------------------------|--------|--|
| 1 | AppXz3hm7ep1whwarat9tgfhxm3t9fkcsajv | REG_SZ | Software\Classes\Local Settings\Software\Microsoft\Windows\CurrentVersion\AppModel\Repository\Packages\{...} |
| 2 | AppX0y4q4jh4ryn24yjf1np6qd5v99r9nf2 | REG_SZ | Software\Classes\Local Settings\Software\Microsoft\Windows\CurrentVersion\AppModel\Repository\Packages\{...} |
| 3 | AppXr9xd3sc6tr23fqpbxw6jqhv9aacp9yz | REG_SZ | Software\Classes\Local Settings\Software\Microsoft\Windows\CurrentVersion\AppModel\Repository\Packages\{...} |
| 4 | AppXx76ahk0qqf6m71pvqmfv5am7h8wbx2mg | REG_SZ | Software\Classes\Local Settings\Software\Microsoft\Windows\CurrentVersion\AppModel\Repository\Packages\{...} |
| 5 | AppXcj10ksm7mxc6xm8c8a88rybwbknhcqz | REG_SZ | Software\Classes\Local Settings\Software\Microsoft\Windows\CurrentVersion\AppModel\Repository\Packages\{...} |
| 6 | AppXcamtejemen08wjk8c80q4dgf9wjee89 | REG_SZ | Software\Classes\Local Settings\Software\Microsoft\Windows\CurrentVersion\AppModel\Repository\Packages\{...} |
| 7 | AppXgdtgcm89dd9ycbv8sb8xrhac94xc3786 | REG_SZ | Software\Classes\Local Settings\Software\Microsoft\Windows\CurrentVersion\AppModel\Repository\Packages\{...} |
| 8 | AppX684hyqqd8mxhyrswpn4r0k1f2k4n9sgx | REG_SZ | Software\Classes\Local Settings\Software\Microsoft\Windows\CurrentVersion\AppModel\Repository\Packages\{...} |
| 9 | AppXc7dxxrbc2ma33cpp6srebm7s9e5dksp | REG_SZ | Software\Classes\Local Settings\Software\Microsoft\Windows\CurrentVersion\AppModel\Repository\Packages\{...} |
| 10 | AppXk13xdk9k26nrq0adtnmsvf52q63tkccz | REG_SZ | Software\Classes\Local Settings\Software\Microsoft\Windows\CurrentVersion\AppModel\Repository\Packages\{...} |
| 11 | AppXzcvqqp5jp049nh92yy23vhb7h3xdq7qv | REG_SZ | Software\Classes\Local Settings\Software\Microsoft\Windows\CurrentVersion\AppModel\Repository\Packages\{...} |

FigureB.19: Microsoft Store Applications in Registry View C



FigureB.19: Microsoft Store Applications in Encase

APPENDIX C: POTENTIAL EVIDENCE DATA INTEGRITY

i. Keywords Search Files

| Files Names | MD5 | SHA1 |
|---------------|----------------------------------|--|
| search[1].htm | 16c17a9eafb3890103db0f4f9e2b1ace | 91d9e11f079d9fe14ee636e405330069f547edc3 |
| search[2].htm | 574690a44a362c794fc0204c4d84aabb | dab7b948a324047a0917419c5f2c4090b78dc189 |
| search[3].htm | 3a69b9b0bd9cc3c1eed399faa8f6c282 | 4fa9c07faf5c713eafa6a2a9292031df73bd5c34 |
| search[4].htm | fc975cb304ac2bd25b81f57e40b4df77 | ed02de669f5c82b6948045135b1fad64c2881cd0 |
| search[5].htm | bb824bc6ad741a3d41b65b5ebd1a0d6f | c6fcea46347b4d42178555374765391c1514b1ef |
| search[6].htm | 31ebf79ee750993c3acc77152f0b53e5 | 0875f2dbb887c7e81faa84494ad9a7c5b5b0b206 |
| search[7].htm | 324d4b4aa7020e3836c0b3bbd2658e80 | 9bf087df58212bf7ffb701fd445d131af3a9ab1b |
| search[8].htm | 6535c28333ae94a12ba9a269d86441a5 | c7151599931b10fa5f7b71b3f2870da823737bb9 |

