UNIVERSITI PUTRA MALAYSIA

DIGITAL FORENSIC INVESTIGATION REDUCTION MODEL (DIFReM) FOR WINDOWS 10 OS

YAZID HARUNA SHAYAU

FSKTM 2018 49
DIGITAL FORENSIC INVESTIGATION REDUCTION MODEL (DIFReM) FOR WINDOWS 10 OS

By

YAZID HARUNA SHAYAU

Thesis Submitted to the School of Graduate Studies, Universiti Putra Malaysia, in Fulfilment of the Requirements for the Degree of Master of Information Security June 2018
COPYRIGHT PAGE

All material contained within the thesis, including without limitation text, logos, icons, photographs and all other artwork, is copyright material of Universiti Putra Malaysia unless otherwise stated. Use may be made of any material contained within the thesis for non-commercial purposes from the copyright holder. Commercial use of material may only be made with the express, prior, written permission of Universiti Putra Malaysia.

Copyright © Universiti Putra Malaysia
DEDICATION

“To everyone that makes life in this cold world warm – you are the little and big bits that complete me”
ABSTRACT

Abstract of thesis presented to the Senate of Universiti Putra Malaysia in fulfilment of the requirement for the degree of Master of Information Security

DIGITAL FORENSIC INVESTIGATION REDUCTION MODEL (DIFReM) FOR WINDOWS 10 OS

By

YAZID HARUNA SHAYAU

JUNE 2018

Chair: Dr Aziah Asmawi

Faculty: Faculty of Computer Science and Information Technology

The adoption of the digital age, globalization of the world and move towards automation has made life for individuals and businesses easy. With the increasing use of digital devices and internet, cybercrimes are also increasing day by day so, digital forensics has become more important. And the investigator relies on the effectiveness and efficiency of digital forensics tools. Digital Forensics as defined in ISO/IEC 27001 (Information security standards published jointly by the International Organization for Standardization – ISO and the International Electrotechnical Commission - IEC), provides guidance on identifying, gathering/collecting/acquiring, handling and protecting/preserving Digital Forensic evidence i.e. “digital data that may be of evidential value” for use in court. The six basic steps defined by Digital Forensics Research Workshop (DFRWS) and generally followed in the forensic investigation are Identification, Preservation, Collection, Examination, Analysis and Presentation. The most important part of Digital Forensic Investigation (DFI) is the examination of data – knowing the data type and nature beforehand makes this easier.
Unfortunately, most of the time an investigation is required, such helpful details are not available and the investigator has to “grope in the dark”. The examination phase is the most challenging for an investigator; in Microsoft Windows OS (Operating System), investigators have to go through large storage in Terabytes having hundreds of thousands of OS data most of which are irrelevant (to the investigation) or application files gathered from a suspect’s computer. We propose a data reduction model (DIFReM) and tool which will not only help the investigator in identifying modified system files but also the ability to detect files inserted into system directories and also be able to verify integrity using hashing. We created an index of clean Windows 10 Professional 64-bit edition. After which a filename, filepath and hash analysis of all files was done. The result of which was used as our database for the DIFReM. This database was used by the tool (which is built on Python and C#) to investigate suspect’s system for files that were added to Windows directory or have their content modified in the system files directory regardless of the time the file was Modified, Accessed or Created (MACtimes). An algorithm was used to verify filetypes by looking up a File Signature library to compare files’ header with their extension. Also, a hash integrity comparison was performed on all files. By putting a very few files (12) in such large dataset, we made it more difficult to detect but the tool detected all modified files, added files, deleted files with modified file header, files with changed extension and also files with failed hash verification – this represented a 100% detection rate. We believe this reduction model with its tool geared towards Microsoft Windows 10 Professional operating system is a more efficient forensic tool for Windows 10 64-bit professional than generic tools used and will open a path for OS-defined Forensic tools which will definitely be a delight to many investigators as it will hasten the examination phase of digital forensic process.
ABSTRAK

