Global Scientific JOURNALS
GSJ: Volume 12, Issue 2, February 2024, Online: ISSN 2320-9186
www.globalscientificjournal.com

THE ADVANCED LIVE DIGITAL EVIDENCE ACQUISITION MODEL

Nafuye Ivan, Bwire Felix, Ikwap flavia Agatha, Arinaitwe Joshua

Department of Computer Engineering

Busitema University, 236, Tororo, Uganda

Email: ivanafsberg@gmail.com, bwifex@gmail.com, flav.agatha@gmail.com, arineitwejoshua@yahoo.com

Abstract: This paper discusses the live digital evidence acquisition model that can be used by security investigators during digital investigations process. The model also takes into consideration the non-technical legal experts' opinion as far as digital acquisition is concerned, and this simply is because often times they interface with such evidence and further determine its admissibility in courts of law. The paper also discusses process models currently being used and it's believed they helped in the development of a comprehensive model that will ease investigations as well as address admissibility of such evidence once presented in court

Keywords: Live digital evidence; digital acquisition; Admissible Evidence; digital investigations

I. INTRODUCTION

Bearing in mind fast advancements in information technology and rise in computer related crimes, courts 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 as well taken toll on criminals who use this as a vehicle [2]. More pressing concerns even arise with the volatile form of this evidence, the one acquired live, as it is with other types of evidence, the courts of law using digital evidence assume its reliability if there is evidence of empirical testing in relation to the theories and techniques associated with its production [3]. It is so becoming of lawyers to be requested to present evidence in electronic format [4]. 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 [5].

However in this quest, greatest concern is that of the tools and procedures adopted by digital investigators for acquisition being outside the knowledge and understanding of the courts and juries [6]. This hence fourth has burdened forensic experts like any other expert witness presenting such evidence [7].

Other than some of the major challenges faced during live acquisition, other scholars such as [8], [9] and [10] as well point out that the whole field of digital forensics still lacks consensus. By providing a model it's anticipated that this will not only ease perception of such evidence during court proceedings but rather as well fast truck progresses of investigating. This model represents an innovative and effective approach to acquiring digital evidence from live systems while minimizing the risk of altering or damaging the data.

Compared to existing models, the Advanced Live Digital Evidence Acquisition Model incorporates advanced technologies and techniques, such as virtualization, containerization, and memory forensics, to improve the accuracy, speed, and efficiency of digital evidence acquisition. A number of digital evidence models such as the advanced digital acquisition model, enhanced Digital Investigation Process Model, the Digital Crime Scene Analysis Model among other models were evaluated and these showed different use cases and environments of applicability. Others showed effectiveness in preserving the integrity of the original data but can be time-consuming and may not be practical in live system acquisition scenarios while others were effective in capturing critical data, such as passwords and encryption keys, but were limited by the fact that volatile data is constantly changing and can be lost if not acquired quickly.

It is also important to note that while the proposed model involves acquiring data from a live system while the system is still operational and beneficial in scenarios where immediate action is required, it may be challenging to perform this without altering the data or introducing artifacts.

In this context, it is essential to understand the state of existing models and their limitations. By analyzing and comparing the different approaches to digital evidence acquisition, we can identify the strengths and weaknesses of each model and evaluate their effectiveness in specific scenarios

The main objective of this paper is to develop a standardized model with clear and practicable methods that will assist in quickening digital acquisition of live evidence that is reliable and admissible in the courts of law. It is with great intent that the final model meets on its desired outcome of acquiring reliable and admissible live digital evidence. None admissibility has led to high case back log and walking scot free by crime offenders. The subsequent section addresses the objective of the paper. Section II presents current state of live digital forensics with sub section: A presenting acquisition of live digital evidence, subsection B presenting digital forensic tools currently being used with their merits and demerits, subsection C presenting on digital forensic model classifications and section D assessment of previous models. It also has Section III presentation and interpretation of results from findings, section IV that describes the approach that the study undertook while attempting to develop the model especially using design science then Section V presents the proposed model with subsection A representing stage one of the ALDEM, subsection B representing stage two of ALDEM, subsection C the Final ALDEM and finally subsection D the model evaluation eventually the paper sums up with the conclusion in section VI.

II: CURRENT STATE OF LIVE DIGITAL FORENSICS

A: acquisition of live digital evidence

Long an ending debates still wage on regarding live or dead acquisition say to pull the plug or not to on current running systems [2]. Computers are often not actively used in the committal of a crime, but contain digital evidence that can prove that the crime was committed [11]. The computer may either be a tool of the crime, or be subsidiary to the crime and as such nature of the computer's role will inform decision either on Dead or Live Forensic Acquisition [2].

Many large organizations have moved to mostly live investigations and this has been as result of advancements in technology that have seen huge amounts of data in real time worthy paying attention to [12]. For instance applications can be installed from external media and then virtualized into RAM; data in RAM can be lost when the device is rebooted, powered off or when an open session is closed; dedicated software can be used to scrub a disk and delete the audit trail and history of actions on closedown; hidden areas of a hard disk are often used that are not visible to the standard operating system; malware that is fully RAM resident having no traces on the hard disk; root kits designed to remain hidden to the operating system so that trusted tools are required; soft wares and web browsers have evidence eradication processes [13]

Imaging Virtual Machines

Virtualization technology enables a single PC or server to simultaneously run multiple operating systems or multiple sessions of a single operating system [14]. A machine with virtualization software can host numerous applications including those running on different operating systems onto a single platform [12]. If the VM itself is the only item of interest, there may not be a need to acquire the entire drive. The virtual machine can also only be acquired in scenarios where it's very difficult to image entire drive such as in storage area network [14].

The host operating system can support a number of virtual machines each of which has the characteristics of a particular Operating systems [12]. The case for imaging the entire drive would be that the VM may have shared folders on the host machine and some install folders on the host machine where live computers can be stored and as such Evidence can easily be missed if entire environment is not captured [15]

RAID Acquisition

Raid acquisition can be the hardware or software. software raid is easiest and one can acquire entire volume using tools such as encase, pro discovery and with this acquisition it allows us access to data that is hidden on individual disks [16] with this raid type the operating system sees individual disks but as a single volume and CPU calculates parity information [17]. For hardware raid we can acquire special controllers that plug into one of the buses or the device that plugs into normal disk controllers but eventually the computer sees this as a single volume [18]

When performing hardware raid acquisition, first step is acquire and investigate completely raid volumes as single volumes and use device drivers such as those contained on Linux distributions, then the second step acquire individual disks and look for hidden data in possible areas that the

RAID volume did not use. And then perform Keyword searches on the individual disks [19]

If you have administrator credentials, the fastest and simplest live imaging method is to run your favorite imaging tool such as FTK from a thumb drive [20]. Eventually the image can either be saved to a formatted storage drive connected directly to the RAID system or sent across a network [21]

When imaging across the network, a storage device is connected to a remote system and then shared out as a network resource. The storage device can then be mounted as a network share on the RAID system and used as the destination for the forensic image [22]

USB acquisition (DAQ)

The term USB DAQ means that the communication occurs using a computers USB ports with help of USB Live Acquisition Tool [23]. Often time these tools are very easy to use such as US-LATT. Plug USB data acquisition device into an available USB port on your examining system, once the system has mounted the device, open the USB data acquisition tool's configuration

Utility program [24]. With these USB data acquisition tools, you can save a configuration or load an existing configuration from a directory. To run these devices, simply plug in to a USB port on your target device, navigate to the USB utility device and open it, often times a folder named Program, a bitmap and an executable will be seen [25]

B. digital forensics tools

A number of techniques and tools are available for the digital forensic investigators to use during the acquisition and analysis of electronic evidence. Even with these it's unfortunate that pace at which growing sophisticated crime does not match rate of new tools development [26]. Most of the industry and open source available tools such as Encase, FTK, oxygen forensic suite, and

XWF (X-ways) are often for performing specific tasks [27].The digital forensic investigator therefore needs to choose the right tool necessary for a given task and bear in mind the pros and cons of these tools as some alter state of machine being acquired. These tools are discussed below with their merits and demerits

EnCase

It's designed purposely for digital security investigations and e-discovery use. Also well known for retrieving proof from seized hard drives and aiding investigators in conducting out a holistic investigation while gathering digital evidence [27]. The technology used in EnCase is the only extensively tested technology to ensure integrity and reliability of electronic evidence. Its ability to obtain the device's serial number, location, manufacturer information etc, proves why it's the major standardized tool for investigations [28]

FTK

Forensic Toolkit as popularly called FTK, is a product of Access Data [20]. It examines a hard drive by searching for all kinds of information for example deleted emails [29].

