# PROPOSING AN OPEN STANDARD FOR REPORTING DIGITAL AUDIO EVIDENCE ANALYSED BY OPEN SOURCE TOOLS

**IRENE WILLIAM MAGOMA**

**MASTER OF SCIENCE IN INFORMATION TECHNOLOGY**

**THE UNIVERSITY OF DODOMA**

**OCTOBER, 2019**

# PROPOSING AN OPEN STANDARD FOR REPORTING DIGITAL AUDIO EVIDENCE ANALYSED BY OPEN SOURCE TOOLS

BY

IRENE WILLIAM MAGOMA

A DISSERTATION SUBMITTED IN PARTIAL FULFILLMENT OF THE REQUIREMENTS FOR THE DEGREE OFMASTER OF SCIENCE IN INFORMATION TECHNOLOGY OF THE UNIVERSITY OF DODOMA

THE UNIVERSITY OF DODOMA

OCTOBER, 2019

## DECLARATION

## AND

## COPYRIGHT

**I, Irene William Magoma,** declare that this dissertation is my own original work and that it has not been presented and will not be presented to any other University for a similar or any other degree award.

Signature:……

## CERTIFICATION

The undersigned certify that they have read and hereby recommend for acceptance by the University of Dodoma a dissertation entitled "***Proposing an Open Standard for Reporting Digital Audio Evidence Analyzed by Open Source Tools"***in partial fulfillment of the requirements for the Master Science in Information Technology of the University of Dodoma.

Name of the first supervisor Signature:

…… Date: ……..

(Supervisor)

Dr. Salehe Mrutu

Name of the second supervisor Signature:

…… Date: ……..

Dr. Florence Rashidi

## ACKNOWLEDGMENT

Firstly, I would like to give my heartfelt thanks to the living God who gave me strength and the ability to pursue this study to its completion.

Secondly, my sincere thanks to my supervisors Dr. SaleheMrutu and Dr. Florence Rashidi for their willingness to take time on the progress of this research, from proposal to the final report by providing me insights throughout. Their guidance enlighten me in all the time of this study.

Thirdly, I would like to express my gratitude to all people who have given me at least something that today has shown a valuable feedback, these are Dr. Kilavo, Mr. Mutembei, Mr.Barongo, Mr. Dudu,Mr.Cralletand Mr.Chanhemo.

My gratitude goes out to all those who devoted their time to respond to my questionnaires and to Lina Magoma, Brian Magoma and Isaac Temu for the moral support they showed me during the data collection process.

Lastly, I confer my appreciation to my loving parents and guardians Mr. and Mrs. Magoma, Mr. and Mrs. Nyabiri and my devoted little sister Virginia Nyabiri for the tolerance they showed during my demanding times.

## DEDICATION

I would like to dedicate this dissertation to my divine parents, Mr. and Mrs. William Magoma for the value, love and support they have given me. Also, to my family and friends who showed concern to this study towards its completion and through their prayers. May God bless you abundantly.

## ABSTRACT

The increase of technology in business processes, Tanzania has lead to a class of crimes known as cybercrimes. Towards the mitigation of the occurrence of the crime, Tanzania enacted the cyber law which helps in ensuring all necessary security measures maintained. However, with the growth of science and technology in the investigation process, the high court of Tanzania with the help of forensic professionals is in practice digital legislation whereby the analyzed digital evidence data results are being brought in court for evidence. The process of analyzing digital evidence employs different tools and the reporting process is experienced to be of different formats. This study proposes a common format to be used for reporting the digital audio evidence data in the courtroom by the use of open-source tools.

