A FRAMEWORK FOR CYBERCRIME DIGITAL EVIDENCE ACQUISITION

OPOLOT FRANCIS

REG NO: BU/GS20/MCF/6

Student No. 2000402125

A RESEARCH REPORT SUBMITTED TO THE DIRECTORATE OF GRADUATE STUDIES, RESEARCH AND INNOVATIONS IN PARTIAL FULFILLMENT OF THE REQUIREMENTS FOR THE AWARD OF A MASTER'S DEGREE IN COMPUTER FORENSICS OF BUSITEMA UNIVERSITY

February, 2024

DECLARATION

I, OPOLOT FRANCIS, 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 any other university or institution of higher learning for any award.

Name: OPOLOT FRANCIS

Registration Number: BU/GS20/MCF/6

Signature: Francis

Date 28th/01/2024

SUPERVISORS APPROVAL

This research report titled "*A Framework for Cybercrime Digital Evidence Acquisition*" is submitted for examination with the approval of the following academic supervisor(s);

Signature: Date:.21/01/2024

Dr. Owomugisha Godliver (PhD)
Department of Computer Engineering
Faculty of Engineering

Signature: ……………… Date. January 27th 2024

Dr. Alunyu Andrew Egwar (PhD)
Department of Computer Engineering
Faculty of Engineering

DEDICATION

I dedicate this research to my Lord and Savior, Jesus, to whom I have walked and triumphed through all seasons, and to my parents, Mrs. Akol Hellen and Mr. Osauro John, for their unwavering support and belief in me. I also dedicate this with much affection. And to my devoted wife Wanjala Nafula Teresa and siblings, who put up with their hectic schedules and missed me while I was conducting the study: not forgetting my friend ASP Wehire Lamech, your unwavering love, support, and encouragement served as a soft foundation for me in the midst of trying challenging circumstances. You are the reason this research has such strong foundations; I am incredibly grateful and will always be beholden to you.

ACKNOWLEDGEMENT

I will never grow exhausted from thanking the all-powerful God who gave me insight, discernment, and a persistent attitude in pursuing this endeavour. I certainly am nothing, Jesus, without you.

My profound appreciation goes out to my superiors, Dr. Owomugisha Godliver and Dr. Alunyu Andrew Egwar, for their unwavering support and guidance. Without them, I would not have been able to compose this.

Many thanks to Dr. Odongtoo Godfrey, Dr. Matovu Davis and professor Ocen Gilbrays, who were all important contributors to maintaining the focus and concentration necessary to complete the procedure.

To my beloved classmates and pals, Mr. Wehire Lamech, Moses, Max, Kisakye and everyone else who has supported me, even though I haven't included you all here? Thank you, and may you be incredibly blessed by the Good Lord who sees our hearts.

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

ABBREVIATIONS

ICT:	Information communication technology
CVs:	Commercial Victimization Survey
NCSI:	Network Connectivity Status Indicator
SMBs:	Small and Medium Size Businesses
GPS:	Global Positioning System
CD/CDR:	Compact Disc / Compact Disc Recordable
DSRM:	Design Science Research Methodology
DSRP:	Design Science Research Process
BCFL:	Block Chain Cloud Forensic Logging
DLT:	Distributed Ledger Technology
GDPR:	General Data Protection Regulation
IaaS:	Infrastructure as a Service
PaaS:	Platform as a Service
SaaS:	Software as a Service
ADAM:	Advanced Data Acquisition Model
UML:	Unified Modeling Language
FTK:	Forensic Toolkit
FAT32:	File Allocation Table32
NTFS:	New Technology File System
ISO:	International Organization for Standardization
CRT:	Telnet Client and Terminal Emulator
VPN:	Virtual Private Network
NITA:	National Information Technology Uganda
URA:	Uganda Revenue Authority
SPSS:	Statistical Package for Social Sciences
RAM:	Random Access Memory
DGAL:	Directorate of Government Analytical Lab

ABSTRACT

Over the years, the field of digital forensics has grown significantly, and courts have seen an increase in cases pertaining to it. In today's technologically advanced culture, the prevalence of computer/cyber-connected criminal attacks has increased the demand for digital evidence in court. It is vital to successfully prosecute those who commit such crimes and hold them accountable. Digital forensics is the procedure used to obtain the evidence presented in these court cases.