The tool kit comes along with an independent disk imaging program the FTK Imager that saves an image of a hard disk in one document or in a different segment which can then be recreated later. The program as well computes MD5 hash values while at same time confirming their integrity and eventually creates an image file which can be saved in several formats [15].

Oxygen Forensic Suite

This tool at the moment is common among agencies in Europe more precisely with tax and customs bodies and law enforcement. It has made a name for its self as one capable of extracting all kinds of information from smartphones i.e. sim card and phone basic information. The tool is advantaged over others because of its ability to tap into the Symbian phone operating system precisely the geotagging [30].

Table 1: digital forensic tools

Tool	Merit	Demerit
ENCASE	User friendly tool.	Very expensive tool.
	Encase Imager is easy to use	The latest versions of Encase
	has good reporting functionalities	Sometimes are not compatible with other forensic based tools.
	Encase has built in support for almost all types of encryption	Processing takes a lot of time in case of very large files and mail boxes.
	Good keyword searching capabilities and scripting features	
FTK	Simple user interface and advanced searching capabilities.	Does not support scripting features.
	Produces a case log file.	Hard to estimate remaining time
	It has significant bookmarking and reporting features.	FTK does not have a timeline view.
	FTK Imager is free.	Does not have multi-tasking capabilities.
	Supports EFS decryption.	
OXYGEN FORENSIC SUITE	Allows for android physical extraction of information and data.	Supported mobile devices are limited.
	User interface and options are very simple and clear.	It uses a brute force technique which incur a lot of time to complete the process.
	It has a built in functionality that can be used to crack passwords for encrypted iTunes, locked iPhone or android backups.	Since tool is computer based, there is a higher statistical probability of virus/malware entering inside the phone that is being examined.
	The final report can be saved in multiple readable formats such .xls, .xlsx, .pdf, etc.	
	It is an economically better option when compared to other mobile forensic tools.	
XWF (XWAYS)	Evidence processing options can be customized.	The user interface is complex.
	Very flexible and highly customizable search functions.	It is a dongle based software.
	It is portable in nature and it checks for new features on a regular basis.	There is no support for Bitlocker.

C: digital forensic model classification

For purpose of understanding the current state of affairs and best practices being adopted, some of the existing models advanced by other scholars as regards digital evidence practices and procedures have been studied. Some have the authors attempting to develop generic approaches while others focus on a particular environments say incident response [31].

Before carrying out a digital forensic investigation, the investigator must know that there are a number of steps that need to be undertaken and well thought out [13]. Each of the different scholars in their models advance certain steps that uniquely identifying with the models that should be undertaken during investigations. It should be noted that a generalized methodology should be adopted when conducting an investigation for purposes of admissibility of such evidence once brought before court [32].

The abstract digital forensics model (ADFM) defines common steps from previous forensic protocols. The steps reflect the traditional forensics approach applied in a digital forensic context and outline nine components [33]. The major ones of these include Identification, Preparation, and approach strategy, Preservation, Collection, Examination, Analysis and Presentation. The components are seen as being a complete representation of the process undertaken by a digital forensic investigator [34] Integrated digital investigation process (IDIP) adopts physical crime scene procedures for digital crime scenes with the computer being treated as a step to another mystery. In this model, there is clear differentiation of Physical Crime Scene as physical environment where the first criminal act occurred and Digital Crime Scene as the virtual environment created by software and hardware where digital evidence of a crime or incident exists [35]. Later on at the 2004 Digital Forensics Research Workshop digital crime scene is in the same way treated as a physical crime scene [36]

In the Framework for a digital forensic investigation (FDFI), the important factor in a digital forensic model is knowledge of the legal environment [37]. It proposes three key stages, namely preparation, investigation and presentation which were derived partly from works on the Extended Model of Cybercrime Investigations [38]. Its Preparation stage contains standards used in the organization, Policies and procedures, Training, Legal advice, Notification to the correct authorities, documentation of previous incidents, and Planning [39]. Major concern for this study is around legal advice and planning.

The four step forensic process (FSFP) develops a guide whose aim is to provide information that would allow an organization to develop their own digital forensic capability using IT professionals [40]. It takes into consideration the different laws and regulations hence advising that the guide should only be considered at start of developing policies and procedures [41]. It consists of four stages the main ones for this study being the Collection stage consisting Identifying Possible Sources of Data, developing a plan to acquire the data, acquire the data and verify the integrity of the data [42]

The common process model for incident response and computer forensics (CPMIRCF) gives a clear distinction between incident response and digital forensics by describing the area of incident response as focusing on the activities of organizations after a security breaches with aim of detection, containment and recovery and digital forensics as being a forensic science that deals with obtaining, analyzing and presenting digital evidence after employing proven techniques and principles [43]. The model consists of three main phases' pre analysis, analysis and post analysis and is applicable in any environment of incidence response.

The Systematic digital forensic investigation model (SDFIM) proposes eleven phases analysis phases, Preparation which covers the authorization as well as collecting together the necessary resources to undertake the investigation, another phase involves securing the Scene with a perimeter to prevent unauthorized access, surveying and Recognition, Documenting the Scene,

Communication Shielding to any devices involved in the incident, evidence collection of either volatile or nonvolatile collection, Preservation involving packaging, transportation and subsequent storage prior to analysis and finally result & reviewing [44].

End to end digital investigation process (EEDI) model is not suitable for simple digital forensic investigations [20]. It is characterized by a set of general steps that must be taken by an investigator in order to preserve, collect, examine and analyze digital evidence that follows the framework set by the DFRWS [45]. Of the nine general steps used in the EEDI process only one is relevant to the acquisition of digital data and that is called Collecting Evidence [46].

The Advanced Data Acquisition model (ADAM) consists of three stages associated specifically with the acquisition of digital data [47]. These stages are in versions but for purpose of this study we took on those stages relevant to the study especially after its evaluation. These include in stage one the initial planning stage which relates to the documentation associated with the investigation, determination of investigation logistics. It as well involves a covert survey depending on the type and nature of the investigation being undertaken and finally checking paperwork where law enforcement officers have already seized devices and presented this for examination. Stage two consists of onsite survey and finally stage three the acquisition of digital data [9]

D. assessment of previous models

There are no comprehensive studies from which to draw assessment data for earlier process models and this section describes how this research has assessed these models. The assessment process is by scores being assigned to the various models to provide an indication of how many of the attributes stated in the selection criteria have been met by a particular model. The earlier process models included in the literature review were assessed individually and scored based on the criteria stated in table below

Table 2 previous model evaluation scores

MODELS	Formal representation	Acceptable	Relevant	Reverse engineered	Steps are direct & practical
The Abstract Digital Forensic Model	√	√	√	×	×
The Integrated Digital Investigative Process	×	√	√	×	×
The Enhanced Digital Investigation Process Model	√	√	√	×	×
The Digital Crime Scene Analysis Model	√	√	√	×	√
A Hierarchical, Objectives- Based Framework for the Digital Investigations Process	×	√	√	×	×
Framework for a Digital Investigation	√	√	√	√	×
The Two-Dimensional Evidence Reliability Amplification Process Model	×	√	√	×	×
The Digital Forensic Investigations Framework	√	√	√	×	×
The Four Step Forensic Process	√	√	√	×	×
The Common Process Model	√	√	√	×	
The Systematic Digital Forensic Investigation Model (SRDFIM)	×	√	√	×	√
An Extended Model of Cybercrime Investigations	×	√	√	×	×
End to End Digital Investigation (EEDI) process	×	√	√	×	√
Advanced digital Acquisition model	×	√	√	×	×

III: PRESENTATION AND INTERPRETATION OF RESULTS FROM THE FINDINGS

Reliability and admissibility of digital evidence

There are challenges with the admissibility of digital evidence in Ugandan courts, but it does not necessarily mean that digital evidence itself is not reliable. The moderate consensus on the admissibility of digital evidence ($\mu = 3.16$; $SD = 0.867$) is based on the legal professionals' confidence in the process of acquiring and presenting the evidence, as well as the sufficiency of laws and the credibility of the methods and tools used.

Steps undertaken when carrying out digital investigations

Majority of investigators are in agreement with the processes of a digital forensic investigation. The pooled mean and standard deviation for this agreement are high ($\mu = 4.23$; SD = 0.617), indicating a good level of knowledge about these processes across investigators. However, when looking at individual scores for the analysis process, the mean is moderate ($\mu = 3.69$; SD = 0.822). This may be due to investigators not engaging in this process thoroughly, leading to a lack of in-depth knowledge.

