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

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

Penerimaan kehidupan digital selama ini, globalisasi dunia juga bergerak ke arah automasi menjadikan kehidupan individu dan perniagaan mudah. Penggunaan peranti digital dan internet meningkat, justeru jenayah siber juga semakin meningkat dari hari ke hari, dengan itu forensik digital menjadi lebih penting. Tambahan pula penyiasat yakin dengan pada keberkesanan dan kecekapan alat forensik digital. Forensik Digital yang didefinisikan dalam ISO/IEC 27001 (Piawaian keselamatan maklumat yang diterbitkan bersama oleh Organisasi Antarabangsa untuk diselaraskan – ISO dan Suruhanjaya Elektroteknikal Antarabangsa – IEC), menyediakan panduan untuk mengenal pasti, menghimpunkan/mengumpul/memperoleh, mengendalikan dan menjaga/memelihara bukti-bukti Forensik Digital seperti "data digital yang mungkin nilai yang jelas" untuk digunakan dalam mahkamah. Enam langkah asas yang ditakrifkan oleh Bengkel Penyelidikan Forensik Digital (DFRWS) dan umumnya diikuti dalam penyiasatan forensic adalah Pengenalpastian, Pemeliharaan, 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 tugasan 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 mengesahkan 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 mengesahkan *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'oje, 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

LIST OF TABLES

Table of Contents

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.

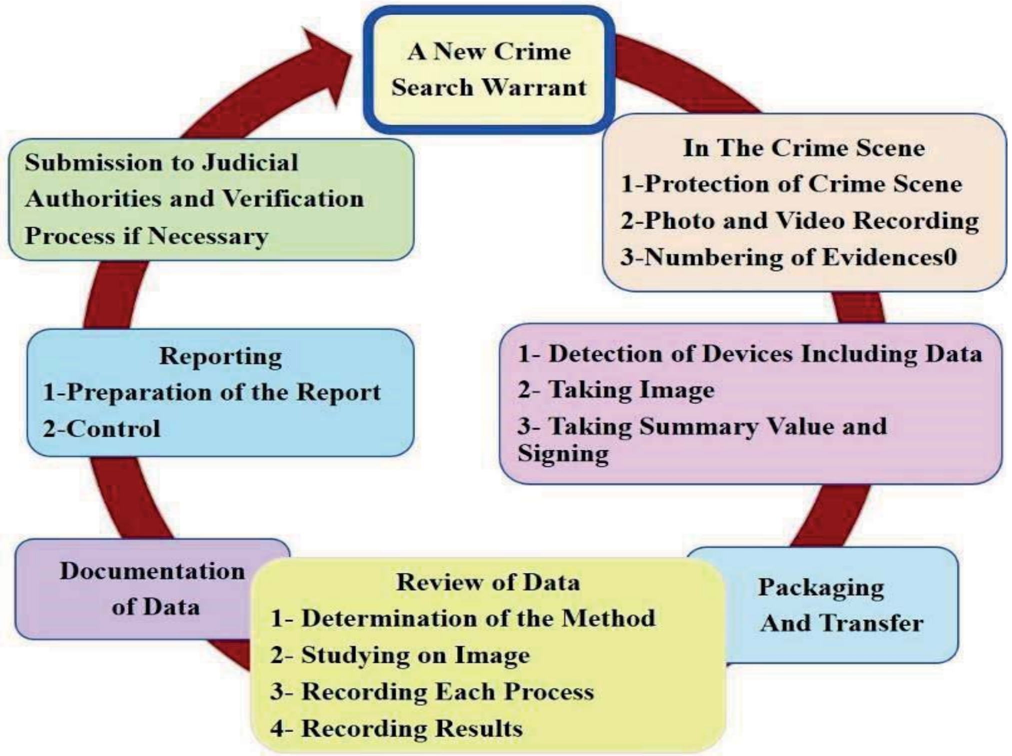
A New Crime
Search Warrant
In The Crime Scene
1-Protection of Crime Scene
2-Photo and Video Recording
3-Numbering of Evidences0
1- Detection of Devices Including Data
2- Taking Image
3- Taking Summary Value and Signing
Packaging
And Transfer
Review of Data
1- Determination of the Method
2- Studying on Image
3- Recording Each Process
4- Recording Results
Documentation
of Data
Reporting
1-Preparation of the Report
2-Control
Submission to Judicial
Authorities and Verification
Process if Necessary

Figure 1. Digital Forensics Phases

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.

REFERNCES

[1] G. Palmer and M. Corporation, "*A road map for digital forensic research*", in Proc. the 1st Digital Forensic Research Workshop, 2001, pp. 1-48

[2] Guidance Encase Tool, [Online], Available: http://www.guidancesoftware.com/, 2017. [Accessed 05 10 2017].