The main aim of the research was to design a framework for cybercrime digital evidence acquisition that would be adopted for use during the digital crime evidence acquisition process with the following specific objectives, i) to establish requirements for the framework adopted by private organizations and law enforcement agencies for Uganda in cybercrime evidence acquisition; ii) to develop a framework that adopts the use of digital evidence acquisition processes by computer forensics practitioners in Uganda; and iii) to evaluate the performance of the framework that adopts the use of digital evidence acquisition processes by computer forensics practitioners in Uganda. Research results from the survey indicate that there is a need to establish requirements for the framework adopted by private organizations and law enforcement agencies in Uganda, and the results of the entire framework were tested and evaluated by the simulation using data and tools like Autopsy and FTK Imager.

It was concluded that achieving proficiency in digital forensics involves a holistic understanding of evidence encounters, effective handling, and adept presentation for it to be admissible to courts of law. The dynamic nature of the field necessitates adaptability to emerging tools, techniques, and best practices. Also, continuous professional development and collaboration with legal experts are crucial for maintaining high standards in digital evidence analysis and its admissibility to the court.

CHAPTER ONE: INTRODUCTION

1.0 Background of the study

Information and communication technology (ICT) is a broad word that encompasses all advanced computer-based technologies for managing and transferring information, according to [1]. ICT is a broad term that encompasses all forms of communication, such as videoconferencing and distance learning, as well as the associated services and technologies, such as radio, television, cellular phones, computer and network hardware, and satellite systems. This increased reliance on and usage of ICT opens up new opportunities for criminals and other bad actors to target ICT and or use it to perpetrate crimes.

Technology improvements are causing firms to swiftly evolve regardless of industry vertical. Industry 4.0 refers to this stage. With Industry 4.0, businesses are attempting to use information technology to boost production and profitability [3]. Companies are now required to display their presence on social media due to the rise in its use [2]. This has improved efficiency and streamlined operations but has also broadened the attack surface. An organization's vulnerability to outside attacks due to advances in information technology and an increase in computer-related crimes has given rise to new types of digital evidence known as an attack surface. Given the damage, various reforms are urgently required, and delayed adoption is preferred.

Digital forensics is crucial for incident response and compliance audits in a business setting. The investigators establish the security criteria rather than employing them directly [4]. The responsibility of a good business suggests assembling verifiable proof and defining the perimeters of a scene's security. Computer crime scenes can be controlled and serve as secondary sources of evidence [1]. Thanks to a fingerprint scan of the keyboards, the accessories offer palpable evidence. The study applies to crime scenes that unintentionally or intentionally change their environment. Consider, for instance, that you are a digital investigator for a local police force. One of the nearby schools is the target of a bomb threat that your department manager gets via anonymous email. In [5] since the anonymous email was sent from a home in the school's area, you are instructed to conduct the investigation with the help of information from a subpoena about the last known ISP where the message originated. To ensure the preservation of computer evidence when the warrant is executed, investigators create a list of components that must be included in an initial-reaction field kit in response to the victim.

REFERENCES

[1] Aralu, U. O. (2015). Influence of information and communication technology on digital divide. Global Journal of Computer Science and Technology.

[2] Appel, G., Grewal, L., Hadi, R., & Stephen, A. T. (2020). The future of social media in marketing. Journal of the Academy of Marketing science.

[3] Psarommatis, F., Sousa, J., Mendonça, J. P., & Kiritsis, D. (2022). Zero-defect manufacturing the approach for higher manufacturing sustainability in the era of industry 4.0: a position paper. International Journal of Production Research.

[4] Archibald, M. M., Ambagtsheer, R. C., Casey, M. G., & Lawless, M. (2019). Using zoom videoconferencing for qualitative data collection: perceptions and experiences of researchers and participants. International journal of qualitative methods.