On the other hand, the mean and standard deviation for seizure, acquisition, and reporting processes are high ($\mu = 4.50$; SD = 0.504), ($\mu = 4.27$; SD = 0.45), ($\mu = 4.44$; SD = 0.692), indicating that investigators have a good level of knowledge and understanding of these processes.

Overall, the results suggest that investigators generally have a good level of knowledge and understanding of digital forensic investigation processes, but there may be room for improvement in the analysis process.

Common forms of live digital forensic evidence

The study found that there was a moderate level of knowledge representation about the various forms of live evidence ($\mu = 3.54$; SD = 0.93). However, when it came to scheduled running processes, there was a high level of knowledge ($\mu = 4.03$; SD = 0.91), indicating that investigators had a good understanding of this form of live evidence, and interfaced with it frequently during live acquisition.

Live digital forensic acquisition tools being used

Study highlights that the majority of investigators have little knowledge about the tools required for live acquisition of digital evidence. This is evident from a low pooled mean and standard deviation ($\mu = 2.97$; SD = 0.86) and a poorly distributed SD, indicating a lack of understanding across investigators. Specifically, the sleuth tool had the lowest representation ($\mu = 2.77$; SD = 0.86), while Encase and FTK had moderate representation ($\mu = 3.10$; SD = 1.00) and ($\mu = 3.05$; SD = 0.71), respectively. The poorly distributed standard deviations reinforce the fact that investigators have not been sufficiently exposed to the acquisition of live evidence, including the necessary tools and methods.

This lack of knowledge about the tools required for live acquisition of digital evidence could have significant implications for the quality of digital forensic investigations conducted by investigators. Without proper understanding and use of the tools, investigators may fail to collect crucial evidence, resulting in incomplete investigations or even false conclusions. Therefore, it is critical for investigators to receive adequate training and exposure to the tools and methods necessary for live acquisition of digital evidence, in order to improve the overall quality and reliability of digital forensic investigations.

Rules that are applied during live acquisition

There is a moderate consensus on whether some rules are being implemented during live acquisition in digital forensics investigations in Uganda. The pooled mean and standard deviation show that most investigators did not pay attention to these rules but rather focused on retrieving anything that could hold the case. However, there was a high consensus on the rule of hash files copied from the suspect machine. The standard deviations for the other rules were fairly distributed. This indicated that some investigators were implementing these rules, while others were not. The text suggests that the main focus of the investigators was to retrieve anything that could hold the case, rather than following the rules during live acquisition.

Common incidences that contain digital evidence

Highlights a disparity between investigators and legal professionals regarding the incidences that contain live evidence. According to the investigators, incidences such as threat & extortion, commercial disputes, property right infringement, fraud, and money laundering contain essential digital evidence. On the other hand, accidents, stalking, harassment, disagreements, deception, malpractices, privacy invasion, and identity theft are considered to have less digital evidence.

However, legal professionals have a slightly different perspective, with the only notable difference being property rights infringement. This difference in opinion could be due to a lack of education or awareness about the subject matter of property rights infringement. Another possible reason for the variation could be that not all investigated cases reach the courts of law.

Despite the differences, there is a moderate consensus among both investigators and legal professionals regarding the incidences that contain digital evidence, as seen by the means and standard deviations ($\mu = 3.88$; $SD = 1.04$) and ($\mu = 3.699$; $SD = 0.699$), respectively. This suggests that both investigators and legal professionals generally agree on which types of cases are likely to contain digital evidence, which can aid in the planning and execution of digital forensic investigations.

Some of the guiding principles that help fasten digital investigations

There is a lack of consensus among investigators regarding guiding principles in digital forensic investigations. Not so many investigators follow any guiding principles, and those who do have their own set of guidelines. This lack of consensus has led to a delay in investigations due to the absence of a standard protocol to follow.

However, there is a moderate level of acceptance of guidelines among investigators ($\mu = 3.673$; $SD = 0.728$). Some of the guidelines that have high means include identifying available sources and types of potential evidence, establishing the capacity for gathering admissible evidence, specifying when to undertake full formal investigations, and ensuring legal redress. On the other hand, many of the other guidelines are not followed by most investigators.

In summary, while there is a moderate level of acceptance of guidelines among investigators, there is still a lack of consensus on what guiding principles to follow, which can cause delays and inconsistencies in digital forensic investigations.

Vital questions about data one should consider before carrying out an investigation

Investigators often do not take the time to figure out important details before starting an investigation, which can lead to issues later on. Results showed that the investigators tend to overlook essential questions before starting the investigation, with a pooled moderate mean and standard deviation average of ($\mu = 3.715$; SD = 0.736). Only the question of how data is going to be made available is given high importance, with a mean of ($\mu = 4.00$; SD = 0.768). This is because investigations cannot proceed without access to data. However, the rest of the questions are not given much thought unless the need arises, as seen in the moderate means and SDs. This lack of attention to important details at the start of an investigation can lead to delays and the need for obvious fixes as the investigation progress.

Ugandan courts and the common digital evidence questions presented

It seems that there are still some concerns and reservations regarding the use of digital forensics as evidence in Ugandan courts of law. While there is a moderate consensus on whether this evidence should be admissible and treated as any other evidence, there are still some factors that need to be addressed. The means and standard deviations suggest fair scores on the relevancy, lay man understanding of process, laws being sufficient, and credibility of the methods and tools. However, the scores are lower when it comes to trust in the competence of those acquiring this evidence, reproducibility of procedures and methods, and acceptance of digital evidence in place of paper evidence. This indicates that there may be some skepticism about the reliability and validity of digital evidence, as well as concerns about the technical expertise and proficiency of those involved in acquiring and analyzing the evidence.

Some of the common sources of live evidence

There is a moderate level of understanding among legal professionals in Uganda about sources of live evidence. The mean score of 3.595 and standard deviation of 0.878 show that there is some knowledge, but there is still a lot of room for improvement. The legal professionals seem to have a better understanding of simpler sources of evidence, such as CCTV cameras, backups, archives, and phones, with higher mean scores. However, more complex sources such as equipment, software, application, and monitoring, web traffic, and logs have moderate mean scores, and their standard deviations are fairly distributed. This suggests that legal professionals find these sources difficult to comprehend due to their complex nature. Overall, there is room for improvement in the knowledge and understanding of sources of live evidence among legal professionals in Uganda.

The common components of case files

Legal professionals have a general idea of what should be included in a case file, but there is not a high level of agreement on the specifics. The moderate pooled means and standard deviation indicate that there is some variability in what different legal professionals believe should be included in a case file. However, the fact that there is general consensus on including incident description, hypothesis, evidence, proving hypothesis and impact could be a result of the fact that investigators often provide this information in their reports, which the legal professionals then use to build their case files.

IV: DESIGN SCIENCE RESEARCH METHOD

Design science research method was adopted because it suites the task of creating an artefact or new process model [83]. It was best to use design science because the focus was on designing an admissible live digital Evidence Model which makes it an ideal approach.

The design science paradigm not only was it used for design of the ALDEM but also for evaluation of this model in its applicable environment of digital investigations with hope of solving the research problem [84].

The final artifact the ALDEM is developed targeting computer forensic investigators both private practitioners and those in security organs like police and judicial officers such as Judges and magistrates that interface with live digital evidence. The model covers if not all at least most of the possible avenues of live digital evidence such as virtual machines, network connections, cookies and browser cache, events logs, scheduled tasks, root kit among many other more. Other existing models are reviewed to assist in development of the model and these majorly constitute the knowledge base [92]. Below are the design science steps and how they were used in this study:

The Relevance Cycle

Before even the model was thought off, there had to a business need in this case the problem at hand that needed to be addressed. Clearly there is a great concern for live digital evidence in the Ugandan courts of law as regards its admissibility. Technology advancements in the forms of cloud computing and virtual reality have presented massive live evidence to the investigating organizations majorly police. It is undeniable that such evidence is all the courts have in hearing and adjudicating on computer crimes. Eventually the developed model had to be evaluated in its applicable environment to see if it would serve its purpose.

The Rigor Cycle

During Rigor, there was skilled selection and application of appropriate theories and methods for constructing and evaluating the Admissible Live digital Evidence Model. There were additions to the Knowledge Base through extensions to theories and methods, new experiences and expertise, new artifact and design processes eventually coming up with a model for Uganda.