Abstrak tesis yang dikemukakan kepada Senat Universiti Putra Malaysia Sebagai memenuhi keperluan untuk ijazah Sarjana Keselamatan Maklumat

DIGITAL FORENSIC INVESTIGATION REDUCTION MODEL (DIFReM) FOR WINDOWS 10 OS

Oleh

YAZID HARUNA SHAYAU

JUNE 2018

Pengerusi: Dr Aziah Asmawi

Fakulti: Fakulti Sains Komputer dan Teknologi Maklumat

Pengumpulan, Pemeriksaan, Analisis dan Pembentangan. Bahagian yang paling penting dalam Penyiasatan Forensik Digital (DFI) adalah pemeriksaan data – mengetahui jenis data dan sifat dahulu membuatkannya lebih mudah. Malangnya, kebiasaannya penyiasatan memerlukan, butiran yang jelas tidak diperoleh dan penyiasat perlu “meraba dalam kegelapan”. Fasa pemeriksaan adalah tugas yang paling ketara; dalam Microsoft Windows OS (Sistem Operasi), penyiasat perlu melalui simpanan yang besar pada komputer peribadi dengan Terabytes yang mempunyai ratusan dan ribuan data dimana kebanyakkannya yang tidak relevan (pada penyiasatan) OS atau fail-fail aplikasi yang dikumpulkan dari komputer suspek. Kami mencadangkan model pengurangan data (DIFReM) dan alat forensik yang bukan hanya akan membantu penyiasat mengenal pasti fail sistem yang diubah suai malah berupaya untuk mengesan fail yang dimasukkan ke dalam direktori sistem dan juga dapat mengesan integriti dengan menggunakan hashing. Kami mencipta indeks edisi 64-bit Windows 10 Professional yang tulen. Selepas nama fail, filepath dan hash analisis untuk semua fail telah dilakukan, hasilnya digunakan sebagai pangkalan data kami untuk DIFReM. Pangkalan data ini digunakan oleh alat (yang dibina menggunakan Python dan C#) untuk menyiasat sistem suspek terhadap fail yang ditambahkan pada direktori Windows atau kandungannya diubah suai dalam direktori fail sistem tanpa mengira masa fail tersebut diubahsuai, diakses atau dicipta (MACtimes). Algoritma digunakan untuk mengesan filetype dengan melihat perpustakaan Fail Signature untuk membandingkan header fail dengan pelanjutan mereka. Perbandingan integriti hash juga dilakukan pada semua fail. Meletakkan fail yang sangat sedikit (12) dalam dataset yang besar, kami menjadikannya lebih sukar untuk dikesan tetapi alat ini mengesan semua fail yang diubah suai, menambah fail, fail yang dihapuskan dengan header fail yang diubahsuai, fail dengan lanjutan yang
berubah dan juga fail dengan pengesahan hash yang gagal - ini mewakili kadar pengesanan 100%. Kami percaya model pengurangan ini dengan alat yang diarahkan ke sistem pengendalian Microsoft Windows 10 Professional adalah lebih maju sebagai alat forensik untuk Windows 10 64-bit Professional daripada alat generik yang digunakan dan akan membuka laluan untuk alat Forensik yang ditakrifkan OS yang pasti akan menjadi kesenangan kepada banyak penyiasat kerana ia akan mempercepatkan fasa peperiksaan proses forensik digital.
ACKNOWLEDGEMENTS

With a deep sense of admiration, my profound gratitude goes to my supervisor, Dr. Aziah Asmawi for her patience and guidance. She did not only take pain to go through the project with me and make necessary corrections as/when needed but was benevolent enough to ensure I was able to balance the research with my other academic and personal commitments.

My sincere thanks to my assessor, Dr. Mohd. Taufik Abdullah who enchanted me into the beautiful world of Digital Forensics.