[5] Luu, J., & Imwinkelried, E. J. (2016). The challenge of Bitcoin pseudo-anonymity to computer forensics. Criminal Law Bulletin.

[6] Kalhoro, S., Rehman, M., Ponnusamy, V., & Shaikh, F. B. (2021). Extracting key factors of cyber hygiene behaviour among software engineers: A systematic literature review.

[7] Reinhard, S. C., Feinberg, L. F., Houser, A., Choula, R., & Evans, M. (2019). Valuing the invaluable 2019 update: Charting a path forward. AARP Public Policy Institute.

[8] Gless, S. (2019). AI in the Courtroom: a comparative analysis of machine evidence in criminal trials.

[9] Wolfgang, M. E. (2016). Patterns in criminal homicide. University of Pennsylvania Press.

[10] Alenezi, A., Atlam, H., Alsagri, R., Alassafi, M., & Wills, G. (2019, May). IoT forensics: A state-of-the-art review, callenges and future directions. In Proceedings of the 4th International Conference on Complexity, Future Information Systems and Risk.

[11] Gilmour, P. M. (2021). Exploring the barriers to policing financial crime in England and Wales. Policing: A Journal of Policy and Practice.

[12] Jarrett, A., & Choo, K. K. R. (2021). The impact of automation and artificial intelligence on digital forensics. Wiley Interdisciplinary Reviews: Forensic Science.

[13] Khan, S., Gani, A., Wahab, A. W. A., Shiraz, M., & Ahmad, I. (2016). Network forensics: Review, taxonomy, and open challenges. Journal of Network and Computer Applications.

[14] Nweze-Iloekwe, N. (2022). The Legal and Regulatory Aspect of International Cybercrime and Cybersecurity: Limits and Challenges.

[15] Alahmari, A., & Duncan, B. (2020, June). Cybersecurity risk management in small and medium-sized enterprises: A systematic review of recent evidence. In 2020 international conference on cyber situational awareness, data analytics and assessment.

[16] Dobbie, W., Goldin, J., & Yang, C. S. (2018). The effects of pre-trial detention on conviction, future crime, and employment: Evidence from randomly assigned judges. American Economic Review.

[17] Odinot, G., Verhoeven, M. A., Pool, R. L. D., & de Poot, C. J. (2017). Organised cybercrime in the Netherlands.

[18] AKYEŞİLMEN, N. (2022). Türkiye in the Global Cybersecurity Arena: Strategies in Theory and Practice. Insight Turkey/Summer 2022: Embracing Emerging Technologies.

[19] Dai, M., Xia, Y., & Han, R. (2022). Temporal variations in calls for police service during COVID-19: Evidence from China. Crime & Delinquency.

[20] Kemp, S., Buil-Gil, D., Miró-Llinares, F., & Lord, N. (2021). When do businesses report cybercrime? Findings from a UK study. Criminology & Criminal Justice.

[21] Katterbauer, K., Hassan, S. Y. E. D., & Cleenewerck, L. (2022). Financial cybercrime in the Islamic Finance Metaverse. Journal of Metaverse.

[22] Connolly, L. Y., Lang, M., Taylor, P., & Corner, P. J. (2021). The evolving threat of ransomware: From extortion to blackmail.

[23] Perenc, L. (2022). Psychopathic personality disorder and cyber-criminalty: an outline of the issue. Current Issues in Personality Psychology.

[24] Kling, D., Phillips, C., Kennett, D., & Tillmar, A. (2021). Investigative genetic genealogy: Current methods, knowledge and practice. Forensic Science International.

[25] Bhandari, S. (2022). Research and implementation of timeline analysis method for digital forensics evidence (Doctoral dissertation, Kauno technologyes universitates).

[26] Boguszewicz, C., Boguszewicz, M., Iqbal, Z., Khan, S., Gaba, G. S., Suresh, A., & Pervaiz, B. (2021). The fourth industrial revolution-cyberspace mental wellbeing: Harnessing science & technology for humanity. Global foundation for cyber studies and research.

[27] Stainton, I., & Ewin, R. (2022). Criminal investigation. Critical Publishing.