[3] Access Data Forensic Toolkit, [Online], Available: http://www.accessdata.com, 2017. [Accessed 05 10 2017].

[4] Sleuth Kit & Autopsy Tool, [Online], Available: http://www.sleuthkit.org, 2017. [Accessed 05 10 2017].

[5] Y. Kim and J. Kim, "*A Forensic Model on Deleted-File Verification for Securing Digital Evidence,*" 2010 International Conference on Information Science and Applications (ICISA), Seoul, Korea, 2010. doi:978-1-4244-5493-8710

[6] A. H. Ekizer, "*Adli Bilisim (Computer Forensics),"* [Online] Available: ttp://www.ekizer.net/content/view/16/1/1. [Accessed 05 10 2017].

[7] Adedayo, O. M. (2016, 12-14 June 2016). *Big data and digital forensics*. Paper presented at the 2016 IEEE International Conference on Cybercrime and Computer Forensic (ICCCF).

[8] Netmarketshare, [Online], http://www.netmarketshare.com, 2017.

[9] S. Sagiroglu and M. Karaman, "*Adli Bilisim*", Telepati Dergisi, no. 203, pp. 62, 2012.

[12] M. Ozen and G. Ozocak, "*Adli Bilisim, Elektronik Deliller ve Bilgisayarlarda Arama El El Koyma Tedbirinin Hukuki Rejimi (CMK M. 134)",* Ankara Barosu Dergisi, pp. 43–77, 2015.

[13] M. Z. Gunduz, "*Bilisim suclarina yonelik IP tabanlz delil tespiti-IP-based evidence detection"*, Elazig: Firat Universitesi, Fen Bilimleri Enstitusu, Yuksek Lisans Tezi, 2013.

[14] M. Orta, "*Bilisim Suclartnda Adli Analiz*", Konya: Selcuk Universitesi Sosyal Bilimler Enstitusu, Doktora Tezi, 2015.

[15] L. Keser Berber, *Adli Bilisim*, Ankara: Yetkin Yayinlar, 2004.

[16] Y. Uzunay, *"Dijital Delil Arastirma Sureci*", Available: http://slideplayer.biz.tr/slide/1918963/, Ankara, 2005.

[17] E. Casey, Digital Evidence and Comptuer Crime Scene, ABD: AP, 2004.

[18] Quick, D., & Choo, K.-K. R. (2016). *Big forensic data reduction: Digital forensic images and electronic evidence* (Vol. 19).

[19] Association of Chief Police Officers (ACPO) 2006. *Good practice guidelines for computer based evidence* v4.0. www.7safe.com/electronic_evidence

[20] Beebe N 2009. *Digital forensic research: The good, the bad and the unaddressed*, in Pollitt M & Shenoi S (eds), Advances in digital forensics: 17–36

[21] Bunting S & Wei W 2006. *EnCase computer forensics:* The official EnCE: EnCaseCertified examiner study guide. Indianapolis, IN: John Wiley & Sons

[22] Carrier B 2005. *File system forensic analysis*. Boston, NJ: Addison-Wesley

[23] Carvey H 2011. *Windows registry forensics: Advanced digital forensic analysis of the Windows registry*. Burlington, MA: Elsevier

[24] Casey E 2011. *Digital evidence and computer crime: Forensic science, computers, and the internet.* Burlington, MA: Elsevier

[25] Garfnkel S 2006. *Forensic feature extraction and cross-drive analysis*. Digital Investigation 3: 71–81

[26] Kenneally E & Brown C 2005. *Risk sensitive digital evidence collection*. Digital Investigation 2(2): 101–119

[27] McKemmish R 1999. *What is forensic computing? Trends & Issues in Crime and Criminal Justice* no. 118. Canberra: Australian Institute of Criminology. http://aic.gov.au/publications/current%20series/tandi/101-120/tandi118.html

[28] Schatz BL & Clark A 2006. *An open architecture for digital evidence integration*, in AusCERT Asia Pacific Information Technology Security Conference. Refereed R&D Stream. 21–26 May 2006. Gold Coast, Queensland

[29] Turner P 2005. *Unification of digital evidence from disparate sources (digital evidence bags*). Digital Investigation 2(3): 223–228

[30] National Institute of Justice (NIJ) 2004. *Forensic examination of digital evidence: A guide for law enforcement.* http://nij.gov/nij/pubs-sum/199408.htm

[31] National Institute of Justice (NIJ) 2008. *Electronic crime scene investigation: A guide for first responders,* 2nd Ed. http://www.nij.gov/pubssum/219941.htm

[32] Quarnby N & LJ Young 2010. *Managing intelligence—The art of influence*. Sydney: The Federation Press

[33] Quick D & Choo K 2014. *Google drive: Forensic analysis of data remnants*. J Network and Computer Applications 40: 179–193