FigureC.1: Keywords Search Files

ii. SkyDrive Documents

| Files Names | MD5 | SHA1 |
|-----------------------------|----------------------------------|--|
| Thesis MS skydrive 001.docx | c2ee32f56c05f2ae8fde2548b0d58124 | b32617b79964b78f89424b6c30f53de60a211514 |
| Thesis MS skydrive 002.docx | fb915a9fdbd82c58d4551cc0d6c4bf68 | 671f02a6368fc73875966bf55e0b733179f4ec84 |
| Thesis MS skydrive 003.docx | b0dc29aacc94a8dde0631db8aa170f8 | 0629d8e389bcb066e30293ac3c2e7e9906c7b55b |
| Thesis MS skydrive 004.docx | bcfa788a94d5c186ff4c00a4f5fc5719 | 900cd5282faed3ea44838fb7bfdec5cc3137902c |
| Thesis MS skydrive 005.docx | fb915a9fdbd82c58d4551cc0d6c4bf68 | 671f02a6368fc73875966bf55e0b733179f4ec84 |
| Thesis MS skydrive 006.docx | 9247308c775177d2b515113f980f1d2f | 806ea6d688592efad71ad50f8ed8540b4c2c7955 |
| Thesis MS skydrive 007.docx | 8daa12220c6173c84aed4caf15e27ead | e096034818dde3f0f019c3a0d9fcdc4d48f682c0 |
| Thesis MS skydrive 008.docx | c022fcecfc35368c8a9c9fdbbba03685 | 5ef7e8b33d8e01ac343879ddb96e5fec399529db |
| Thesis MS skydrive 009.docx | 8daa12220c6173c84aed4caf15e27ead | e096034818dde3f0f019c3a0d9fcdc4d48f682c0 |
| Thesis MS skydrive 010.docx | 9247308c775177d2b515113f980f1d2f | 806ea6d688592efad71ad50f8ed8540b4c2c7955 |

FigureC.2: SkyDrive Documents

iii. SkyDrive Images

| File Name | MD5 | SHA1 |
|--------------------------------|----------------------------------|--|
| thesis image skydrive 001.jpg | a549fb5a0aa0b99cf5fec938ea55b014 | 7f5c95544ae6e3b0b9d5082fe7db54fa8a16fea6 |
| thesis image skydrive 005.jpg | dad770d6bc14854901697acf47ac4429 | 1968d33db600ae4f6650b2b4ea37e5b67796e8e4 |
| thesis image skydrive 006.jpg | c05db13e428049db3e1cdade23e762a6 | 7fb6c136c0c9e8f61bd7c088f4f2633ded4d5dbd |
| thesis image skydrive 007.jpg | 57c1efdd3271853463f7ccbc5965f2d4 | 55ff5abbd854be8a17dd41cfe14b6b253440a7aa |
| thesis image skydrive 008.jpg | ed5981760ec63da12fee3b16891d10df | a1c321419817352236406976ffcb8ee0716b216d |
| thesis image skydrive 009.jpg | fa78d517b1897afa326b59ff4433f896 | 230d9f3d366f5fc9a745e664adc75d4007882042 |
| thesis image skydrive 010.jpg | d9a82c05db4c7158c596df0bbee21841 | b6ef85d867febade86adbdbb30d227d26229332f |
| thesis image skydrive002.jpg | aff8a924cbb4b5113b49b4d3a31468b0 | fb902b9fff15ae77add4e046f093532fe84c84c |
| thesis images skydrive 003.jpg | 3a4a63dd62e2e571e280d2e52af7c9fe | a1498bf40c37544f6f9f1813c46a1814a2c62f77 |
| thesis images skydrive 004.jpg | 075a53ed60f05fa9558385757c2bf0e8 | 2a1d3f87b794cad4f72ec32c17284186cf087a95 |

FigureC.3: SkyDrive Images

iv. Documents Created

| Files Names | MD5 | SHA1 |
|-------------------|----------------------------------|---|
| RTD test 001.rtf | 4e161e1603eeca36ac90334d2c799dd6 | 6dce5d775e48d59a18b0cdd2d7e bc80b9cc8521b |
| RTD test 002.rtf | 48dbb6184503c721728925dce2dbd794 | cda49249e9d1bc9d2956f8aff3dbf33376dea4d2 |
| RTD test 003.rtf | 757dae2debc342d1e0f1f7b5d86f454f | 22185b6a0b6173d71b6fe3cd0fd2a8fa72513f25 |
| RTD test 004.rtf | cb0467051dc7bb338ae636d5fab016c5 | 919715c7f3fef6c79528dc01463bcc3dff6f6661 |
| RTD test 005.rtf | 7a81ae35f55e242ce70675002f127025 | 592a682681bb405e8cf7ada58cb26f9a42352443 |
| RTD test 006.rtf | 47ef8da604ce841f1f530b50ad7e8f9e | 50686b6a9fc8317a710531dea43548ccd0b3a775 |
| RTD test 007.rtf | 54823ea553e952f85616dfee9ae7b286 | 329e13ae181da5a83fb8143c287a18fd53dfb237 |
| RTD test 008.rtf | abeddec2ff604961719fbf3164847b6c | 6766c230184b459210c6dc32315da214a10ccd02 |
| RTD test 009.rtf | 535edc593cdf2afef2de297e5ee1dc37 | 76d6aaa4e7df3a8c616f7dccc7ca00c3ffd2a7cc |
| RTD test 010.rtf | 521c37ef983b3a35d2cd8bf043eb0f92 | f5303ae339acf44bb2cff63dc6b3acbbf34f9e02 |
| Test file 001.txt | f90e61b8b12fd24032baecb5dd14ad66 | 3416ff60ec2475c7387a73fd19bf297d14272417 |
| Test file 002.txt | a1da9584e8e4be6e1ba283d1bc958cd6 | 901909e60e119c901a9968803a9b13c7acb7914c |
| Test file 003.txt | 8cef63e4ccab52019d2e2f5d2b2e324a | 0051e5a34698045c44f5aea2c062cb68c74ba9e5 |
| Test file 004.txt | c4999bfec1bfae0e1b26a316f6eeebc9 | 649f13a0af787f684c31579b1948df85adafde06 |
| Test file 005.txt | 974750c03d4a47d692e48cc067ecb97f | c9d0643212a3db59a43567f3fc0864b6be238927 |
| Test file 006.txt | 81cbab3116dfb317c44b58d2827e5d21 | 483f686df2db6a7dc02cb5d68b165da53e13cda0 |
| Test file 007.txt | b56d4cd90a434dc6d598c1f1089398d7 | d54e1ec22ecffc2f225e351ed312f4b1642c74f1 |
| Test file 008.txt | c534b34143350884b9d45302a02b41bd | cf6fd2906b77bed86663ed8c2364b79d6cca13f7 |
| Test file 009.txt | 0e5f37a718c09b6f43416e9f88c1ffad | e1d8f0acf5d30b351dceb9419ef746eb25740a14 |
| Test file 010.txt | bd08c0c1427a4901c7825d0f57863c3f | a538d59f2f77511dfb9bc1d328c218d510be0eba |