Design Cycle

Rapid iteration of build and evaluate activities were carried out hence creating and Refining the ALDEM design as a process. Unified modelling language (UML) was opted for in the design of

the major fundamental building blocks for each of the model stages. UML well represents the processes and activities in the model clearly bringing out even the complexities. The ALDEM after its design was evaluated and this involved testing it with the technical users in a controlled environment.

Design Science Research Guidelines implementation in building the model

Bearing in mind that design science is a problem solving process. The research borrowed majorly guidelines 1, 2 and 3 during study and development of the new ALDEM. In order to achieve desired outcome these guidelines were integrated during development as seen below.

Design as an artifact (Guideline 1)

As design science research requires the creation of an innovative and purposeful artifact, the new live acquisition model (ALDEM) that was created addresses especially court problems, as regards to admissibility of live acquired evidence in Ugandan courts of law, as well as aid computer forensic investigators in gathering such evidence in an admissible way. This was possible because of its effective description, hence enabling its implementation and application both in and out of court

Problem Relevance (Guideline 2)

The live acquisition model is useful in providing solutions to an ending questions and doubt on such evidence in the Ugandan courts. This model comes at a time when courts are yet to appreciate this form of evidence, doubt often times arises from the scientific methods employed. Because the artifact is built purposefully, it will yield utility for the specified problem.

Design Evaluation (Guideline 3)

The Admissible Live Digital Evidence Model (ALDEM) was evaluated after its development using methodologies in the knowledge base consisting majorly already existing models advanced by other scholars. Another evaluation stage was a field study carried out using an evaluation questionnaire issued to technical forensic investigators in police. Evaluation involved studying the model in depth both in court and in an investigative environment.

ALDEM components representation with design science

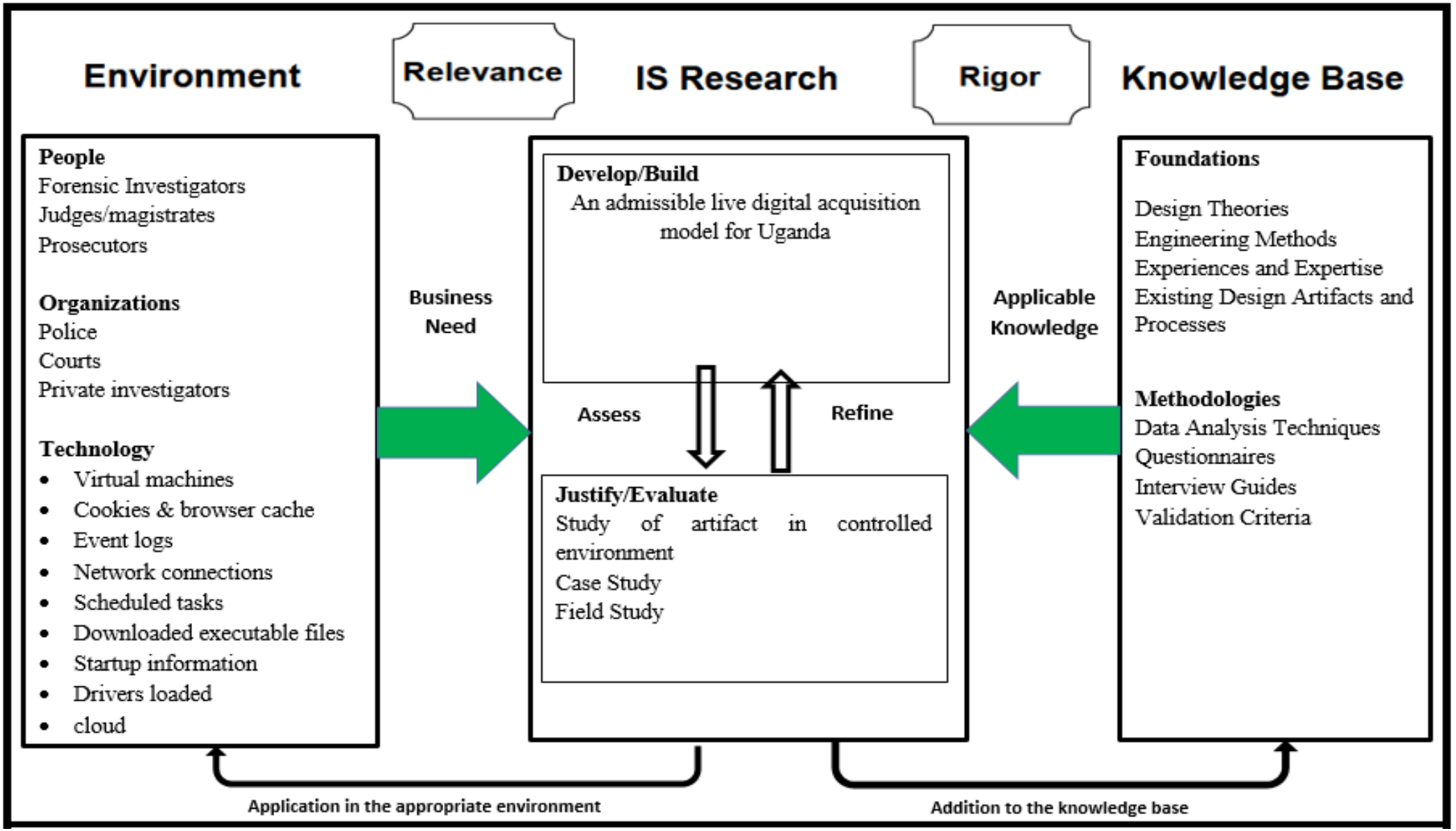

Figure 1: design science applicability & components extracted from design science applicability [85]

V: Proposed model

In this section the proposed methodology is presented especially using the subsequent figures that are eventually discussed.

Fundamentals of the admissible live digital evidence model (ALDEM)

Some of the fundamental building blocks on which the admissible live digital evidence model was based were: Take into consideration guiding principles from the international standards, police force, and other security organs on ways investigations are conducted. Put into consideration the opinion of other important stake holders more so the legal opinion to whom most often this evidence gets presented to. In all this, the model strived to have a balanced representation hoping this could accelerate its acceptance. Most of these were from the field collected results as per attached questionnaires both for the legal and forensic experts in Uganda.

The respondents were first identified with major focus on investigators in the field of forensics majorly in the security organs of the Uganda police force particularly in the departments of forensics, ICT and legal and most of these were investigating officers. However, to incorporate the legal opinion, the judiciary was also included with samples of judges, deputy registrars, chief magistrates and all these hear criminal cases and these were the target group for questionnaires. A representative sample of ninety seven (97) was selected using Krejice & Morgan table. The views of the sample were assumed to represent those of the entire population. Stratified proportionate sampling was adopted eventually.

Requirements for the admissible live digital evidence model are presented using descriptive statistics inform of mean and standard deviation. These were after analysis of collected data from the respondents to ascertain their views on the subject matter.

ALDEM principles

From involvement of both parties of digital forensic investigators and Judicial officials it was very evident that some form of rules rather principles need to be in place not only for standardization of operating principles during investigations but as well as build confidence in other none technical key influential stake holders.

The investigator should minimize amount of time they touch disk or memory or even anything within the crime scene area. This is with intent of proving that there was never alteration of original data [94].

Do not install any other programs on victim machine or even do anything else out of your investigation on this vary machine unless really need arises. Proceed to copy and hash files that have been copied from the suspect machine [95].

Ensure reputable results and methods and this is from being able to reproduce same results with the given methods under similar circumstances. Exhaust all possible would be scenarios rather

hypothesis' and equal outcomes that could have been attained from these [96].

Document all actions, scripts and timelines and always build up independent case files for each of the incidences under investigation. Some of those not to forget when building a case file include: incidence description, hypothesis, evidence, impact and necessary authorizations for carrying out the investigation [97]

Always stick to the core professional principles and ethics throughout and after the investigations. This will always come handy in backing up your submissions on credibility of work methods and results [98]

Model creation

For our ALDEM in the subsequent text we describe major elements that are used as the building blocks for the new model.

The model representation

The model was represented using Unified Modelling Language (UML). The use of the UML is supported by [99] and these dual believe that the UML describes the high level processes involved in digital forensics. UML was used to come up with activity diagrams for each of the two Stages of ALDEM representing the process flows at various stages.

