A PROCESS MODEL TO ENHANCE THE ACCURACY OF DIGITAL FORENSIC INVESTIGATION:

A CASE OF NIRA UGANDA

BY

ALEX MAKHETI

BU/GS18/MCF/9

.

A DISSERTATION SUBMITTED TO THE DIRECTORATE OF GRADUATE STUDIES, RESEARCH AND INNOVATION IN PARTIAL FULFILLMENT OF THE REQUIREMENTS FOR THE AWARD OF MASTER OF COMPUTER FORENSICS DEGREE OF BUSITEMA UNIVERSITY

MAY, 2022

DECLARATION

I **Makheti Alex**, declare that this research report is my original work, except where due acknowledgement has been made. I declare that this work has never been submitted to this University or to any other institution for funding/ for partial fulfillment for any award.

Signature : .... Date: ……………………….

Reg No: BU/GS18/MCF/9

APPROVAL

This research report submitted as a partial fulfillment for the award of Masters of Computer Forensics of Busitema University, with our approval as the academic supervisors.

1. Supervisor:

Prof. Ssemwogerere Twaibu (PhD)

Signature---

Date---

2. Supervisor:

Dr. Ocen Gilbert Gilibrays (PhD)

Signature --

Date---

2. Supervisor:

Mr. Alunyu Andrew Egwar

Signature --

Date---

DEDICATION

This research report is dedicated to my beloved family, my father Wafula Augustine, teacher retired and mother Wafula Wobule Teopista for continuously encouraging me to push forward, also my lovely wife Aguti Jane for physical and mental support, also to my children Makheti Annet, Makheti Caleb, Makheti Enock and Makheti Jeremy.My brother Sally Fred, my sisters Mayuba Sylivia, Khayanga Lydia,Kwaka Mary, Sikhoya Malita, Khwaka Zitah and Mukite Sarah. Special dedication to my friend and brother Ndaala Moses and Mataya Richard, dependable person that is there when there is need. And finally, brother Felix Nabusamu who has been so supporting and encouraging in every step of this Journey, in a special way, I wish to remember the support of the my supervisor and lecturer the late Bwire Felix (RIP) for the great support, Ladies and gentlemen, may the almighty God bless you.

ACKNOWLEDGEMENTS

The completion of this piece of work has been such a task that would have not been a success if handled by myself solely. In a special way, I would like to acknowledge the following;

I first of all thank the Lord Almighty, who gave me abundant health, strength, and courage to be able to complete this work. My sincere gratitude goes to my supervisors Prof. Semwogerere twaibu (PhD), Dr. Ocen Gilbert (PhD), Mr. Alunyu Andrew Eguar and the late Bwire Felix (RIP) whose commitment, patience and guidance, gave credence to this piece of work.

I would also like to appreciate all the staff of Busitema University for imparting in me various skills and knowledge during the course of my study.

I am highly indebted to my beloved wife Aguti Jane and my father Wafula Augustine, my Mother Wafula Wabule Teopista, My children, Makheti Jeremy, Makheti Enock, Makheti Caleb and Makheti Annet for their moral and material support. Not forgetting my beloved brothers and sisters also for their moral support.

In the same vein, my sincere appreciation goes to the staffs of NIRA for their participation and for giving me permission.

Finally, special thanks go to my friends, particularly, Mataya Richard of Abrah Shopping Centre and Nabusamu Filex and many others not mentioned, for their moral and material support where necessary.

May the almighty God reward them abundantly.

TABLE OF CONTENTS

LIST OF ABBREVIATIONS/ACRONYMS

API	: Application Programme Interface
CD-ROM	: Computer Device- Read only Memory
DFI	: Digital Forensic Investigation
FBI	: Federal Bureau of Investigations
FSFP	: Four Step Forensic Process
HRM	: Human Resource Management
NIRA	: National Identification and Registration Authority
SDAPM	: Standardised Data Acquisition Process Model
SOPs	: Standard Operating Procedures
UNBS	: Uganda National Bureau of Standards
UPDF	: Uganda People’s Defense Forces
USA	: United States of America

DEFINITION OF OPERATIONAL TERMS

Computer Forensics: Computer forensics is a branch of digital forensic science pertaining to evidence found in computers, Internet, Network, Databases and other digital storage media (Digital evidence and computer crime).

Digital Forensics: Digital forensics is a specific, predefined and accepted process applied to digitally stored data or digital media that use scientific proven and derived methods, based on a solid legal foundation, to produce after-the-fact digital evidence.

Framework: The term framework is used extensively in this study. In the literature, a number of other terms are often used, for instance architecture. Framework is defined as a structure for supporting, specifically a skeletal support used as the basis for something being constructed or a structure supporting something.