My research would have been impossible without sponsorship from the Federal Republic of Nigeria through the Tertiary Education Trust Fund (TETFund) and my institution, Kebbi State University of Science and Technology, Aliero (KSUSTA) by granting me the opportunity to undertake this program.

I owe a great many thanks to the people who supported me during my academic forays. Precious appreciation goes to Nurul Nadia, who has always been helpful and supportive, thank you for translating the abstract and also formatting the entire thesis, you are amazing. My brother, Abbas also, Aliyu, Harmi, Asma’u and all my course mates.

A special thank you to the entire staff of Fakulti Sains Komputer dan Teknologi Maklumat, University Putra Malaysia especially all my lecturers. Not forgetting the Admin, Security and IT staff who were always at hand to help. Also, the Cleaners that
kept the amenities in top shape and always cleaned up after us for a wonderful
eighteen months of conducive educational and moral enrichment.

Heartfelt thanks go to an endless list of friends, well-wishers, the entire Naijacom and
UPMISA, wish I could write out all your names here, I’m honored for the unending
physical, emotional and moral support.

I would like to thank the beacons of my life, my special mothers; Hon. Justice Fati
Yusuf Imam -Your love and support have been equivalent to those of a biological
mother, Hajiya Maryam Sadiq Marafa and Hajiya A’isa Siddiq. My brother from my
other mother, Abullahi Yusuf Imam, my uncles, Yaya Rabi’u NaAllah, Haruna Ka’oji, Sadiq Abdullahi, Attahiru Ibrahim Mayaki, Yahaya Aliyu, Yusuf H. Sarki, Abdullahin
Mayaki Family, the entire Shayau, Alkali Tanko and Baura Families, thank you for
supporting me during this challenging period.

Finally, the cream of appreciations goes to my parents for their steadfast support,
patience, unrivaled love and care. Immeasurable thankfulness goes to mum, for
showing superhuman patience and proving that, a mother’s love knows no bounds-
you’ll always be my star, my wife for putting up with me and my siblings for the fun,
crazy and mad moments that make life worth living.

Yazid Haruna Shayau
APPROVAL

This thesis was submitted to the Senate of Universiti Putra Malaysia and has been accepted as fulfillment of the requirement for the degree of Master of Information Security. The members of the Supervisory Committee were as follows:

Signature: _________________________________

DR AZIAH ASMAWI

Faculty of Computer Science and Information Technology
Universiti Putra Malaysia
(Supervisor)
Date: ____________
DECLARATION

I hereby confirm that:

This thesis is my original work; except for the quotations and citations which have been duly acknowledged. I declare that it has not been previously submitted for any other degree at Universiti Putra Malaysia or at any other institutions.

Signature:___________________ Date:__________________

Name and Matric No.: Yazid Haruna Shayau (GS48608)
LIST OF FIGURES

Figure 1. Digital Forensics Phases.................................................................2
Figure 2. Digital Forensic Data Reduction and Data Mining Framework...........10
Figure 3. Everything.......................................................................................36
Figure 4. Locate32.........................................................................................38
Figure 5. MasterSeeker..................................................................................40
Figure 6. Recursive hash list generation........................................................47
Figure 7. FAT16 Directory Structure...............................................................52
Figure 8. FAT32 Directory Structure...............................................................52
Figure 9. NTFS Directory Structure.................................................................53
Figure 10. Extensions in regedit......................................................................54
Figure 11. File extension change.................................................................55
Figure 12. Pre-processing Windows 10 64-bit OS files index..........................61
Figure 13. DIFReM components flowchart....................................................62
Figure 14. Comparing suspect’s OS files to index for investigation..............63
Figure 15. Filetype verification using file signature in file header..................64
Figure 16. DIFReM Framework.....................................................................65
Figure 17. Indexing framework with Python................................................66
Figure 18. Framework for Index comparison...............................................68
Figure 19. Framework for file signature and header comparison..................72
Figure 20. DIFReM1 Index with Python.........................................................83
Figure 21. DIFReM2 Index with Python.........................................................83
Figure 22. DIFReM1 Index with Everything..................................................84
Figure 23. DIFReM2 Index with Everything..................................................84
Figure 24. DIFReM1 Index with Locate32.....................................................85
Figure 25. DIFReM2 Index with Locate32.....................................................85
Figure 26. DIFReM1 Index with MasterSeeker..............................................86
Figure 27. DIFReM2 Index with MasterSeeker..............................................86
Figure 28. Recursive File hashing of all files...............................................87
Figure 29. Selecting index database for comparison...............................89
Figure 30. Summary of comparison result.............................................90
Figure 31. Details of the comparison result...........................................91
Figure 32. Hash Analysis with Successful Match...................................92
Figure 33. Hash Analysis with Failed Match........................................92
Figure 34. Selecting File for File Signature Analysis.............................93
Figure 35. File Signature Analysis Result...........................................93
Figure 36. File Header Analysis with Successful Match.........................94
Figure 37. File Header Analysis with Failed Match...............................95
LIST OF TABLES