ALDEM Stages

This model consists of two stages unlike the advanced data acquisition model. These are more purposely targeting acquisition of admissible live digital evidence in a Ugandan judicial setting. These stages include:

First stage: The planning stage

One of the reasons it's called the planning stage is because we seek majorly to establish what will be required for the investigation and to ensure its success. In due process of identifying these requirements some of the guiding questions and actions that will help are what trigger event caused the suspicion or alarm, visit the site, internalize the big picture, and define the parameters. And some of the events which cause or trigger suspicion and alarm include majorly threat and extortion, commercial disputes, property rights infringement, fraud and money laundering, accidents, negligence, stalking, harassment and malpractices [81].

Proceed to identifying the parties involved and these could include the victim, potential offender or offenders and regularly make it a point to reference to these as the investigations scale on. It's however important to always update these identified parties as new evidence keeps trickling in [64]

Address safety not just for you the investigator but as well as the team you constituted to work with. Safety is paramount and this cross cuts the equipment both those to be used for the investigations as well as those cordoned off at the crime scene. Have a safety plan laid out and enforce this at all times [100]

Seal off and preserve crime scene. Crime scene is very vital especially for the kind of investigation that is to be carried out. Having this scene preserved will so much save us the trouble of altering any data before analysis. Only the team and any other authorized person may access this with extra caution and observing maximum working principles that have been put in place [38].

Seek authorization. Authorization right even before visiting the crime scene inform of a search warrant will guarantee first step to admissibility of your evidence and credibility of work methods. However a warrant to search should come along with seizure so that during such period the objects or subject matter of the investigation are in custody legally [101]

Address anticipated challenges. For every kind of work challenges are always anticipated and neither is computer forensics any different. These may arise right away from how to access the data, the tools limitations in particular investigations, building and keeping the team together and focused to admissibility of the gathered evidence [102].

Set time frame: It's crucial to have estimated time periods in which to accomplish set targets. Time targets may be set on smaller sub tasks or on the task in its entire form. Well proper coordinated and scheduled activities enable adherence to set deadlines and achievement to desired goals [40].

Classify type of Investigation: It's at this level that the Investigator gets prepared either to take on a fully investigation or a targeted one. The right kind of investigation prepares one for the right tools to be opted for, the methods to be used, and the team to be assembled and even the scope of the activities to be undertaken [103].

Plan necessary logistics: Among some of these are equipment both hardware and software ones to be used such as write blockers, team and monetary implication on their numbers, transport cost and means of moving the evidence to the lab, storage costs incurred in preserving and keeping [81].

Lay out a plan for evidence acquisition: with all this in place, the investigator has at his/her disposal all that will help him kick start and run the acquisition processes of live digital evidence. It is at this stage that the next level may be proceeded to and that is stage two of ALDEM [104]

A: STAGE ONE OF ALDEM

Figure 2: the ALDEM planning stage

One of the reasons it's the planning stage is because we seek majorly to establish what will be required for the investigation and to ensure its success. In due process of identifying these requirements some of the guiding questions and actions that will help are what trigger event caused the suspicion or alarm, visit the site, internalize the big picture, and define the parameters. And some of the events which cause or trigger suspicion and alarm include majorly threat and extortion, commercial disputes, property rights infringement, fraud and money laundering, accidents, negligence, stalking, harassment and malpractices.

Proceed to identifying the parties involved and these could include the victim, potential offender or offenders and regularly make it a point to reference to these as the investigations scale on. It's however important to always update these identified parties as new evidence keeps trickling in.

Address safety not just for you the investigator but as well as the team you constituted to work with. Safety is paramount and this cross cuts the equipment both those to be used for the investigations as well as those cordoned off at the crime scene. Have a safety plan laid out and enforce this at all times.

Seal off and preserve crime scene. Crime scene is very vital especially for the kind of investigation that is to be carried out. Having this scene preserved will so much save us the trouble of altering any data before analysis. Only the team and any other authorized person may access this with extra caution and observing maximum working principles that have been put in place.

Seek authorization. Authorization right even before visiting the crime scene inform of a search warrant will guarantee first step to admissibility of your evidence and credibility of work methods. However a warrant to search should come along with seizure so that during such period the objects or subject matter of the investigation are in custody legally.

Address anticipated challenges. For every kind of work challenges are always anticipated and neither is computer forensics any different. These may arise right away from how to access the data, the tools limitations in particular investigations, building and keeping the team together and focused to admissibility of the gathered evidence.

Set time frame: It's crucial to have estimated time periods in which to accomplish set targets. Time targets may be set on smaller sub tasks or on the task in its entire form. Well proper coordinated and scheduled activities enable adherence to set deadlines and achievement to desired goals.

Classify type of Investigation: It's at this level that the Investigator gets prepared either to take on a fully investigation or a targeted one. The right kind of investigation prepares one for the right tools to be opted for, the methods to be used, and the team to be assembled and even the scope of the activities to be undertaken

Plan necessary logistics: Among some of these are equipment both hardware and software ones to be used such as write blockers, team and monetary implication on their numbers, transport cost and means of moving the evidence to the lab, storage costs incurred in preserving and keeping

Lay out a plan for evidence acquisition: with all this in place, the investigator has at his/her disposal all that will help him kick start and run the acquisition processes of live digital evidence. It is at this stage that the next level may be proceeded to and that is stage two of ALDEM.

B: STAGE TWO OF ALDEM

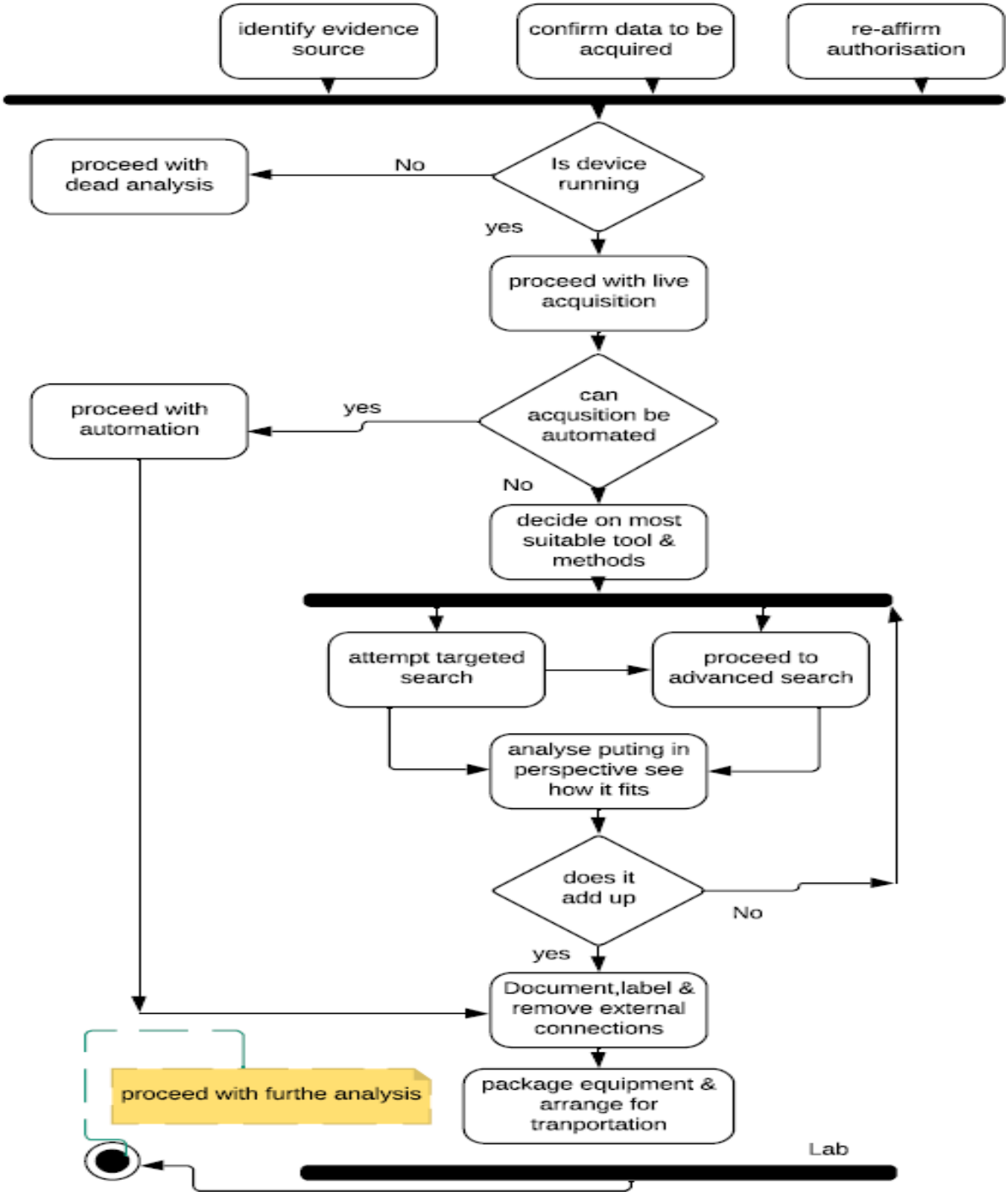

Figure 3: stage 2 live acquisition stage

The starting point of this stage is identification of the evidence source. Most of these source have been identified as equipment such as routers, firewalls, servers and clients, software such as application software, monitoring software, general logs, CCTV, and phone logs, back-ups, laptops and desktops.