Investigation: The online dictionary gives the following definition for an investigation: The act or process of investigating. A second definition is a detailed inquiry or systematic examination An investigation is primarily defined as a careful search or examination in order to discover facts. In a digital forensic investigation, the facts that are discovered form part of the evidence presented in court.

Preservation: This is taking control of the evidence to avoid any alterations that can cause change to the evidence

Process model: are processes of the same nature that are classified together into a model. Thus, a process model is a description of a process at the type level. One possible use of a process model is to prescribe how things must/should/could be done in contrast to the process itself which is really what happens

Process: a process is the instance of a computer program that is being executed by one or many threads. It contains the program code and its activity. Depending on the operating system (OS), a process may be made up of multiple threads of execution that execute instructions concurrently. However, process has a number of meanings which are all considered important, but for purposes of this research, most of the meanings have been considered and regardless of the underlying operations performed, the process must enable effective data extraction to aid in further investigation.

LIST OF TABLES

LIST OF FIGURES

ABSTRACT

The study sought to assess process models and their role in enhancing the accuracy of digital forensic investigation in NIRA-Uganda. The specific objectives were; to examine the process of digital investigation at NIRA-Uganda, acquiring evidence, establish how authentication of evidence has enhanced the accuracy of digital forensic investigations conducted and to determine the strength and weaknesses of exiting models assess evidence analysis process and how it has enhanced the accuracy of digital forensic investigations conducted by NIRA-Uganda. To determine the requirements for developing a process model and to develop and validate a process model for the said purpose. The study used a descriptive research design. The descriptive research design was used to obtain information concerning the status of the process model and also describe what exists with respect to the situations on the ground concerning how it enhances digital forensic investigation. A total of 125 respondents participated in the study out of the earmarked 150, which gave the rate of 83.3%.

The study found out that digital forensic investigations are carried out in a systematic way by following procedures set forth. This is through observance of all protocols, deployment of the right tools, allowing the experts to carry out their investigations and corroborate the evidence by logically putting together the pieces seized from computers and storage devices like CD-ROMS, Flash Disks among others while at the same time studying the psychological state of the person under investigation. In addition, the current system was found to be having strength which happen to be aiding digital forensic investigations and also weaknesses which have significantly affected the accuracy of digital forensic investigations. The study found out that the requirements for developing a model need utmost attention in order to make an informed decision on the best software and the possibility of having one which can be a game changer. Finally, The model for determining the adoptability of digital forensics in organization is a web based application designed using the latest web technologies. The system was evaluated and validated which confirmed that it can perform the intended functions. The multiple correlation analysis indicated that the relationship between the process model used and the accuracy of digital forensic investigations is at (r) = .368**, p<.01). Multiple regression analysis indicated that up to r^2 = 0.249 (24.9%), was accounted for by the independent variables included in the study. This prediction is significant as envisaged in the way evidence is acquired, authenticated and analyzed have all combined to determine the accuracy of digital forensic investigations. As per the results, carrying out digital forensic investigation process enhances the accuracy of digital forensic investigations.

In conclusion, digital forensic investigation is a systematic process which NIRA happens to be following and drawing on the strengths and weaknesses highlighted in the study, a lot needs to be improved for NIRA to accurately carry out digital forensic investigations The study recommends that government needs to get involved in the fight against cyber-crime, increase NIRA’s funding and other agencies to step up investigations, build the capacity of staff in NIRA and police forensic department, government needs to set up a digital forensic laboratory to help in electronic evidence analysis. Finally, the researcher recommended that SOPs from Scientific Working Group on Digital Evidence (SWGDE) are accepted as guidelines in electronic evidence management for admissibility purposes since they cover both the crime scene and the Forensic laboratory as well.

CHAPTER ONE: INTRODUCTION

1.0 Introduction

The field of digital forensics has become common place due to the increasing prevalence of technology since the late 20th century, and the inevitable relevance of this technology in the conducting of criminal activity (Kendra, 2019). In traditional forensics, the evidence is generally something tangible that could identify the criminal, such as hair, blood or fingerprints. In contrast, digital forensics deals with files and data in digital form extracted from digital devices like computer, phones among other digital devices, meaning is derived from the fact that a computer or computerized device is the subject or object of crime. Digital forensics is a widely-used term, referring to the identification, acquisition and analysis of digital evidence originating from much more than just computers, such as smartphones, tablets, Internet of Things Devices, or data stored in the cloud, then preservation and presentation of the same in the courts of law as evidence.

With increased use of technology in organizations and rapid changes in technology, cyber forensic process is also advancing into new ways. In this context, NIRA, Uganda also needs to align their technological infrastructure to meet the challenges in conducting successful process of forensic investigations to attain maximum and desired benefits of it. NIRA is an authority in Uganda that houses the national bio-metric database, maintaining various updated registers of Uganda in its safe custody, these registers include, the national identification register, birth register, death register and adoption orders register, this is sensitive information that may attract cyber criminals from the external locations of the organization or internal by insiders who may want to advance their illegitimate intentions.