[28] Saadat, S., Pandya, H., Dey, A., & Rawtani, D. (2022). Food forensics: Techniques for authenticity determination of food products. Forensic Science International.

[29] Reedy, P. (2020). Interpol review of digital evidence 2016-2019. Forensic Science International.

[30] Nafuye, I. (2019). A process model and matrix for acquisition of admissible live digital evidence (ALDEM) (Doctoral dissertation, Busitema University).

[31] Stoykova, R., & Franke, K. (2020, May). Standard representation for digital forensic processing. In 2020 13th International Conference on Systematic Approaches to Digital Forensic Engineering.

[32] Raj, K. (2020). E-Evidence: Moving Parallel with Today's World. Issue 4 Int'l JL Mgmt. & Human.

[33] Smith, T. G. (2017). Subjectivity. In Politicizing Digital Space. London: University of Westminster Press.

[34] Tully, G., Cohen, N., Compton, D., Davies, G., Isbell, R., & Watson, T. (2020). Quality standards for digital forensics: Learning from experience in England & Wales. Forensic science international.

[35] Colgan, B. A. (2018). The Excessive Fines Clause: Challenging the Modern Debtors' Prison.

[36] Stoykova, R. (2021). Digital evidence: Unaddressed threats to fairness and the presumption of innocence. Computer Law & Security Review.

[37] Haber, L., & Haber, R. N. (2008). Scientific validation of fingerprint evidence under Daubert. Law, Probability and Risk.

[38] Dweikat, M., Eleyan, D., & Eleyan, A. (2020). Digital Forensic Tools Used in Analyzing Cybercrime. Journal of University of Shanghai for Science and Technology.

[39] Bananuka, J., Tumwebaze, Z., & Orobia, L. (2019). The adoption of integrated reporting: a developing country perspective. Journal of Financial Reporting and Accounting.

[40] Anaya, K. L., & Pollitt, M. G. (2022). A social cost benefit analysis for the procurement of reactive power: The case of Power Potential. Applied Energy.

[41] Awuson-David, K., Al-Hadhrami, T., Alazab, M., Shah, N., & Shalaginov, A. (2021). BCFL logging: An approach to acquire and preserve admissible digital forensics evidence in cloud ecosystem. Future Generation Computer Systems.

[42] Barrett, D. (2020). Cloud Based Evidence Acquisitions in Digital Forensic Education. Information Systems Education Journal.

[43] Abbas, T. M. J., & Abdulmajeed, A. S. (2021). Identifying Digital Forensic Frameworks Based on Processes Models. Iraqi Journal of Science.

[44] Casey, A., & MacPhail, A. (2018). Adopting a models-based approach to teaching physical education. Physical Education and Sport Pedagogy.

[45] Kebande, V. R., & Venter, H. S. (2018). Novel digital forensic readiness technique in the cloud environment. Australian Journal of Forensic Sciences.

[46] Montasari, R. (2021). The comprehensive digital forensic investigation process model (CDFIPM) for digital forensic practice. University of Derby (United Kingdom).

[47] Zia, T., Liu, P., & Han, W. (2017, August). Application-specific digital forensics investigative model in internet of things (iot). In Proceedings of the 12th International Conference on Availability, Reliability and Security.

[48] Göbel, T., Türr, J., & Baier, H. (2019, August). Revisiting data hiding techniques for apple file system. In Proceedings of the 14th International Conference on Availability, Reliability and Security.

[49] Hosgor, E. C. (2020). Detection and Mitigation of Anti-Forensics. International Journal of Computer Science and Information Security.

[50] Alloghani, M., Alani, M. M., Al-Jumeily, D., Baker, T., Mustafina, J., Hussain, A., & Aljaaf, A. J. (2019). A systematic review on the status and progress of homomorphic encryption technologies. Journal of Information Security and Applications.

[51] Amato, F., Castiglione, A., Cozzolino, G., & Narducci, F. (2020). A semantic-based methodology for digital forensics analysis. Journal of Parallel and Distributed Computing.