Table 1. Windows framework files.................................................................19
Table 2. Files found on Windows by Indexing tools......................................87
Table 3. Time Taken to Index Files Found on Windows.................................88
Table 4. Time To generate hash values of Windows files..............................88
Table 5. Differences Between Proposed and Existing Digital Forensics Tools.....96
Table 6. File Signature and Corresponding File Types..................................111
# Table of Contents

ABSTRACT ............................................................................................................................. iv  
ABSTRAK ............................................................................................................................... vi  
ACKNOWLEDGEMENTS ........................................................................................................... ix  
APPROVAL ............................................................................................................................. xi  
DECLARATION .......................................................................................................................... xii  
LIST OF FIGURES .................................................................................................................. xiii  
LIST OF TABLES ..................................................................................................................... xv  
CHAPTER 1 ............................................................................................................................. 1  
INTRODUCTION .................................................................................................................... 1  
   1.1 Digital Forensics ............................................................................................................. 1  
   1.2 Digital Forensics Processes ............................................................................................ 1  
   1.3 Purpose and significance of the Study .......................................................................... 3  
   1.4 Problem Statement ......................................................................................................... 4  
   1.5 Research Questions ........................................................................................................ 4  
   1.6 Research Objectives ....................................................................................................... 5  
   1.7 Research Scope ............................................................................................................... 5  
   1.8 Report Structures ........................................................................................................... 6  
CHAPTER 2 ............................................................................................................................. 7  
LITERATURE REVIEW ............................................................................................................ 7  
   2.1 Review of the Existing Application Techniques .............................................................. 7  
   2.2 Digital Forensic Data Reduction and Data Mining Framework ....................................... 7  
   2.3 Digital Forensic Data Reduction by Selective Imaging .................................................. 18  
   2.4 Reduction as a Solution .................................................................................................... 26  
   2.5 Windows Index ................................................................................................................ 27  
   2.6 Windows.edb File in Windows 10 Professional 64-bits .................................................. 30  
   2.7 Python ........................................................................................................................... 32  
   2.8 Use of Applications Designed for Searching and Indexing Files .................................... 36  
      2.8.1 Everything ............................................................................................................. 36  
      2.8.2 Locate32 ................................................................................................................. 38  
      2.8.3 Masterseeker ......................................................................................................... 40  
   2.9 Hash Analysis .................................................................................................................. 42  
   2.10 Hash Algorithm Security .............................................................................................. 43  
      2.10.1 Positive Hash Analysis ........................................................................................ 46
RESULTS AND DISCUSSION ................................................................. 88
   4.1 Introduction .............................................................................. 88
   4.2 Findings ............................................................................... 88
   4.3 Using Index Database to Test DIFReM3 ................................. 89
   4.4 Hash Comparison Between Database and DIFReM3 .............. 92
   4.5 Filetype Signature Comparison .............................................. 93
   4.6 Header Modification Comparison ......................................... 94
   4.7 Review of the Application .................................................... 95
   4.8 Differences Between Proposed Method and Existing Methods/Tools .................................................. 96
CHAPTER 5 .......................................................................................... 97
SUMMARY, CONCLUSION, AND RECOMMENDATIONS FOR FUTURE RESEARCH ................................................................. 97
   5.1 Introduction .............................................................................. 97
   5.2 Consequence of Result .......................................................... 97
   5.3 Glossary ............................................................................... 98
   5.4 Conclusion .............................................................................. 100
   5.5 Future Work .......................................................................... 102
      5.5.1 Indexing .......................................................................... 102
      5.5.2 File Hash ......................................................................... 102
      5.5.3 Filetype Signature ............................................................ 102
      5.5.4 Header Analysis ............................................................... 102
      5.5.5 Updated Files (Windows) ................................................ 103
      5.5.6 Windows Upgrade/Change ............................................ 103
      5.5.7 ADS .............................................................................. 103
      5.5.8 Keyword Search ............................................................. 103
REFERENCES .................................................................................. 104
BIBLIOGRAPHY ............................................................................... 107
APPENDIX A .................................................................................. 111
CHAPTER 1
INTRODUCTION

