



**BUSITEMA
UNIVERSITY**
Pursuing Excellence

FACULTY OF ENGINEERING
DEPARTMENT OF COMPUTER ENGINEERING

A Process Model and Matrix for Acquisition of Admissible Live Digital
Evidence (ALDEM): Case of Uganda

By

Nafuye Ivan
BU/GS16/MCF/007



A Dissertation Submitted to the Directorate of Graduate Studies, Research &
Innovation for the Degree of Masters of Computer Forensics of
Busitema University

September 2019

Declaration

I Nafuye Ivan declare that this dissertation is my original work except in instances where references have been made, and acknowledgement of any other assistance received during its preparation. It has not been published or submitted for any degree award of Busitema or any other university or institution of higher learning that am aware of. It has been prepared as a partial requirement for the award of a degree of Masters of Computer Forensics of Busitema University.

Signature: 

Date:.....10/09/2019.....

Name: Nafuye Ivan

BU/GS16/MCF/7

Faculty of Engineering

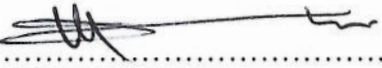
Department of Computer Engineering

Busitema University



Approval

This research dissertation titled “A Process Model & Matrix for Acquisition of Admissible Live Digital Evidence: Case of Uganda (ALDEM)” has been submitted for examination with the permission and approval of my University Supervisors.

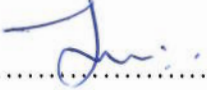
Signature: 

Date: 11/09/2019

Dr Semwogerere Twaibu

Deputy Dean & Senior Lecturer, Department of Computer Engineering

Busitema University

Signature: 

Date: 11th / Sept / 2019

Mr. Ocen Gilibrays Gilbert

Lecturer, Department of Computer Engineering

Busitema University

Dedication

I dedicate this research to my lord Christ Jesus with whom have walked and overcome all seasons, my beloved parents Mr. Nafuye Davis and Mrs. Nafuye Mary for always supporting and believing in me. With great love I also dedicate this work to my loving wife Kyomuhendo Dorcus and son Vinson Kusime who endured with the busy schedules and missed me while was carrying out the study. All your encouragements, support and unconditional love was soft ground for landing during difficult and testing times. All strong pillars in this research are because of you, thank you so much and am forever indebted.

Acknowledgments

I would not get tired thanking the almighty God who has given me knowledge and wisdom and a spirit of persistence in carrying out this project. Surely am nothing worthy without you Jesus

I would like to express my sincerest and heartfelt gratitude to my supervisors, Dr. Semwogerere Twaibu and Mr Ocen Gilibrays, for their encouragement and tireless counsel, I could not have compiled this without them.

Special thanks to Mr. Bwire Felix, Mr. Arineitwe Joshua, Mr Lusiba Badru, Mr. Odongtoo Godfrey and Mr. Matovu Davis whose warm reception and openness where another key great pillar in keeping the focus and concentration on accomplishing the entire process.

To my dear friends and classmates Flavia Agatha Ikwap, Halongo Godfrey and Kisembo Moses and all other people who have been there for me but haven't mentioned you here, thank you and May the Good Lord that sees our hearts immensely bless you.

Finally, I would like to acknowledge the love and support of my parents, my wife and son to whom I dedicate this work.

Table of content

Declaration	i
Approval	ii
Dedication	iii
Acknowledgments	iv
Table of figures	viii
List of figures	ix
List of Acronyms	x
Abstract	xi
CHAPTER ONE: INTRODUCTION	1
1.1 introduction.....	1
1.2 Background.....	1
1.3 problem statement.....	4
1.4 research objective	4
1.4.1 Research objective	4
1.4.2 Specific objectives	4
1.5 research questions.....	4
1.6 justification of the study	5
1.7 Conceptual frame work	5
1.8 Research Scope.....	5
1.8.1 Process scope	5
1.8.2 Geographical scope.....	6
CHAPTER 2: LITERATURE REVIEW	7
2.1 introduction.....	7
2.2 reliability and relevancy of digital evidence.....	7
2.3 admissible digital evidence.....	8
2.4 live forensic acquisition.....	9
2.4.1 Imaging Virtual Machines	10
2.4.2 RAID Acquisition.....	10
2.4.3 USB acquisition (DAQ).....	11
2.5 dead or live acquisition.....	12
2.6 review of digital forensic process models	13
2.6.1 The abstract digital forensics model (ADFM)	13
2.6.2 Integrated digital investigation process (IDIP)	14
2.6.3 Framework for a digital forensic investigation (FDFI).....	14