[34] Quick D & Choo K 2013a. *Digital droplets: Microsoft SkyDrive forensic data remnants*. Future Generation Computer Systems 29(6): 1378–1394

[35] Quick D & Choo K 2013b. *Dropbox analysis: Data remnants on user machines*. Digital Investigation 10(1): 3–18

[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

[37] Quick D, Martini B & Choo K 2014. *Cloud storage forensics.* Waltham, MA: Syngress Publishing

[38] United Nations Office on Drugs and Crime (UNODC) 2011. *Criminal intelligence manual for analysts*. New York: UNODC

[39] Grier, J., Richard III, G.G.: *Rapid forensic acquisition of largemedia with sifting collectors*. Digit. Investig. 2015(14), S34–S44 (2015)

[40] Greiner, L.: *Sniper Forensics*. netWorker 13(4), 8–10 (2009)

BIBLIOGRAPHY

Quick, D., & Choo, K. K. R. (2016). Big forensic data reduction: digital forensic images and electronic evidence. *Cluster Computing*, *19*(2), 723–740. https://doi.org/10.1007/s10586-016-0553-1

Kigwana, I., Kebande, V. R., & Venter, H. S. (2017). A proposed digital forensic investigation framework for an eGovernment structure for Uganda. *2017 IST-Africa Week Conference, IST-Africa 2017*, 1–8. https://doi.org/10.23919/ISTAFRICA.2017.8102348

Reader, M. M. (2014). Forensic Focus – Articles DIGITAL FORENSICS ARTICLES AND RESEARCH PAPERS, (April), 1–6.

Murphy, C. (2014). Blackberry Forensics, (June).

Quick, D., & Raymond Choo, K.-K. (2014). Data reduction and data mining framework for digital forensic evidence: Storage, intelligence, review and archive. *Tre n Ds & Issues in Crime and Criminal Justice*, *480*(480), 1–11. Retrieved from http://www.aic.gov.au/media_library/publications/tandi_pdf/tandi480.pdf

Duce, D. A., Mitchell, F. R., & Turner, P. (2010). the Use of Artificial Intelligence in Digital Forensics : an Introduction. *Digital Evidence and Electronic Signature Law Review*, *7*, 35–41. Retrieved from http://sas-space.sas.ac.uk/5533/1/1922-2707-1-SM.pdf

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

Irons, A., & Lallie, H. (2014). Digital Forensics to Intelligent Forensics. *Future Internet*, *6*(3), 584–596. https://doi.org/10.3390/fi6030584

Quick, D., & Choo, K. R. (n.d.). *SPRINGER BRIEFS ON Big Digital Forensic Data Volume 1 : Data Reduction Framework and Selective Imaging* (Vol. 1).

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.

Analysis, F. S., & Analysis, H. (n.d.). File Signature Analysis and Hash Analysis, 1–52.

Naqvi, S. (n.d.). File Signature Analysis. Retrieved from http://www.garykessler.net/library/file_sigs.html

Rosenfeld, M. (2014). Analysis of Hashrate-Based Double Spending, 1–13. Retrieved from http://arxiv.org/abs/1402.2009

Mascarnes, S., Lopes, P., & Sakhare, P. (2016). Search model for searching the evidence in digital forensic analysis. *Proceedings of the 2015 International Conference on Green Computing and Internet of Things, ICGCIoT 2015*, 1353–1358. https://doi.org/10.1109/ICGCIoT.2015.7380677

Peterson, G. (2009). *Advances in Digital Forensics V* (Vol. 306). https://doi.org/10.1007/978-3-642-04155-6

Tiwari, R. K., Mesra, B. I. T., Cet, R. V. S., Sencar, H. T., Memon, N., Satrya, G. B., … Thi, T. T. P. (2016). Digital Forensic Investigation Tools and Procedures. *Computing*, *4*(4), 1–5. https://doi.org/10.1109/IWCI.2016.7860344

Board, E., Ferrari, D., & Gerla, M. (2009). *Lecture Notes of the Institute for Computer Sciences , Social Informatics and Telecommunications Engineering*. *Middle East*. https://doi.org/10.1007/978-3-642-27317-9_36

Mathews, C. (2016). Cloud Data Integrity using Password Based Digital Signatures, *7*(1), 101–103.

Information, V. (2013). vLive FOR408 Session Computer Forensic Investigations - Windows In- Depth.

Hashim, N., & Sutherland, I. (2011). An architecture for the forensic analysis of windows system artifacts. *Lecture Notes of the Institute for Computer Sciences, Social-Informatics and Telecommunications Engineering, LNICST*, *53*, 120–128. https://doi.org/10.1007/978-3-642-19513-6_10

Guide, F. R. (n.d.). Active @ File Recovery User Guide, 1–54.