1.1 Digital Forensics

The primary purpose of digital forensics may be explained as the processes of discovery, protection, collection, analysing, and presenting legal electronic evidences which are thought of as potential evidences[9,10]. Digital forensics aims to discover digital evidence for different types of cases ranging from identification of a digital intruder to resolution of a murder case.

In digital forensics, the main objective is not to directly expose a person as guilty or innocent. It aims to provide numerical evidences to forensics unit in a different way as complete and impartial interpretation of the evidence. Conclusion on the culpability of the suspect lies on the judicial authorities by using the evidence presented by the forensics investigator as a result of his/her investigation of the evidence obtained through digital judicial processes to judicial units [12].

There are other areas of digital forensics which can be known as data recovery, data annihilation, data conversion, encryption, decryption, finding undercover files, identifying criminals with the help of IP numbers[13] etc.

1.2 Digital Forensics Processes

Processes which culminate to arriving at legal electronic evidence from investigated electronic evidence is called “Digital Forensics phases”[14] Digital forensics phases are shown in figure 1[11,12,14,15]; these parts explain how evidences are processed
beginning with the crime scene investigation then collection of evidence, protection of evidence, analysing evidence, reporting and presenting the evidence.

Every processes begins at its starting point[16]. For Digital forensics, the starting point is a realization of a crime or incidence due to a report, suspicious records, sign of intrusion, alteration denunciation of an individual or crime case.

Those that respond first to a crime scene are responsible for its security and that of the evidences. Therefore, first responders and digital forensics investigators should be properly trained on protocols of identifying a crime scene (taking pictures and videos) beforehand [16,17] They should be well trained in securing and protecting the crime scene. The figure below shows the Digital forensics phases.

![Figure 1. Digital Forensics Phases](image-url)
1.3 Purpose and significance of the Study

As explained above, a forensics Investigator has to go through a structured process to ensure having not only the right evidence which will be accepted in a court but also to do that within the shortest possible time to ensure the trial process doesn’t stall or getting the information after trial.

With this in mind, anything that can help expedite the investigative process without being detrimental to the veracity and integrity of the evidence is a welcome development for the investigator. As such we look into digital crimes with a concentration on Microsoft platform and also Windows 10 64bit Operating System as it is steadily taking over the niche dominated by earlier versions of Windows family (Windows 10 has been slowly clutching up the OS user share. It’s a topsy-turvy fight between Windows 7 and 10 but considering the fact that support for Windows 7 will end January 14, 2020, Windows 10 will surely take over). Also, all computers manufactured now with Microsoft OS only run Windows 10 OS OOB (Out of Box).