2.6.4 The four step forensic process (FSFP).....	15
2.6.5 The common process model for incident response and forensics (CPMIRCF).....	16
2.6.6 Systematic digital forensic investigation model (SDFIM)	16
2.6.7 End to end digital investigation process (EEDI).....	16
2.6.8 The Advanced Data Acquisition model (ADAM).....	17
CHAPTER 3: METHODOLOGY	21
3.1 introduction.....	21
3.2 research strategy	21
3.3 research methods	21
3.3.1 Quantitative research method	21
3.3.3 Design science	21
3.4 the research design.....	25
3.4.1 The Descriptive Field Study	25
3.4.2 Reliability and validity of the Questionnaire	28
3.5 ethical considerations	29
3.6 assessment criteria for previous models	29
3.7 assessment of previous models.....	30
CHAPTER FOUR.....	32
presentation, analysis and interpretation of results.....	32
4.0 Introduction.....	32
4.1 Response rate	32
4.2 Demographic data of respondents.....	32
4.3 Steps undertaken when carrying out digital investigations.....	37
4.4 Common forms of live digital forensic evidence.....	38
4.5 Live digital forensic acquisition tools being used.....	39
4.6 Rules that are applied during live acquisition.....	39
4.7 Existing models that are helping in conducting live forensic acquisition in Uganda	40
4.8 Common incidences that contain digital evidence.....	41
4.9 Some of the guiding principles that help fasten digital investigations	42
4.10 Vital questions about data one should consider before carrying out an investigation...	42
4.11 Ugandan courts and the common digital evidence questions presented	43
4.12 Some of the common sources of live evidence.....	44
4.13 Importance of an evidence based file during investigations	45
4.14 The common components of case files.....	45

4.15 The role of legal advice in digital evidence investigations.....	46
CHAPTER 5: DESIGN AND DEVELOPMENT	47
fundamentals of the admissible live digital evidence model (aldem)	47
5.1: ALDEM principles	47
5.2 Model creation	48
5.3 The model representation.....	48
5.4 ALDEM Stages	48
5.5 Assumptions.....	57
5.6 Model evaluation	57
5.7 Reliability of the evaluation questionnaire	57
5.8 Evaluation analysis results for the ALDEM	58
CHAPTER SIX	60
Discussion of Findings	60
6.1 Introduction	60
6.6 The implications of the research.....	65
6.7 Summary of contributions.....	66
CHAPTER SEVEN.....	67
CONCLUSIONS AND FUTURE WORK.....	67
7.0 INTRODUCTION	67
7.1 CONCLUSION.....	67
7.2 Future work.....	68
REFERENCES.....	69
Appendices.....	78

Table of figures

Table 3:1 Uganda Police Force Statistical Abstract 2016 [95].....	26
Table 3:2 Number of officers in Judicially [29]	27
Table 3:3 Uganda Police Force Sample Size Selection	27
Table 3:4 Judicial sample size selection	28
Table 3:5 model scores	31
Table 4:1 Summary of Population of Study and Sample Size.....	32
Table 4:2 Gender of respondents	33
Table 4:3 Age of respondents	34
Table 4:4 working experience of respondents	35
Table 4:5 academic qualification of respondents.....	35
Table 4:6 marital status for respondents	36
Table 4:7 Reliability and admissibility of digital evidence	37
Table 4:8 steps during digital investigations (Security organ opinion)	38
Table 4:9 Forms of live evidence (Security organ opinion)	38
Table 4:10 Live acquisition tools (Security organ opinion)	39
Table 4:11 Live acquisition rules (Security organ opinion)	40
Table 4:12 Digital forensic models (Security organ opinion)	40
Table 4:13 Incidences with live evidence (investigators opinion).....	41
Table 4:14 Principles that fasten investigations (investigator opinion).....	42
Table 4:15 Evidence source questions	43
Table 4:16 Digital evidence in Ugandan courts of law (Legal opinion).....	44
Table 4:17 Live Evidence sources (Legal opinion)	44
Table 4:18 Importance of an evidence based case file (Legal opinion)	45
Table 4:19 components of case files (Legal opinion)	46
Table 4:20: Legal advice is about the following	46