Confirm data to be acquired: live evidence in the above evidence sources can be in various forms these being scheduled running processes and tasks, disk & memory dump, start up information, cookies & browser cache etc.

Re-affirm authorization: at this level it's not just authorization but re affirm most of the necessities in stage one just to make sure all that is required for the job is available. Most important be certain that both legal and other necessary authorization have been attained and these should be well documented and kept in the case file

Device state: Confirm state of the device whether its powered on and running, if this is off then immediately proceed with a dead acquisition and arrange for transportation to the lab there after. However if the device is running, then proceed with live acquisition of the evidence

Acquisition automation: when performing live acquisition, we can either automate the process or directly manually proceed with the process. If automation is possible then proceed with the acquisition and there after document label and remove external connections and then package equipment and arrange for transportation. However if automation is not possible proceed with manual acquisition

Select tools & methods to use: The investigator is now certain of type of investigation to be carried out and hence they decide on the most suitable tools and methods for this kind of investigation. Some of the tools often at the disposal of the investigator are Encase, FTK and sleith tool [52]

Target search: after selection of appropriate tool for the acquisition, the investigator may attempt a target search especially with probing questions as seen in chapter 4 such as where is the data generated, what format is it in, for how long has it been stored, who currently controls it, how is it secured and managed, who has access, is the data archived and where, how much must be retrieved, what other additional evidence sources, who is responsible for it, how could it be made available and who is the formal owner.

During target search, in summary always look at files created or modified in the last Z days or particular date, files owned or modified by a particular user in last Z days or particular date and indicators of compromise which are either by searching in memory dump and disk

C: Final ALDEM Representation

The final steps for carrying out a live acquisition are summarized in the ALDEM into nine major objects and these have been identified as identifying the trigger event from perhaps monitoring software, seek necessary authorizations before proceeding to anything else, plan necessary logistics such as team build up, identify the potential evidence source, select the acquisition methods and tools to be used, proceed to acquire the data from running equipment, have admissible evidence extracted during the entire process and present this evidence before the court.

While all this is being done ensure that thorough documentation takes place at all these stages and this is what will Advanced search: after a target search and there is need for more evidence then it may be necessary to proceed to an advanced search and acquire more evidence such as events logs & drivers loaded, registry keys, disk and memory dump, DNS cache, shell bags, last 50 DLLs created. An advanced search is always important when acquiring the entire system and when dealing with a broad nature of investigations

Sum up & put in perspective all: while a target search and an advanced search are being undertake, analyze putting in perspective all that is acquired and see how it all fits up to your arguments and hypothesis. If these do not add up move back up and re attempt the target and advanced searches. However if these do document, label and remove external connections.

Move to the lab: After documentation and labeling, package equipment and arrange for transportation to the lab where the investigator will further proceed with more analyze on this acquired data. The lab is the only place that will guarantee the investigator and the jury that the evidence was well kept without tempering and alternation and perhaps its admissibility. Build the evidence case file to be submitted as admissible evidence e in court.

These final summarized steps that form the core of the model have been built using unified modelling language and the central block or core of it is the Evidence case file. From the below UML diagram it is evident that evidence case file and documentation has a composition relationship implying this would not be in place without all the other components or stage contributors.

There is as well a composition relationship between admissible live evidence and the evidence case file implying this live evidence will only be admissible once you have an evidence case file.

And then finally the composition relationship in the last step meaning live evidence will only be used for prosecution, punishment, dispute resolving, insurance claiming and compensation once it has been admitted as admissible evidence in the court.

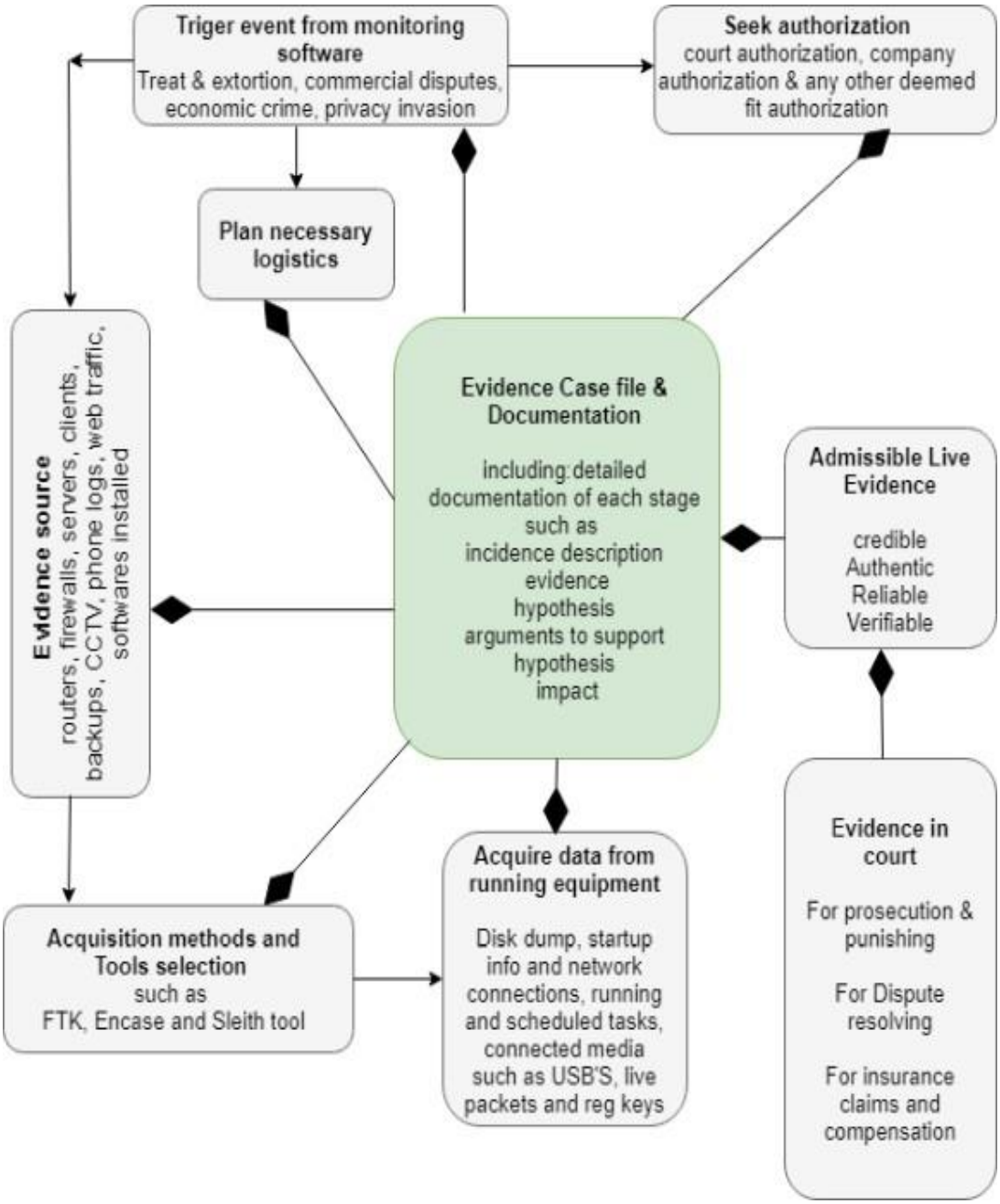

Figure 4: final ALDEM

Assumption of the model

The assumptions of the ALDEM are more like those of the previous scholars such as advanced data acquisition model [82], The Enhanced Digital Investigation Process Model [110] and The Digital Forensic Investigations Framework [111]

- The Investigator is authorized, trained and qualified with knowledge, skills and abilities for performing live digital acquisition
- There is proper documentation and methods can be reproducible using the same tools and under similar circumstances

D: Model evaluation

The model was evaluated so as to ensure that it met its intended purpose and consists the necessary requirements. A questionnaire was designed and used to collect evaluation data for the admissible live digital evidence model (ALDEM). A team of 10 forensics experts were availed with the Model and asked to rate it on the basis of the evaluation questionnaire.