The primary objective of this study is to develop a process model to enhance the accuracy of digital investigation, a case of NIRA Uganda which houses the national database of bio-metrics that can act as unique identifiers in any given investigation process. Therefore, this chapter presents, the background of the study, statement of the problem, research objectives, research questions, justification of the study, significance of the study, scope of the study, the conceptual framework and definition of key terms.

1.1 Background of the study

New developments in the digital world challenge law enforcement, legal and judicial professionals to maintain current proficiencies concerning legal issues and technical aspects in the rapidly changing environment (Taveras, 2018)). The boundaries of forensic science are

REFERENCES

Adam, I., Imafidon, C. and Preston, D. (2011) ‘A new approach of digital forensic model for digital forensic investigation’, International Journal of Advanced Computer Science and Applications, Vol. 2, No. 12, pp.175–178.

Adams, R. (2019). “The emergence of cloud storage and the need for a new digital forensic process model” (PDF). Murdoch University.

Adams, R., Hobbs, V. and Mann, G. (2014) ‘The advanced data acquisition model (ADAM): a process model for digital forensic practice’, Journal of Digital Forensics, Security and Law, Vol. 8, No. 4, pp.25–48.

Africa cyber security report. (2018). *A skills gap is the difference between skills that employers want or need, And skills their workforce offer*. Kenya, Nairobi

Ballou, S. (Ed.). (2010). Electronic crime scene investigation: A guide for first responders. Diane Publishing.

Baryamureeba, V.,& Tushabe, F. (2015):The Enhanced Digital Investigation Process Model.Makere University Institute of Computer Science, Uganda 2004.

Beebe, N. and Clark, J. (2015) ‘A hierarchical, objectives-based framework for the digital investigations process’, Digital Investigation, Vol. 2, No. 2, pp.147–167.

Brown, C. (2019) Computer Evidence: Collection and Preservation, 2nd ed., Course Technology, Boston.

Bulbul, H., Yavuzcan, H. and Ozel, M (2018) ‘Digital forensics: an analytical crime scene procedure model (ACSPM)’, Forensic Science International, Vol. 233, No. 1, pp.244–256.

Caelli, W. J., & Liu, V. (2018). Cyber security education at formal university level: An Australian perspective. In Journal for the Colloquium for Information Systems Security Education. 5(2): 26-44.

Carlton, H. and Worthley, R. (2019) ‘An evaluation of agreement and conflict among computer forensic experts’, 42nd Hawaii International Conference on System Sciences (HICSS), IEEE, Hawaii, 5–8 January.

Carrier, B. & Winter (2020). Defining Digital Forensic examination and analysis Tools Using Abstraction layers. International Journal of Digital Evidence.

Carrier, B., & Spafford, E. H. (2017). Getting physical with the digital investigation process. International Journal of digital evidence, 2(2), 1-20.

Casey, E. (2019). Digital evidence and computer crime: Forensic science, computers, and the internet. Academic press.

Casey, E., & Turnbull, B. (2014). Digital evidence on mobile devices. Forensic Science, Computers, and the Internet, Third Edition. Academic Press.

Checkland, P., & Poulter, J. (2016). Learning for Action: A Short Definitive Account of Soft Systems Methodology and its Use for Practitioners, Teachers and Students. Chichester: John Wiley.

Cohen, F. (2017) 'Putting the science in digital forensics', Journal of Digital Forensics, Security and Law, Vol. 6, No. 1, pp.7–14.

Cohen, F. (2019) Digital Forensic Evidence Examination, 2nd ed., Fred Cohen & Associates, California.

Cole, G. F., Smith, C. E., & DeJong, C. (2018). The American system of criminal justice. Cengage Learning.

Cooper, D.T., & Schindler, P.S. (2011). Business Research Methods. Mumbai: Tata.

Davis, K. (2018). The Criminal Investigation Process - Volume 1: Summary and Policy Implications. Santa Monica, California: Rand.

Fraser, J. (2017). Making Domestic Violence a Crime: Situating the Criminal Justice Response in Canada. In Global Responses to Domestic Violence (pp. 41-59). Springer, Cham.

Hope, K. R. (2018). The police corruption "crime problem" in Kenya. Security Journal, 1-17.

Hossain, M., Hasan, R., & Skjellum, A. (2017). Securing the internet of things: a meta-study of challenges, and open problems. In 2017 IEEE 37th International Conference on Distributed Computing Systems Workshops (ICDCSW) (pp. 220-225). IEEE.

Howard Jr, J. W. (2019). Courts of appeals in the federal judicial system: A study of the second, fifth, and District of Columbia circuits. Princeton University Press.

Jones, A. (2016). Keynote speech. In: First International Conference on Forensic at Oxford.