List of figures

Figure 1-1: Conceptual frame work [20],[21],[22]	5
Figure 2-1: US-LATT home screen [62]	12
Figure 2-2: digital crime scene investigation phases [64]	14
Figure 2-3: The Three Stage Process [66]	15
Figure 2-4: The Four Step Forensic Process [72]	15
Figure 2-5: EEDI stages [76]	17
Figure 2-6: stage 1 of ADAM [80]	18
Figure 2-7 stage 2 of ADAM [80]	19
Figure 2-8: Stage 3 of ADAM [80].....	20
Figure 3-1: Design science [85].....	24
Figure 5-1: The ALDEM Stage 1 (planning stage) [82],[11]	51
Figure 5-2: Stage 2 (Live Acquisition stage) [109],[104],[17]	54
Figure 5-3: Final ALDEM [20], [19].....	56

List of Acronyms

CCTV	Closed Circuit Television
CD-R	Compact Disk-Read
CD-ROM	Compact-Disk, Read-Only Memory
CID	Criminal Investigation Department (plain clothes department)
CIRT	Computer Incident Response Team
DF	Digital Fingerprint
DFIR	Digital Forensics, Incident Response
DFRWS	Digital Forensic Research Workshop
US-CERT	United States Computer Emergency Readiness Team
DF	Digital Forensics
DFTT	Digital Forensics Tool Testing
FBI	Federal Bureau of Investigation
GOU	Government of Uganda.
ICTS	Information and Communications Technologies
I.T	Information Technology.
JLOS	Justice Law and Order Sector
ULRC	Uganda Law Reform Commission
URA	Uganda Revenue Authority.
ALDEM	Advanced Live Digital Evidence Model
ADAM	Advanced Data Acquisition Model
AIGP	Assistant Inspector General of Police
ASP	Assistant Superintendent of Police
CID	Criminal Investigations Directorate
CMI	Chieftaincy of Military Intelligence
CPC	Chief Political Commissar
CPS	Central Police Station
DPP	Directorate of Public Prosecutions.
MoU	Memorandum of Understanding
UPF	Uganda Police Force

Abstract

Evidence relating to computer crimes is far much different from that associated with the everyday traditional crimes. Unlike for digital forensics, there are well established standards, procedures and models to which courts of law can refer to as regards traditional crimes and their acquisition

This thesis makes an original contribution in the field of digital forensics in Uganda, by developing a process model and matrix for admissible live digital evidence acquisition for Uganda. This is intended for acquisition of relevant and reliable live digital data by addressing the practical steps to be undertaken by investigators before the courts of law can admit such evidence.

The methodology adopted for this research is design science on the basis that it is particularly suited to the task of creating a new artifact. This was achieved by determining the matrices for admissibility of live digital evidence in Ugandan courts of law which help in attaining relevancy and reliability and later admissibility. To do so, both a literature review and model assessment of previous models and a descriptive field study using questionnaires was carried out. All this helped to identify the major activities, steps, guiding principles and rules, potential sources of live evidence and the major tools and methods used in Uganda.

The combination of these identified matrices from the results of the field study were used to extend the advanced data acquisition model, which in end led to the final stages of the admissible live digital evidence model for Uganda. Eventually the model was evaluated in a questionnaire based field study and the results showed that at least a good number thought the model was formally represented and easy to use, the language used could be understood, model is relevant, it can be reverse engineered and the steps are direct. The feedback from these were taken into consideration for the final development of the ALDEM.

The final ALDEM consists of two major stages that is preparation and live acquisition stages, these stages are eventually summarized into nine major objects and all these are represented using unified modeling language.

CHAPTER ONE: INTRODUCTION

1.1 INTRODUCTION

The chapter covers background to the study, problem statement, research objectives both major and specific ones, research questions, justification of the study, conceptual frame work, research scope including process scope and geographical scope.

1.2 BACKGROUND

Bearing in mind fast advancements in information technology and rise in computer related crimes, courts of law have been whelmed with a new form of evidence [1]. This evidence has been necessitated by the digitization of all aspects of life and this has taken a toll even on criminals who use this as a vehicle [2]. With this evidence, a wide range of reforms are urgently needed, unfortunately the tides are not swinging in favor of those slow at adopting especially the legal professionals, this has been evident in the courts of law which still grapple with admissibility of this form of evidence [3]. More pressing concerns even arise with the volatile form of this evidence, the one acquired live, this will hence be the center back interest of this research. A "live" acquisition is where data is retrieved from a digital device directly via its normal interface; for example switching a computer on and running programs from within the operating system. This has some level of risk, as data is likely to be modified [2]. This process is rapidly becoming the more common approach as disk drive capacities increase to the point where they are impractical to image and technology such as cloud computing means that you cannot even access the hardware in many cases [4].

Now days it is so becoming of lawyers to be requested evidence in electronic format [5]. Since the average lawyer does not have sufficient experience in collecting and analyzing electronic data, they can use the expertise of forensic investigators to ensure that they collect and authenticate data in a forensically sound manner [6].