Among the questions were: the model is easy to use, the language used is easy to understand, model will deliver on admissible live evidence, less time is taken when using the model, steps are direct and can easily translate into practical daily processes.

Evaluation analysis results for the ALDEM

Table 3: model & matrix represent live acquisition process & it's easy to use

	Response	Frequency	Percent	Valid Percent	Cumulative Percent
Valid	neutral	2	20.0	20.0	20.0
	agree	7	70.0	70.0	90.0
	strongly agree	1	10.0	10.0	100.0
	Total	10	100.0	100.0	

From the Table 3, in response to evaluation on ease of use of the model and its formal representation, 20% of respondents were not sure if it was easy to use and was formally represented, another 70% agreed that the model is easy to use and was formally represented while 10% strongly disagreed that the model was easy to use and formally represented. In line with this analysis a 70% agreement is a good representation on agreement of ease of use of the model and its formal representation.

Table 4: language used is easily understandable and hence model is accepted

	Response	Frequency	Percent	Valid Percent	Cumulative Percent
Valid	neutral	5	50.0	50.0	50.0
	agree	3	30.0	30.0	80.0
	strongly agree	2	20.0	20.0	100.0
	Total	10	100.0	100.0	

In Table 4 above, a highest percentage of 50% of the respondents are not very sure if the language used for the model description is easily understood by many while only 30% do think the language used is easy, another 20% strongly disagree that the language is understandable. With this it is understandable that not so many of the investigators and the legal professionals comprehended the technical terms used in forensics but rather were mere knowledgeable with carrying out the investigations.

Table 5: model is relevant and will deliver on admissible live digital evidence

Response	Frequency	Percent	Valid Percent	Cumulative Percent
Valid	neutral	4	40.0	40.0	40.0
	agree	6	60.0	60.0	100.0
	Total	10	100.0	100.0	

As seen in the Table 5, an agreement of more than half say 60% is a representation that more respondents think the model is relevant and will help in delivering admissible live digital evidence to the Ugandan courts. However 40% of the respondents were not sure if the model was relevant and would achieve on admissible live digital evidence.

Table 6: less time taken when using the model and can be reverse engineered

	Response	Frequency	Percent	Valid Percent	Cumulative Percent
Valid	neutral	3	30.0	30.0	30.0
	agree	7	70.0	70.0	100.0
	Total	10	100.0	100.0	

From Table above, majority of the respondent represented by 70% believe less time is taken if the model is used for carrying out the investigations and it can be reverse engineered and 30% of these are not sure if the time spent when using the model for investigations is less and if processes can be reverse engineered.

Table 7: steps are direct & can be practically implemented

	Response	Frequency	Percent	Valid Percent	Cumulative Percent
Valid	neutral	4	40.0	40.0	40.0
	agree	5	50.0	50.0	90.0
	strongly agree	1	10.0	10.0	100.0
	Total	10	100.0	100.0	

Table 7 shows that half of the respondents believe that the steps reflected in the model can be practically implemented and followed for live digital investigations while 40% of these are not sure if the steps of the model can be practically followed while carrying out an investigation.

The model was tested and evaluated before a number of technical investigators and findings reveled that more than half of these thought it was formally represented and easy to use, only a quarter of these did think it being acceptable and agreed that the language used was easy to understand, at least more than half found the model relevant and thought it would help in delivering admissible digital evidence, another half saw the model being easy to reverse engineer its processes and hence less time taken when using it, half as well saw the model steps being direct and practical for implementation.

VI: CONCLUSION

Compelled as the courts of law are to admit digital evidence, there still major challenges being presented regarding such evidence say competence of those acquiring evidence, methods and steps being taken, tools employed for the job, reproducibility of similar results among many more other challenges. In an effort by the investigators to meet some of these challenges, barriers in form of lack of standardization across the field of digital forensics and lack of bridge between the courts and investigators are yet to be overcome. Investigators are still struggling with technicalities of the subject matter and perhaps the same reason the courts won't give them better audience. A number of issues go wrong when investigations are being carried out were the investigators tend to more concentrate on the technicalities and pay less attention to the legal issues.

The Admissible live digital evidence model presented here outlines the major activities that ought to be undertaken for any successful live digital forensic investigation. Some of these include identifying trigger event, seeking necessary authorizations, planning necessary logistics, proceeding to acquiring the evidence by identifying the evidence source and selecting the necessary tools for the type of acquisition. In all this most important is documenting an evidence case file and presenting it before court which decides on admissibility of such acquired evidence before taking of hearing and later passing Judgment. These matrices that are the major building blocks extended the existing ADAM [53] to come up with the final model for the developing country settings such as Ugandan setting. This model will play a vital role in collecting live digital evidence by the investigators and on adjudication of cases in the courts of law. The model is

generic and can be adopted equally in other developing country jurisdictions with similar laws and settings.

Recommendations

Based on the conclusions drawn from the given text, it is recommended that measures be taken to improve the reliability of digital evidence in Uganda. This can be achieved by providing clear guidelines and procedures for the acquisition and presentation of digital evidence, as well as ensuring that the methods and tools used are transparent and reproducible. It is also important to strengthen the laws and regulations related to digital evidence to ensure that they are adequate and up-to-date.

In addition, efforts should be made to raise awareness and educate legal professionals, law enforcement agencies, and the general public about the importance of digital evidence and its role in the justice system. This can help to build trust and confidence in digital evidence, and increase its admissibility in the courts of law.

Overall, improving the reliability of digital evidence in Uganda can have significant benefits in terms of enhancing the efficiency and effectiveness of the justice system, and ensuring that justice is served in a fair and equitable manner.

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. Zawoad 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. Oyeniyi, "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, "TM 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+aquis&gs_l=psy-ab.1.1.0i22i30k1j0i22i10i30k1l2.15728.32693.0.37628.44.23.0.0.0.0.655.4022.2-11j1j0j1.14.0....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. Hevner 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 I NFORMATION," 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," dfrws.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. Anzaldua, 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-up- date/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."

Appendices

Appendix 1: Questionnaire for Security Investigators

BUSITEMA UNIVERSITY
DEPARTMENT OF COMPUTER ENGINEERING
QUESTIONNAIRE

Title: A Process Model for Acquisition of Admissible Live Digital Evidence Based on Ugandan Investigations

Preamble

Digital evidence is essentially the major form of evidence being presented before Ugandan courts. This has been as result of growing sophistication of computer crime. Almost all crime now days has some element of electronic evidence. However challenges still exist especially in the formal processes employed during acquisition of this. Another challenging fact about this evidence is that often times its volatile and can easily be lost especially when these electronic devices are switched off, hence such evidence would require immediate extraction without always going through the normal channels of evidence acquisition as necessitated by the evidence act that in its self has not been reviewed to incorporate the recent technology advancements and evolution of nature of crime. As result most of the evidence has always been rejected or rather not been admitted in the courts. It is hoped that a formal process model for the acquisition of live evidence may come in handy to solve this. This questionnaire has been formulated with questions that invite you to participate in identifying these factors that will later be used to develop this model.

NB: This study is entirely for academic purposes as a requirement for the partial fulfillment of

an award for a masters of computer forensics and hence all the findings and responses shall be treated in that effect with at most discretion and anonymity

INSTRUCTIONS

Please tick in the right box against the right answer or fill in the blank space provided below a specific question.

SECTION A. DEMOGRAPHIC CHARACTERISTICS

Q1. What is your sex?

Male ☐ Female ☐

Q2. In which Age bracket do you fall?

18-27yrs ☐ 28-37yrs ☐ 38-47yrs ☐ 48-57yrs ☐ 58- above ☐

Q3. Under what line of work do you fall?

Security organ ☐ Judiciary ☐

Q4.How long have you worked in that that profession?

0 - 5yrs ☐ 6 -10yrs ☐ 1 - 15yrs ☐ 16- above ☐

Q5. What is your highest level of academic qualification?

Certificate ☐ Diploma ☐ Degree ☐ Masters ☐ PhD ☐ None ☐

Q6. What is your marital status?