[52] Chanuan Uakarn, Kajohnsak Chaokromthong, & Nittaya Sintao. (2021). Sample Size Estimation using Yamane and Cochran and Krejcie and Morgan and Green Formulas and Cohen Statistical Power Analysis by G*Power and Comparisions. APHEIT International Journal , 10(2), 76–86. https://so04.tci-thaijo.org/index.php/ATI/article/view/254253

[53] D. Peacock and A. Irons, "Gender Inequality in Cybersecurity: Exploring the Gender Gap in Opportunities and Progression," *International Journal of Gender, Science and Technology,* vol. 9, no. 1, pp. 25–44, May 2017, Available: https://genderandset.open.ac.uk/index.php/genderandset/article/view/449

[54] Zhang, Z., F. Werner, H.-M. Cho, G. Wind, S.E. Platnick, A.S. Ackerman, L. Di Girolamo, A. Marshak, and K. Meyer, 2017: A framework for quantifying the impacts of sub-pixel reflectance variance and covariance on cloud optical thickness and effective radius retrievals based on the bi-spectral method. In *Radiation Processes in the Atmosphere and Ocean (IRS2016): Proceedings of the International Radiation Symposium (IRC/IAMAS), 16-22 April 2016, Auckland, New Zealand,* AIP Conference Proceedings, vol. 1810, pp. 030002, doi:10.1063/1.4975502

[55] A. Leppänen and T. Kankaanranta, "Cybercrime investigation in Finland," *Journal of Scandinavian Studies in Criminology and Crime Prevention*, vol. 18, no. 2, pp. 157–175, Jul. 2017, doi: https://doi.org/10.1080/14043858.2017.1385231.

[56] Marryville university, "Cyber Crime Investigation: Making a Safer Internet Space," *Maryville Online*, Sep. 08, 2021. https://online.maryville.edu/blog/cyber-crime-investigation/

[57] O. AY, "Digital Forensics Investigation Jurisprudence: Issues Of Admissibility Of Digital Evidence," *Journal of Forensic, Legal & Investigative Sciences*, vol. 6, no. 1, pp. 1–8, Jul. 2020, doi: https://doi.org/10.24966/flis-733x/100045.

[58] A. Kasper and Eneli Laurits, "Challenges in Collecting Digital Evidence: A Legal Perspective," *Springer eBooks*, pp. 195–233, Jan. 2016, doi: https://doi.org/10.1007/978-3-319-26896-5_10.

[59] A. Antwi-Boasiako and H. Venter, “A Model for Digital Evidence Admissibility Assessment,” *Advances in Digital Forensics XIII*, pp. 23–38, 2017, doi: https://doi.org/10.1007/978-3-319-67208-3_2.

[60] A. Yeboah-Ofori, E. Yeboah-Boateng, and H. Gustav Yankson, “Relativism Digital Forensics Investigations Model: A Case for the Emerging Economies,” *2019 International Conference on Cyber Security and Internet of Things (ICSIoT)*, May 2019, doi: https://doi.org/10.1109/icsiot47925.2019.00023.

[61] A. F. Moussa, “Electronic evidence and its authenticity in forensic evidence,” *Egyptian Journal of Forensic Sciences*, vol. 11, no. 1, Aug. 2021, doi: https://doi.org/10.1186/s41935-021-00234-6.

[62] S. Saleem, “Protecting the Integrity of Digital Evidence and Basic Human Rights During the Process of Digital Forensics,” 2015.

[63] Reja, U., Manfreda, K. L., Hlebec, V., & Vehovar, V. (2003). Open-ended vs. close-ended questions in Web questionnaires. Metodoloski zvezki, 19, 159-177.

[64] Holland, J. L., & Christian, L. M. (2009). The influence of topic interest and interactive probing on responses to open-ended questions in web surveys Social Science Computer Review, 27(2), 196-212

[65] Amin, M.E. (2005) Social Science Research: Conception Methodology and Analysis. Makerere University Printeryafd, Kampala.

[66] https://aag-it.com/the-latest-cyber-crime-statistics

[67] https://casetext.com/case/american-express-trav-v-n-atlantic-res