In courts of law, the admissibility of evidence is governed by both state and common laws [7]. All countries have their own Evidence Acts supplemented by other forms of laws such as computer misuse act for the case of Uganda [8]. These however are inadequate laws and most of which cannot much the advanced cyber-crimes that have evolved and taken toll in all aspects of crimes brought before courts of law [9]. However, general principle adopted by majority courts of law for

REFERENCES

- [1] Kahrama, "Annual Performance," no. October, p. 30, 2012.
- [2] M. Kolhe, "Live Vs Dead Computer Forensic Image Acquisition," vol. 8, no. 3, pp. 455–457, 2017.
- [3] S. G.-R. Litig. and undefined 2009, "The admissibility of electronic evidence," *HeinOnline*.
- [4] S. Zawood and R. Hasan, "Digital Forensics in the Cloud," *CrossTalk*, no. October, pp. 17–20, 2013.
- [5] S. E. Goodison, R. C. Davis, and B. A. Jackson, "Digital evidence and the U.S. criminal justice system," *Prior. Crim. Justice Needs Initiat.*, pp. 1–32, 2015.
- [6] ITU Council, "The Admissibility of Electronic Evidence in Court: Fighting Against High-Tech Crime," pp. 1–25, 2006.
- [7] P. K.-C. neuropsychology in the criminal forensic and undefined 2008, "Admissibility of neuropsychological evidence in criminal cases," *books.google.com*.
- [8] T. H. E. Computer and M. Act, "Act 2 Computer Misuse Act," vol. CIV, no. 2, pp. 1–24, 2011.
- [9] S. Mohammed, "An Introduction to Digital Crimes," *Int. J. Found. Comput. Sci. Technol.*, vol. 5, no. 3, pp. 13–24, 2015.
- [10] D. Jones, J. H.- Hypertension, and undefined 2004, "Seventh report of the Joint National Committee on Prevention, Detection, Evaluation, and Treatment of High Blood Pressure and evidence from new hypertension," *Am Hear. Assoc*.
- [11] S. Sherman, "A digital forensic practitioner's guide to giving evidence in a court of law," *Proc. 4th Aust. Digit. Forensics Conf.*, 2006.
- [12] D. J. Daniels and S. V Hart, "Forensic Examination of Digital Evidence : A Guide for Law Enforcement," *U.S. Dep. Justice Off. Justice Programs Natl. Inst. Justice Spec.*, vol. 44, no. 2, pp. 634–111, 2004.
- [13] P. G.-S. H. L. Rev. and undefined 2002, "The Supreme Court's Criminal Daubert Cases," *HeinOnline*.
- [14] K. C.-C. L. Rev. and undefined 1993, "Taking Daubert's focus seriously: The methodology/conclusion distinction," *HeinOnline*.
- [15] M. Losavio, J. Adams, and M. Rogers, "Gap Analysis: Judicial Experience and

- Perception of Electronic Evidence,” *J. Digit. Forensic Pract.*, vol. 1, no. 1, pp. 13–17, Mar. 2006.
- [16] R. Adams, “The Advanced Data Acquisition Model (ADAM): A process model for digital forensic practice The Advanced Data Acquisition Model (ADAM): A Process Model for Digital Forensic Practice This thesis is presented for the degree of Doctor of Philosophy of Murd,” no. February 2013, 2017.
- [17] M. Rafique and M. N. A. Khan, “Exploring Static and Live Digital Forensics: Methods, Practices and Tools,” vol. 4, no. 10, pp. 1048–1056, 2013.
- [18] M. Rogers, K. Scarborough, ... K. F.-... C. on D., and undefined.2007, “Survey of law enforcement perceptions regarding digital evidence,” *Springer*.
- [19] S. Co-promoter and L. J. October, “Liforac - A Model For Live Forensic Acquisition,” no. October 2009.
- [20] R. Koen and M. Olivier, “Chapter 25 AN EVIDENCE ACQUISITION TOOL FOR LIVE SYSTEMS.”
- [21] T. G. Shipley, “Collecting Evidence from a Running Computer,” p. 5, 2006.
- [22] J. G.-C. L. Rev. and undefined 2003, “The Admissibility of Electronic Evidence at Trial: Courtroom Admissibility Standards,” *HeinOnline*.
- [23] Massachusetts Digital and Evidence Consortium, “Digital Evidence Guide for First Responders,” no. May, 2015.
- [24] National Forensic Science Technology Center, “A Simplified Guide To Digital Evidence,” 2009.
- [25] J. Frieden, L. M.-R. J. & Tech., and undefined 2010, “The admissibility of electronic evidence under the federal rules of evidence,” *HeinOnline*.
- [26] “Electronic evidence, document retention and privacy P Argy - ... Corporate Lawyers’ Association (ACLA) NSW Annual ..., 2006 - Google Search.” [Online]. Available: <https://www.google.com/search?ei=W1XPW6LRDM3kkgXD8JewBQ&q=Electronic+evidence%2C+document+retention+and+privacy+P+Argy+-+...+Corporate+Lawyers%27+Association+%28ACLA%29+NSW+Annual+...%2C+2006&oq=Electronic+evidence%2C+document+retention+and+pr.> [Accessed: 23-Oct-2018].
- [27] D. Lillis, B. Becker, T. O’Sullivan, and M. Scanlon, “Current Challenges and Future