FigureC.4: Documents Created

v. Local Drive Images

| Files Names | MD5 | SHA1 |
|-------------------|----------------------------------|---|
| RTD test 001.rtf | 4e161e1603eeca36ac90334d2c799dd6 | 6dce5d775e48d59a18b0cdd2d7e bc80b9cc8521b |
| RTD test 002.rtf | 48dbb6184503c721728925dce2dbd794 | cda49249e9d1bc9d2956f8aff3dbf33376dea4d2 |
| RTD test 003.rtf | 757dae2debc342d1e0f1f7b5d86f454f | 22185b6a0b6173d71b6fe3cd0fd2a8fa72513f25 |
| RTD test 004.rtf | cb0467051dc7bb338ae636d5fab016c5 | 919715c7f3fef6c79528dc01463bcc3dff6f6661 |
| RTD test 005.rtf | 7a81ae35f55e242ce70675002f127025 | 592a682681bb405e8cf7ada58cb26f9a42352443 |
| RTD test 006.rtf | 47ef8da604ce841f1f530b50ad7e8f9e | 50686b6a9fc8317a710531dea43548ccd0b3a775 |
| RTD test 007.rtf | 54823ea553e952f85616dfee9ae7b286 | 329e13ae181da5a83fb8143c287a18fd53dfb237 |
| RTD test 008.rtf | abeddec2ff604961719fbf3164847b6c | 6766c230184b459210c6dc32315da214a10ccd02 |
| RTD test 009.rtf | 535edc593cdf2afef2de297e5ee1dc37 | 76d6aaa4e7df3a8c616f7dccc7ca00c3ffd2a7cc |
| RTD test 010.rtf | 521c37ef983b3a35d2cd8bf043eb0f92 | f5303ae339acf44bb2cff63dc6b3acbbf34f9e02 |
| Test file 001.txt | f90e61b8b12fd24032baecb5dd14ad66 | 3416ff60ec2475c7387a73fd19bf297d14272417 |
| Test file 002.txt | a1da9584e8e4be6e1ba283d1bc958cd6 | 901909e60e119c901a9968803a9b13c7acb7914c |
| Test file 003.txt | 8cef63e4ccab52019d2e2f5d2b2e324a | 0051e5a34698045c44f5aea2c062cb68c74ba9e5 |
| Test file 004.txt | c4999bfec1bfae0e1b26a316f6eeebc9 | 649f13a0af787f684c31579b1948df85adafde06 |
| Test file 005.txt | 974750c03d4a47d692e48cc067ecb97f | c9d0643212a3db59a43567f3fc0864b6be238927 |
| Test file 006.txt | 81cbab3116dfb317c44b58d2827e5d21 | 483f686df2db6a7dc02cb5d68b165da53e13cda0 |
| Test file 007.txt | b56d4cd90a434dc6d598c1f1089398d7 | d54e1ec22ecffc2f225e351ed312f4b1642c74f1 |
| Test file 008.txt | c534b34143350884b9d45302a02b41bd | cf6fd2906b77bed86663ed8c2364b79d6cca13f7 |
| Test file 009.txt | 0e5f37a718c09b6f43416e9f88c1ffad | e1d8f0acf5d30b351dceb9419ef746eb25740a14 |
| Test file 010.txt | bd08c0c1427a4901c7825d0f57863c3f | a538d59f2f77511dfb9bc1d328c218d510be0eba |

FigureC.5: Local Drive Images

vi. Communication Applications Logs

| Files Name | MD5 | SHA1 |
|-------------|----------------------------------|--|
| edb.log | 31cee041fda0f561173f2396883de2ed | 6696dedd7d2f727001a578a07d7562f760df4826 |
| livecom.edb | 1d0555c4ccef9b52071e6d367233a74d | 1e3468626da54dcd358b3fb762f19c9df7e632a2 |
| main.db | 3b6008828d2b7edf88c72bb1a4adfebf | 0e795d32db5968bc2fb1be7501b0c52d3c6eb003 |

FigureC.6: Communication