Jones, R. (2016b) Safer Live Forensic Acquisition. University of Kent at Canterbury. Available from: http://www.cs.kent.ac.uk/pubs/ug/2007/co620-projects/forensic/report.pdf.

Kendra, M, (2019) 'Internet forensics: legal and technical issues', 2nd International Workshop on Digital Forensics and Incident Analysis, Samos, Greece, pp.3–12.

Kessler, C. (2020) Judges' Awareness, Understanding, and Application of Digital Evidence, PhD thesis, Nova Southeastern University.

Kim, D., & Solomon, M. G. (2016). Fundamentals of information systems security. Jones & Bartlett Publishers.

Kohn, M., Eloff, M. and Eloff, J. (2013) 'Integrated digital forensic process model', Computers and Security, Vol. 38, pp.103–115.

Kruse and Heiser, (2001), Process model: Evolution of Computer Forensic Best Practices: An Update on Programs and Publications. Journal of Digital Forensic Practice 20016; 1:3-11.

Kruse, W. and Heiser, J. (2016) Computer forensics: Incident Response Essentials, Addison Wesley, Boston, USA. 248

Lubaale, E. C. (2015) & Bokolo, V. S. (2014): The practicality of challenging DNA evidence in court. South African Crime Quarterly, 52(1), 39-47.

Montasari, R., Peltola, P. and Evans, D. (2015) 'Integrated computer forensics investigation process model (ICFIPM) for computer crime investigations', Proceedings of 10th International Conference on Global Security, Safety and Sustainability, pp.83–95.

Moreau, D. M. (2013) "Fundamental Principles and Theory of Crime Scene Photography" Quantico: Forensic Science Training Unit, FBI Academy.

Moturi, C. A. (2011). Digital forensics framework for Kenyan courts of laws (Doctoral dissertation, University of Nairobi).

Oriwoh, E., & Williams, G. (2015). Internet of Things: The argument for smart forensics. In Handbook of research on digital crime, cyberspace security, and information assurance (pp. 407-423). IGI Global.

Palmer, G. (2011). A Road Map for Digital Forensic Research: Report from the First Digital Forensic Workshop, 7—8 August 2001. DFRWS Technical Report DTR-TOO]-O]

Quick, D., & Choo, K. K. R. (2014). Data reduction and data mining framework for digital forensic evidence: storage, intelligence, review and archive.

Robertson, B., Vignaux, G. A., & Berger, C. E. (2016). Interpreting evidence: evaluating forensic science in the courtroom.

Rogers, M. (2013) DCSA: A Practical Approach to Digital Crime Scene Analysis, 5th ed., Vol. 3, West Lafayette, Purdue University, USA.

Saini, H., Rao, Y. S., & Panda, T. C. (2017). Cyber-crimes and their impacts: A review. International Journal of Engineering Research and Applications, 2(2), 202-209.

Smith, R., & Shuy, G. (2012) Cyber Criminals on Trial, Cambridge University Press, Cambridge.

Soltani, S., & Seno, S. A. H. (2017). A survey on digital evidence collection and analysis. In Computer and Knowledge Engineering (ICCKE), 2017 7th International Conference on (pp. 247-253). IEEE.

Stanfield, A. (2019) Computer Forensics, Electronic Discovery and Electronic Evidence, LexisNexis Butterworths, Chatswood.

Tajuddin, T. B., & Manaf, A. A (2015). Forensic investigation and analysis on digital evidence discovery throough physical acquisition on smart phone. In Internet Security (WorldCIS), 2015 World Congress on, pp.132-138. IEEE, 2015.

Taveras, P. (2018). SCADA live forensics: real time data acquisition process to detect, prevent or evaluate critical situations. European Scientific Journal, ESJ, 9(21).

Taylor, R. W., Fritsch, E. J., & Liederbach, J. (2019). Digital crime and digital terrorism. Prentice Hall Press.

Throup, D. (2017). Crime, politics and the police in colonial Kenya, 1939–63. In Policing and decolonisation. Manchester University Press.

Valjarevic, A. and Venter, H. (2015) 'A comprehensive and harmonized digital forensic investigation process model', Journal of Forensic Sciences, Vol. 60, No. 6, pp.1467–1483.

Venter, J. (2015b) Process Flow for Cyber Forensics Training and Operations [online] http://researchspace.csir.co.za/dspace/handle/10204/1073 (accessed 29 June 2015).

Wilding, E. (2017). Information risk and security: preventing and investigating workplace computer crime. Routledge.

Perez, S. (2013), Police and the probability of arrest. Social Forces, 81, 1381−1397.

Kalindi, M. (2017), The effectiveness of police crime intelligence in addressing Cyber Crimes. A case study of Uganda Police, Ministry of Internal Affairs, Kampala-Uganda.