- Research Areas for Digital Forensic Investigation,” 2016.
- [28] M. Losavio, J. Adams, M. R.-J. of D. Forensic, and undefined 2006, “Gap analysis: Judicial experience and perception of electronic evidence,” *Taylor Fr.*
- [29] “5. Review of the Evidence Act, Cap. 6 | Uganda Law Reform Commission.” [Online]. Available: <http://www.ulrc.go.ug/content/5-review-evidence-act-cap-6>. [Accessed: 23-Oct-2018].
- [30] A. Oyenyi, “A Review of ESI and EGE Under the Evidence Act, 2011,” 2014.
- [31] A. D.-F. L. Rev. and undefined 1995, “When the postman beeps twice: the admissibility of electronic mail under the business records exception of the Federal Rules of Evidence,” *HeinOnline*.
- [32] J. Frieden, & L. M.-R. J. of L., and undefined 2011, “The Admissibility of Electronic Evidence Under the Federal Rules of Evidence,” *scholarship.richmond.edu*.
- [33] C. Liu, A. Singhal, D. W.-T. J. of Digital, and undefined 2014, “Relating admissibility standards for digital evidence to attack scenario reconstruction,” *search.proquest.com*.
- [34] C. S. D. Brown, “Investigating and prosecuting cyber crime: Forensic dependencies and barriers to justice,” *Int. J. Cyber Criminol.*, vol. 9, no. 1, pp. 55–119, 2015.
- [35] M. M. Nasreldin, M. El-hennawy, H. K. Aslan, and A. El-hennawy, “Digital Forensics Evidence Acquisition and Chain of Custody in Cloud Computing,” vol. 12, no. 1, pp. 153–160, 2015.
- [36] A. Rukayat, O. Charles, and A. Florence, “A Survey and Critique of Digital Forensic Investigative Models,” vol. 14, no. 12, pp. 496–508, 2016.
- [37] D. Lillis, B. Becker, T. O’Sullivan, and M. Scanlon, “Current Challenges and Future Research Areas for Digital Forensic Investigation,” no. c, 2016.
- [38] D. B. Garrie, “Digital Forensic Evidence in the Courtroom : Understanding Content and Quality Digital Forensic Evidence in the Courtroom : Understanding Content and Quality,” *Northwest. J. Technol. Intellect. Prop.*, vol. 12, no. 2, pp. 122–128, 2014.
- [39] L. V.-C. of the A. for Information and undefined 2003, “Electronic evidence and computer forensics,” *aisel.aisnet.org*.
- [40] G. C. Kessler, “Judges’ awareness, understanding, and application of digital evidence,” *ProQuest Diss. Theses*, p. 192, 2010.
- [41] “Arinaitwe Patson Wilbroad: ADMISSIBILITY OF ELECTRONIC EVIDENCE IN