The researcher used a mixed approach to achieving the objectives of the study. Literature review and structured questionnaires were used so as to obtain a set of forensic open source tools to be used in the study and also to propose a format to be used as a standard for reporting the results.The Autopsy forensic browser for the sleuth kit was selected as an open-source tool for performing the tests for audio analysis. Through a computer experiment, a review of different reports was produced. Based on the results from the analysis of the audio data, it was observed that a single audio input could produce a report in multiple forms including the excel format, HTML format and the text file format.The proposed included the chain of custody features which are Examiners name, file type, date, altered; file size, hash value, full path and tool type. The study concluded by proposing a format that was presented in an XML schemer which contained all the defined details for chain of custody.Various challenges were reviled in the study and the researcher recommended number of areas for improvement that would press forward the judicial practices.

## TABLE OF CONTENTS

## LIST OF TABLES

## LIST OF FIGURES

## LIST OF APPENDIX

## LIST OF ABBREVIATIONS

| | |
|---|---|
| AFF | Advanced File Format |
| ECF | Event Correlation of Forensic |
| FAT | File Allocation Table |
| HTML | Hypertext Markup Language |
| NIST | National Institute of Technology |
| NTFS | New Technology File Systems |
| STK | Sleuth Kit |
| TCT | The Coroner Toolkit |
| VCD | Video Compact Disc |
| NICE | The National Institute for Health and Care Excellence |

# CHAPTER ONE

# INTRODUCTION

## 1.1. General Introduction

Cybercrimes have emerged as a result of using computers in committing crimes while living behind the imprints unknowingly (Norden, 2013). According to Lunker (2009), cybercrimes refer to all the illegal and unauthorized practice of people automatically transmitting and processing data over computer systems and network (Lunker, 2009). The issue of cybercrimeshas come to the forefront due to the development of technology and the increase of trend of people depending on the information systems in the cyberspace(Nfuka, Sanga, & Mshangi, 2014). To prevent the associated problems of security breach from escalating, different countries worldwide have enacted cyber laws to minimize the challenge posed by computer-related cases. For example, the USA government in 2000 enacted cyber law to be used in resolving computer-related crimes (Brenner, 2001). In 2001, most of the European countries joined the movement where issues related to cybercrimes are also enforced by legislation(European Commission, 2017). Apart from the USA and Europe other countries like Iran, Canada, India, Japan, Malaysia and Singapore to mention a few have also put in place policies and laws for cybercrimes (Lunker, 2009). Analysis of 54 African countries shows that about 20% of the states have the basic legal framework for legislation on cybercrime (Council of Europe Cybercrime Project, 2016) showing unsatisfactory implementation.

Tanzania is not lagging behind on the issue of cybercrimes prevention because; the Tanzania national assembly has enacted the Cybercrimes Act of 2015. The act makes provisions for criminalizing offenses related to computers. In addition to that, it gives clarity of investigation, collection, and use of electronic evidence in Tanzania high courts (Kashililah, 2015). However, execution of cyber laws requires the police force to acquire the electronic evidence beforehand. Once the electronic evidence datais reported to be presented in the court, computer forensics tools are called upon for extracting crucial data, which connect the crime to the defendant (Ips, 2018).

Computer forensics is the practice of collecting and analyzing electronic evidence and the reports resulted are presented in a way that is legally admissible in a court. The reports generated can be used in the identification and prevention of crime and any dispute where evidence is stored digitally (Nelson et al., 2010). Computer forensics can go beyond solving problems in a corporate setting such as recovering lost files and reconstructing information from damaged equipment. Nevertheless, application of computer forensics reports in courtsrequires the tools used in the process to adhere to a common agreed standard in order to uphold legal aspects when utilizing the evidence.

One of the standard called Advanced File Format (AFF) for storing and transmitting digital data through metadata was proposed by (Baggili, 2010). The standard was agreed upon to be used for enabling the effective processing of metadata by more than one tool in the management of cases. Another standard was defined by Bariki et

al.,(2014) which was in a defined format of eXtensible Markup Language (XML) schema created to complement the former standard.Also, The National Institute for Health Care and Excellence (NICE) proposed a standard for digital health technology to act as a framework for evidence. This standard stratifies health results into tiers based on the potential outputto be verified for evidence and is in a form of guidelines to be practiced by forensic experts on the health arena.