The project is a proposed model as a reduction model is aimed at speeding up the investigative process for the investigator by isolating the OS files and running basic investigative operations while the investigator works on other areas. But this doesn’t mean the investigator can’t fall back to this section if wished. These will be explained further in Chapter 3.
1.4 Problem Statement

During Digital Forensic Investigation (DFI), the examination phase is the most tasking; in Windows OS, Investigators have to go through large storage on personal computers in Terabytes having hundreds and thousands of data most of which are irrelevant (to the investigation) OS or application files gathered from a suspect’s computer.

Also, a suspect is able to hide evidence in such location so an investigator may inadvertently overlook or keep aside the OS files thereby, losing critical information while disregarding them as immaterial artifacts or, change the extension so that the real filetype is not known. A well learned adversary can modify highly technical aspects of a file thereby changing sensitive information and throwing investigators off.

1.5 Research Questions

This research aims at seeing if detection and isolation of Windows OS files from investigation due to their enormous volume will speed up a forensic investigation by giving the investigator ability to conduct artifact-examination on non-OS files.

If so, will knowing the real default index of all installed files help the investigator detect if addition has been made to the Windows OS directories?

Will the identification of file(s) that has/have been morphed as a different filetype(s) by changed file extension or modification of file header help the investigator detect them as masked?
1.6 Research Objectives

To create an algorithm which will reduce the volume of contents to be perused by the Investigator (By eliminating OS files from artifacts to be investigated) thereby making the investigative process less tedious and also, faster. Also, to:

- Provide the investigator with files that are suspected to have been removed from or added to OS installation directory after installation (regardless of MACtimes)
- Give the Investigator the ability to detect which filetype(s) have been modified based on File Signature in the header (countermeasure for hiding files by changing their default file extensions) and also detect any modification of file header data.

1.7 Research Scope

The scope of this project is to develop algorithms that will access and retrieve specific data that the investigator deems relevant from a Windows OS device. It is limited only to Windows 10 Professional 64-bit OS. An application will be designed to do this job in three (3) parts;

1) Compare an index of a clean unadulterated installation index against the suspect’s system for a mirrored analysis including among others, hash function.

2) Weed out irregular files not related to the investigation which include but not limited to application files, windows installation files, registry files etc.

3) Detect files hidden in the OS directories or by change of file extension.

Limitations will come from difficulty in creating the algorithm, designing the application, and harmonizing the two within the given period of time. Python and C#
will most likely be the programming languages I’ll adopt which is a pseudo-problem as I’m not adept in them. The project is estimated to be completed in one-year time.

1.8 Report Structures

As there are six chapters in this report, Chapter 1 is gives an introduction, meaning of Digital Forensics. Research objectives have been covered as solutions to our research problems, and research scope was explained on the requirements before start with the method used, also discussed are limitations of this project. Next, Chapter 2 focuses on the literature review, which includes varieties of existing Digital Forensics Investigative tools and processes with their own upgraded technologies. The methodology is presented in Chapter 3, which includes research design with flowchart, frameworks and project requirements. Then, Chapter 4 explains on results and findings with discussion contained with screenshots to analyze more clearly, also added are the differences of proposed method and existing methods in a table. Chapter 5 holds the summary on the overall project which has been done. Also discussed are conclusions and future work or research areas of this project.
REFERENCES


[36] Quick D & Choo K 2013c. *Forensic collection of cloud storage data: Does the act of collection result in changes to the data or its metadata?* Digital Investigation 10(3): 266–277


BIBLIOGRAPHY


Automated Forensic Analysis using Digital Forensic Framework. (n.d.).


Robert, H. (2011). This is a repository copy of Forensic Data Recovery From The Windows Search Database . White Rose Research Online URL for this paper : Version : Submitted Version Article : Chivers , Howard Robert orcid . org / 0000-0001-7057-9650 and Hargreaves , C ( 201.


107


Big forensic data management in heterogeneous distributed.pdf. (n.d.).