- UGANDA, IS IT 'AUTHENTIC'?" [Online]. Available: <http://patsonarinaitwe.blogspot.com/2010/05/admissibility-of-electronic-evidence-in.html>. [Accessed: 23-Oct-2018].
- [42] A. J.-A. C. L. Rev. and undefined 1996, "God Mail: Authentication and Admissibility of Electronic Mail in Federal Courts," *HeinOnline*.
- [43] "high-court-1990-10."
- [44] Legislation, "The Evidence Act," vol. 2009, no. 2008, 2009.
- [45] The Republic of Uganda, "Constitution of the Republic of Uganda," *Parliam. Aff.*, no. v, p. 192, 1995.
- [46] S. Khan, A. Gani, A. W. A. Wahab, M. Shiraz, and I. Ahmad, "Network forensics: Review, taxonomy, and open challenges," *J. Netw. Comput. Appl.*, vol. 66, pp. 214–235, May 2016.
- [47] D. P.- Computer/LJ and undefined 1980, "Computer abuse research update," *HeinOnline*.
- [48] M. G.-I. L. Rev. and undefined 1980, "Computer Crime: The Law in '80," *HeinOnline*.
- [49] V. Broucek, P. T.-E. C. B. P. Proceedings, and undefined 2004, "Computer incident investigations: e-forensic insights on evidence acquisition," *researchgate.net*.
- [50] D. Barret and G. Kipper, "VIRTUALIZATION AND FORENSICS - A digital Forensic Investigator Guide to Virtual Enviroments," *Libr. Congr. Cat. Publ. Data*, p. 247, 2010.
- [51] S. P.-I. J. of C. S. and and undefined 2009, "Digital forensic model based on Malaysian investigation process," *paper.ijcsns.org*.
- [52] Y. Cheng, X. Fu, X. Du, B. Luo, and M. Guizani, "A lightweight live memory forensic approach based on hardware virtualization," *Inf. Sci. (Ny)*, vol. 379, pp. 23–41, Feb. 2017.
- [53] J. Breeding, W. Jones, ... J. R.-2011 I. N., and undefined 2011, "™ Stream Buffer: Using an FPGA-based RAID controller with solid-state drives to achieve lossless, high count-rate 64-bit coincidence event acquisition for 3-D PET," *ieeexplore.ieee.org*.
- [54] J. Hogendorn, *Slave Acquisition and Delivery in Precolonial Hausaland*. 1980.
- [55] B. Carrier, J. G.-D. Investigation, and undefined 2004, "A hardware-based memory acquisition procedure for digital investigations," *Elsevier*.
- [56] P. S.-D. Investigation and undefined 2004, "The right tools for the job," *Elsevier*.

- [57] T. Anderson, D. A. Schum, and W. L. Twining, *Analysis of evidence*. Cambridge University Press, 2005.
- [58] M. Taylor, J. Haggerty, D. Gresty, D. L.-N. Security, and undefined 2011, "Forensic investigation of cloud computing systems," *Elsevier*.
- [59] X. Hu, W. Y.-M. S. and Technology, and undefined 2006, "Design of a data acquisition and function generation unit with USB," *iopscience.iop.org*.
- [60] M. B.-J. of E. and E. Engineering and undefined 2009, "Measurement experiment, using NI USB-6008 data acquisition," *researchgate.net*.
- [61] B. Bo, S. Shuying, W. C.-2007 8th International, and undefined 2007, "Design of data acquisition equipment based on USB," *ieeexplore.ieee.org*.
- [62] R. Yawn, M. Davis, and D. Ph, "US-LATT," no. June, 2012.
- [63] J. Surmacz and M. Goldberg, "Best Practices - For Seizing Electronic Evidence v3," *Cio*, vol. 17, no. 11, p. 26, 2004.
- [64] "electronics acquisition - Google Search." [Online]. Available: https://www.google.com/search?ei=cSo7W-ynB4zSwQLDxbS4Bw&q=electronics+acquisition&oq=electronic+acquis&gs_l=psy-ab.1.1.0i22i30k1j0i22i10i30k1i2.15728.32693.0.37628.44.23.0.0.0.655.4022.2-11j1j0j1.14.0....0,..1.1.64.psy-ab..30.14.4453.6..0j35i39k1j0i67k1j. [Accessed: 03-Jul-2018].
- [65] M. Lessing, "Live Forensic Acquisition as Alternative to Traditional Forensic Processes."
- [66] L. Wang and H. Li, "Procedia Engineering Effect of Live Evidence Acquisition Process on the Change of Windows XP SP2 Registry," vol. 29, pp. 1246–1252, 2012.
- [67] M. Grobler and T. C. Scientific, "Live Forensic Acquisition as Alternative to Traditional Forensic Processes," no. February, 2016.
- [68] M. Reith, C. Carr, G. G.-I. J. of D. Evidence, and undefined 2002, "An examination of digital forensic models," *just.edu.jo*.
- [69] B. Carrier, E. S.-D. forensic research workshop, and undefined 2004, "An event-based digital forensic investigation framework," *dfrws.org*.
- [70] B. Carrier, E. S.-I. J. of digital evidence, and undefined 2003, "Getting physical with the digital investigation process," *Citeseer*.