Married ☐ Single ☐ Divorced ☐ Widowed ☐ separated ☐

SECTION B

Instructions;

Please tick in the right box against the right response by indicating whether you Strongly Agree (SA), Agree (A), Neutral (N), Disagree (D), Strongly Disagree (SD), with the following views as part the question.

		OPINION				
		SA	**A**	**N**	**D**	**SD**
Q1	**These are some of the steps during a digital evidence investigation**					
Q1a	Seizure					
Q1b	Acquisition					
Q1c	Analysis					
Q1d	Reporting					
Q2	**Live evidence extracted is always in the following form**					
Q2a	Disk & Memory dump					
Q2b	Start- up information & network connections					
Q2c	Scheduled & running processes & tasks					
Q2d	Cookies & browser cache & List of USB devices used					
Q2e	Events logs & drivers loaded					
Q2f	Downloaded executable files & DNS cache					

Q2 g	Live packets capture & registry keys					
Q3	**These tools are used during live digital evidence acquisition**					
Q3a	Encase					
Q3 b	FTK					
Q3c	Sleith tool					
		SA	**A**	**N**	**D**	**SD**
Q4	**These rules are applied during the acquisition process**					
Q4a	Minimise amount of time you touch disks or memory					
Q4 b	Don't install any programs on victims machines					
Q4c	Ensure repeatable results and methods					
Q4 d	Document all actions, scripts and timelines					
Q4e	Hash any files copied from suspected machine					
Q4f	Pay keen interest when analysing disk image					
Q5	**These models are helping in digital forensic acquisition**					

Q5a	The Abstract Digital forensics Model					
Q5 b	Integrated Digital Investigation Process					
Q5c	Framework for a Digital Forensic Investigation					
Q5 d	The Four Step Forensic Process					
Q5e	The common process model for incident response and computer forensics					
Q5f	Systematic Digital Forensic Investigation Model					
Q5 g	End to End Digital Investigation					

Q6	**These incidences often contain live digital evidence**					
Q6a	Threats and extortion					
Q6 b	Accidents and negligence					
Q6c	Stalking and harassment					
Q6 d	Commercial disputes					
Q6e	Disagreements, deceptions, and malpractice					
Q6f	Property rights infringement					
Q6 g	Economic crime e.g. fraud, money laundering					

Q6 h	Privacy invasion and identity theft					
		OPINION				
Q7	These principles help fasten an investigation	**SA**	**A**	**N**	**D**	**SD**
Q7a	Define the business scenarios that require digital evidence.					
Q7 b	Identify available sources and different types of potential evidence.					
Q7c	Determine the evidence collection requirement					
Q7 d	Establish a capability for securely gathering legally admissible evidence to meet the requirement					
Q7e	Establish a policy for secure storage and handling of potential evidence.					
Q7f	Ensure monitoring is targeted to detect and deter major incidents.					
Q7 g	Specify circumstances under which to take on a full formal investigation					
Q7 h	Document an evidence-based case describing the incident and its impact.					
Q7i	Ensure legal review to facilitate action in response to the incident.					

Q8	These questions about evidence sources matter during investigations					
Q8a	Where is data generated?					
Q8 b	What format is it in?					
Q8c	For how long is it stored?					
Q8 d	How is it currently controlled, secured and managed?					
Q8e	Who has access to the data?					
Q8f	Is it archived (where and for how long)					
Q8 g	How much is reviewed?					
Q8 h	What additional evidence sources could be enabled?					
Q8i	Who is responsible for this data?					
Q8j	How could it be made available to an investigation					
Q8 k	Who is the formal owner of the data and is it personal?					

Appendix 2: Questionnaire for Legal Respondents

BUSITEMA UNIVERSITY
DEPARTMENT OF COMPUTER ENGINEERING

QUESTIONNAIRE (Respondents of Legal back ground)

Title: A Process Model for Acquisition of Admissible Live Digital Evidence Based on Ugandan Investigations

Preamble

Digital evidence is essentially the major form of evidence being presented before Ugandan courts. This has been as result of growing sophistication of computer crime. Almost all crime now days has some element of electronic evidence. However challenges still exist especially in the formal processes employed during acquisition of this. Another challenging fact about this evidence is that often times its volatile and can easily be lost especially when these electronic devices are switched off, hence such evidence would require immediate extraction without always going through the normal channels of evidence acquisition as necessitated by the evidence act that in its self has not been reviewed to incorporate the recent technology advancements and evolution of nature of crime. As result most of the evidence has always been rejected or rather not been admitted in the courts. It is hoped that a formal process model for the acquisition of live evidence may come in handy to solve this. This questionnaire has been formulated with questions that invite you to participate in identifying these factors that will

later be used to develop this model.

NB: This study is entirely for academic purposes as a requirement for the partial fulfillment of an award for a masters of computer forensics and hence all the findings and responses shall be treated in that effect with at most discretion and anonymity

INSTRUCTIONS

Please tick in the right box against the right answer or fill in the blank space provided below a specific question.

SECTION A. DEMOGRAPHIC CHARACTERISTICS

Q1. What is your sex?

Male ☐ Female ☐

Q2. In which Age bracket do you fall?

18-27yrs ☐ 28-37yrs ☐ 38-47yrs ☐ 48-57yrs ☐ 58- above ☐

Q3. Under what line of work do you fall?

Security organ ☐ Judiciary ☐

Q4.How long have you worked in that that profession?

0 - 5yrs ☐ 6 -10yrs ☐ 1 - 15yrs ☐ 16- above ☐

Q5. What is your highest level of academic qualification?

Certificate ☐ Diploma ☐ Degree ☐ Masters ☐ PhD ☐ None ☐

Q6. What is your marital status?

Married ☐ Single ☐ Divorced ☐ Widowed ☐ separated ☐

SECTION B

Instructions;

Please tick in the right box against the right response by indicating whether you Strongly Agree (**SA**), Agree (**A**), Neutral **(N),** Disagree (**D**), Strongly Disagree (**SD**), with the following views as part the question.

Objective one:

		OPINIONS

Q9	**Admissibility & reliability of Digital evidence in the courts**	**SA**	**A**	**N**	**D**	**SD**
Q9a	Is digital evidence relevant during court hearings					
Q9b	Is digital evidence often presented before court					
Q9c	Is the process of digital acquisition understandable to lay man					
Q9d	Are the laws sufficient enough to handle digital evidence					
Q9e	Are those acquiring & presenting digital evidence competent					
Q9f	Are the methods and tools used during digital acquisition clear					
Q9g	The procedures and methods of digital evidence are reproducible					

Q9h	Digital evidence is as admissible as paper evidence now days					
Q10	These incidences often contain digital evidence					
Q10a	Threats and extortion					
Q10b	Accidents and negligence					
Q10c	Stalking and harassment					
Q10d	Commercial disputes					
Q10e	Disagreements, deceptions, and malpractice					
Q10f	Property rights infringement					
Q10g	Economic crime e.g. fraud, money laundering					
		SA	**A**	**N**	**D**	**SD**
Q11	Often live evidence get recovered from					
Q11a	Equipment such as routers, firewalls, servers, clients					
Q11b	Application software, such as accounting packages for evidence of fraud					
Q11c	Monitoring software such as Intrusion Detection Software					
Q11d	General logs, such as access logs, printer logs, web traffic					
Q11e	CCTV, door access records, phone logs					
Q11f	Back-ups and archives, for example, laptops and desktops					
Q12	An evidence-based case file during investigations is important as:					
Q12a	It provides a basis for interaction with legal advisers and law enforcement					
Q12b	supports a report to a regulatory body					
Q12c	supports an insurance claim					
Q12d	Justifies disciplinary action					
Q12e	provides feedback on how such an incident can be avoided					

Q12f	provides a record in case of a similar event in the future					
Q12g	provides further evidence if required in the future					
Q13	These are some of the common components of case files					
Q13a	Incident description					
Q13b	The hypothesis					

Q13c	The evidence					
Q13d	The arguments proving the hypothesis					
Q13e	The impact					
Q14	Often legal advice about digital evidence is about					
Q14a	liabilities from the incident and how they can be managed					
Q14b	Finding and prosecuting/punishing					
		OPINION				
		SA	**A**	**N**	**D**	**SD**
Q14c	Legal and regulatory constraints on what action can be taken;					
Q14d	Reputation protection and PR issues					
Q14e	Resolving disputes					
Q14f	Any additional measures required and policy formulation					