Conlan, K., Baggili, I., & Breitinger, F. (2016). Anti-forensics: Furthering digital forensic science through a new extended, granular taxonomy. *Digital Investigation*, *18*(December 2015), S66–S75. https://doi.org/10.1016/j.diin.2016.04.006

Epifani, M., & Stirparo, P. (2015). *Learning iOS Forensics*. Retrieved from https://books.google.com/books?id=mUsZBwAAQBAJ&pgis=1

Winter, C., Steinebach, M., & Yannikos, Y. (2014). Fast indexing strategies for robust image hashes. *Digital Investigation*, *11*(SUPPL. 1), S27–S35. https://doi.org/10.1016/j.diin.2014.03.004

Management, T. I. M. E. W. I. S. E. T. (2016). The Rise of Macro Malware in Malaysia Common Loopholes in Mobile Applications, *41*.

Androulaki, E., & Karame, G. O. (2014). Hiding transaction amounts and balances in Bitcoin. *Lecture Notes in Computer Science (Including Subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*, *8564 LNCS*, 161–178. https://doi.org/10.1007/978-3-319-08593-7_11

Hoelz, B. W. P., Ralha, C. G., & Geeverghese, R. (2009). Artificial intelligence applied to computer forensics. *Proceedings of the 2009 ACM Symposium on Applied Computing - SAC '09*, (September), 883. https://doi.org/10.1145/1529282.1529471

Rajak, S., & Verma, A. (2012). Secure Data Storage in the Cloud using Digital Signature Mechanism, *1*(4), 489–493.

Liu, H., Zhang, P., & Liu, J. (2013). Public data integrity verification for secure cloud storage. *Journal of Networks*, *8*(2), 373–380. https://doi.org/10.4304/jnw.8.2.373-380

Breitinger, F., & Roussev, V. (2014). Automated evaluation of approximate matching algorithms on real data. *Digital Investigation*, *11*(SUPPL. 1), S10–S17. https://doi.org/10.1016/j.diin.2014.03.002

Windows, M. (2009). Microsoft Windows, 1–7.

Nuno Santos. (2015). Operating Systems Forensics, (1), 9–44. Retrieved from https://fenix.tecnico.ulisboa.pt/downloadFile/1126518382178975/csf-03-part2.pdf

Hoelz, B. W. P., Ralha, C. G., Geeverghese, R., & Junior, H. C. (2008). MADIK : A Collaborative Multi-agent ToolKit to Computer Forensics. *Computer*, 20–21.

EC-Council. (2010). *Computer Forensics Investigating Hard Disks, File & Operating Systems*. *Computer*.

Breitinger, F., Baier, H., & White, D. (2014). On the database lookup problem of approximate matching. *Digital Investigation*, *11*(SUPPL. 1), S1–S9. https://doi.org/10.1016/j.diin.2014.03.001

Johnson, J. (2017). Incident Trend Analysis for 2016 Cryptocurrencies 102 and the Dark side of the web Ransomware WannaCry Attack ! Are you at risk ?, *42*.

Caviglione, L., Wendzel, S., & Mazurczyk, W. (2017). The Future of Digital Forensics: Challenges and the Road Ahead. *IEEE Security Privacy*, *15*(6), 12–17. https://doi.org/10.1109/MSP.2017.4251117

SANS DFIR. (n.d.). You Can ' t Protect What You Don ' t Know About Windows Artifact Analysis : Evidence of ... *SANS Institute*, 2.

Bonneau, J., Narayanan, A., Miller, A., Clark, J., Kroll, J. A., & Felten, E. W. (2014). Mixcoin: Anonymity for bitcoin with accountable mixes. *Lecture Notes in Computer Science (Including Subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*, *8437*, 486–504. https://doi.org/10.1007/978-3-662-45472-5_31

ACPO. (2012). ACPO Good Practice Guide for Digital Evidence, (March), 41. Retrieved from http://www.digital-detective.net/digital-forensics-documents/ACPO_Good_Practice_Guide_for_Digital_Evidence_v5.pdf%0Ahttp://www.acpo.police.uk/documents/crime/2014/Revised Good Practice Guide for Digital Evidence_Vers 5_Oct 2011_Website.pdf

Bjelland, P. C., Franke, K., & Årnes, A. (2014). Practical use of Approximate Hash Based Matching in digital investigations. *Digital Investigation*, *11*(SUPPL. 1), S18–S26. https://doi.org/10.1016/j.diin.2014.03.003

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

Jain, A., & Chhabra, G. S. (2014). Anti-Forensics Techniques : An Analytical Review.

Wilson, D., & Ateniese, G. (2015). From pretty good to great: Enhancing PGP using bitcoin and the blockchain. *Lecture Notes in Computer Science (Including Subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*, *9408*, 368–375. https://doi.org/10.1007/978-3-319-25645-0_25