- [71] M. Köhn, M. Olivier, J. E.- ISSA, and undefined 2006, "Framework for a Digital Forensic Investigation.," *pdfs.semanticscholar.org*.
- [72] S. C.-I. J. of D. Evidence and undefined 2004, "An extended model of cybercrime investigations," *utica.edu*.
- [73] N. Karie, H. V.-S. for S. Africa, undefined 2013, and undefined 2013, "Towards a framework for enhancing potential digital evidence presentation," *ieeexplore.ieee.org*.
- [74] K. Kent, S. Chevalier, T. Grance, and H. Dang, "Sp 800-86. guide to integrating forensic techniques into incident response," 2006.
- [75] K. Kent, S. Chevalier, T. Grance, and H. Dang, "NIST SP800-86 Notes," no. August, 2006.
- [76] R. Hegarty, D. Lamb, A. A.- INC, and undefined 2014, "Digital Evidence Challenges in the Internet of Things.," *books.google.com*.
- [77] F. Freiling, B. S.-P. of the IMF2007, and undefined 2007, "A common process model for incident response and digital forensics," *imf-conference.org*.
- [78] A. Agarwal, M. Gupta, ... S. G.-I. J. of, and undefined 2011, "Systematic digital forensic investigation model," *researchgate.net*.
- [79] R. Agarwal and S. Kothari, "Review of Digital Forensic Investigation Frameworks," 2015, pp. 561–571.
- [80] P. S.-I. S. T. Report and undefined 2003, "A comprehensive approach to digital incident investigation," *Elsevier*.
- [81] V. Hobbs and G. Mann, "THE ADVANCED DATA ACQUISITION MODEL (ADAM): A PROCESS MODEL FOR DIGITAL FORENSIC PRACTICE," vol. 8, no. 4, pp. 25–48.
- [82] R. Adams, V. Hobbs, G. Mann, V. Hobbs, and G. Mann, "The Advanced Data Acquisition Model (Adam): A Process Model for Digital Forensic Practice," vol. 8, no. 4, 2013.
- [83] A. Hevner, S. C.-D. research in information systems, and undefined 2010, "Design science research in information systems," *Springer*.
- [84] A. Heyner and S. Chatterjee, "Design Science Research in Information Systems," 2010, pp. 9–22.
- [85] S. Y. R. Esearch, B. A. R. Hevner, S. T. March, J. Park, and S. Ram, "D ESIGN S

CIENCE IN INFORMATION," vol. 28, no. 1, pp. 75–105, 2004.

- [86] E. D.-E. R. and perspectives and undefined 2011, "Validity and reliability in social science research," *search.informit.com.au*.
- [87] R. H. Aday, C. R. Sims, W. McDuffie, and E. Evans, "Changing Children's Attitudes Toward the Elderly: The Longitudinal Effects of an Intergenerational Partners Program," *J. Res. Child. Educ.*, vol. 10, no. 2, pp. 143–151, Jun. 1996.
- [88] R. Chou, A. Qaseem, V. Snow, ... D. C.-A. I., and undefined 2007, "Clinical guidelines," *southcarolinablues.com*.
- [89] T. B.-R. in cyberethics and undefined 2004, "Ethics and the information revolution," *books.google.com*.
- [90] R. Knee, S. Reynolds, M. Ellis, 634,786 JG Hassell - US Patent 7, and undefined 2009, "Interactive television program guide system for determining user values for demographic categories," *Google Patents*.
- [91] L. Jansen, T. Rasekaba, ... S. P.-J. of allied, and undefined 2012, "Finding evidence to support practice in allied health: peers, experience, and the Internet," *ingentaconnect.com*.
- [92] J. Pascual, A. Martín-Blanco, ... J. S.-I. clinical, and undefined 2010, "A naturalistic study of changes in pharmacological prescription for borderline personality disorder in clinical practice: from APA to NICE guidelines," *journals.lww.com*.
- [93] N. T. Beins and K. M. Dell, "Long-Term Outcomes in Children with Steroid-Resistant Nephrotic Syndrome Treated with Calcineurin Inhibitors," *Front. Pediatr.*, vol. 3, Nov. 2015.
- [94] Y. Mizuno, N. Matsunami, K. Sonoda, ... S. K.-U. P., and undefined 2006, "Snapshot acquisition method, storage system and disk apparatus," *Google Patents*.
- [95] US-CERT, "Computer Forensics," *Us-Cert*, pp. 1–5, 2008.
- [96] R. Koen and M. Olivier, "An evidence acquisition tool for live systems," *IFIP Int. Fed. Inf. Process.*, vol. 285, pp. 325–334, 2008.
- [97] K.-K. R. Choo, "Legal Issues in the Cloud," *IEEE Cloud Comput.*, vol. 1, no. 1, pp. 94–96, May 2014.
- [98] I. Ademu, "A Comprehensive Digital Forensic Investigation Model and Guidelines for Establishing Admissible Digital Evidence," 2013.

- [99] C. Ruan and E. Huebner, "Formalizing Computer Forensics Process with UML," 2009, pp. 184–189.
- [100] C. Safran, H. G.-I. J. of M. Informatics, and undefined 2000, "Electronic patient records and the impact of the Internet," *Elsevier*.
- [101] T. Board, "Act 4 National Information Technology Authority , Uganda Act National Information Technology Authority , Uganda Act," vol. CII, no. 3, pp. 1–28, 2009.
- [102] H. Guo, B. Jin, and D. Huang, "Research and review on computer forensics," *Lect. Notes Inst. Comput. Sci. Soc. Telecommun. Eng.*, vol. 56, pp. 224–233, 2011.
- [103] Nlectc, "to Reporting Developments in Technology for Law Enforcement, Corrections, and Forensic Sciences," pp. 1–2, 2005.
- [104] C. C.-F. S. Forum/Forum and undefined 2015, "Basic aspects concerning the evidence aquisition in digital forensic analysis.," *search.ebscohost.com*.
- [105] M. Lessing and B. Von Solms, "Live Forensic Acquisition as Alternative to Traditional Forensic Processes," *4th Int. Conf. IT Incid. Manag. IT Forensics*, vol. 1, no. 802, pp. 1–10, 2008.
- [106] A. Luthfi and A. O. Model, "The Use of Ontology Framework for Automation Digital Forensics Investigation," vol. 8, no. 3, pp. 454–456, 2014.
- [107] N. L. Beebe, J. G. Clark, G. B. Dietrich, M. S. Ko, and D. Ko, "Post-retrieval search hit clustering to improve information retrieval effectiveness: Two digital forensics case studies," *Decis. Support Syst.*, vol. 51, no. 4, pp. 732–744, Nov. 2011.
- [108] C. Richmond, "Computer Forensics Labs: Enhancing Law Enforcement's Capabilities to Investigate Computer Related Crimes," 2004.
- [109] M. Grobler, S. V. S.-2009): Athens, undefined Greece, 25-26 June, and undefined 2009, "Modelling live forensic acquisition," *books.google.com*.
- [110] V. Baryamureeba, F. T.-P. of the F. D. Forensic, and undefined 2004, "The enhanced digital investigation process model," *dfiws.org*.
- [111] S. Selamat, R. Yusof, ... S. S.-J. of C. S. and N., and undefined 2008, "Mapping process of digital forensic investigation framework," *Citeseer*.
- [112] R. Commission, "Uganda Law Reform Commission a Study Report on Electronic," vol. 2004, no. 10, 2004.
- [113] Y. Yusoff, R. Ismail, & Z. H.-I. J. of C. S., and undefined 2011, "Common phases of

computer forensics investigation models,” *Citeseer*.

- [114] I. Homem and P. Papapetrou, “Harnessing predictive models for assisting network forensic investigations of DNS tunnels,” 2017.
- [115] R. Montasari, R. H.-2019 I. 12th I. Conference, and undefined 2019, “Next-Generation Digital Forensics: Challenges and Future Paradigms,” *ieeexplore.ieee.org*.
- [116] K. Chow, F. Law, ... M. K.-... to D. F., and undefined 2007, “The rules of time on NTFS file system,” *ieeexplore.ieee.org*.
- [117] UNODC, “Annual Crime Survey,” 2012.
- [118] L. Volonino, R. Anzaldúa, J. Godwin, and G. Kessler, *Computer forensics: principles and practices*. 2007.
- [119] M. L.-I. I. C. on D. Forensics and undefined 2005, “Non-technical manipulation of digital data,” *Springer*.
- [120] “What it will take to make Ugandan laws up to date - Daily Monitor.” [Online]. Available: <http://www.monitor.co.ug/artsculture/Reviews/make-Ugandan-laws-update/691232-2879442-vuwyop/index.html>. [Accessed: 23-Oct-2018].
- [121] E. Ernst, P. Speck, J. F.-A. emergency nursing, and undefined 2011, “Usefulness: forensic photo documentation after sexual assault,” *journals.lww.com*.
- [122] D. J. Ryan and G. Shpantzer, “Legal Aspects of Digital Forensics,” *2011 44th Hawaii Int. Conf.*, pp. 1–6, 2011.
- [123] M. M. Grobler and S. H. Von Solms, “Modelling Live Forensic Acquisition.”