Moreover, Carrier(2003) discussed the analysis of digital evidence in a wider range with the use of abstraction layers of the electronic data. Analysis of the conducted research indicated that the proposed standards focused on the analysis of electronic evidence in word processing documents, Portable Document Format (PDF) and Hypertext MarkupLanguage (HTML) web pages. For this reason, this study aims to propose an open standard that focuses on digital audio. The proposed standard will be useful for analysis of digital audio evidence with open source tools.

The computer forensics science itself has been around for over years but digital forensics is just a small field related to the digital world and gained popularity after the introduction of computers in the 1980s. The emergence of cybercrime later came as a new class of crimes and brought the need for computer forensics discipline (Makadya, 2011). Until the late 1990s, different legal agencies across the world became aware of the computer forensics. The first forensic labs and tools were developed by the Federal Bureau Investigation (FBI) after a prosecuted cyber case in Texas, USA. With computer-related crimes, there are two broad categories that are the; either a computer being used to commit a crime or a computer as a target for crimes(Hanson, 2014).The computer forensics nature has been open to the entire

process of collection, preservation, analysis and presentation of computer-related evidence.

The primary goal for forensics science is not just the investigation of cyber incidences but also has an impact on valuable results to the court of law. Proving a cybercrime incidence occurrence and the suspects under legal readings can be so challenging. The use of advanced crime e-handling technologyis not subject to the legal key players such as attorneys and magistrates. This gives a clear picture that some experienced experts are trained to perform incidence handling to the final stage of presentation to the courtroom. Digital forensic software tools contribute to 99% success of the entire investigation and different results form a forensics process are handled by the legal key players for judgment. On the other hand, the computer forensics process proves as a smart business practice. This indicates that the entire process of using forensic tools can enhance the security practices in general. Finding why an incidence occurred, can strengthen and tighten the security polices and can be a mitigation practice for future incidences. (L.Ramadhani, 2017).

### 1.2 Statement ofthe Problem

Since the introduction of software tools for investigating cybercrimes in courts,the high court of Tanzania is in practice of the cyber law legislation whereby the analyzed digital evidence data results are being brought in court for evidence. Forensic experts perform analysis through computer forensic software tools. To soften the process, thehigh court of Tanzania with the help of forensic experts uses more than one toolsuch as ProDiscover and the Encase tools(L.Ramadhani, 2017)for verifying the digital evidence.The use of multiple tools for examining digital data in

reporting evidence proceedings is considered important as it ensuresthe validity of the evidence(Mohammed, 2016). However, the technique of incorporating multiple tools for the aim of obtaining a valid set of evidence from audio data may result in inconsistency in reporting the extracted audio results. Due to the mismatch of reports from the evidence resources, there has been a difficulty in verifying the evidence in the court of law resulting to inability of producing concrete judgments in the court.

Assessment of digital datarequires adheringto an agreed standard to make the analysis results from the evidence become admissible before the court of law by having a known report format. In respect to this, Bariki, Hashmi, & Baggili (2014),conducted a study on defining a standardfor reporting digital evidence where they suggested an XML schema to be used in commercial tools. The standard was limited to Encase and ProDiscover commercial tools and analysis was mainly for word processing files. Moreover, NICE (2018) suggested a set of standard used as guideline in performing digital data analysis. Although the standard supports nearly all multimedia formats, it was limited to health-related forensic data hence limiting the judicial effect on these results.

Despite the fact thatBariki et al.,(2014)defined a common standard to eliminate the controversial reporting style in commercial tools, there still is a latency in audio data types.In addition to that, there is a crucial need for open source software solutions to conduct authentic digital audio analysis so as to favor the small judicial bodies lacking sufficient funds to acquire the commercial tools.Therefore, this study aims atproposing an authentic reporting format of the digital audio evidence data with

open source tools.It is expected to propose anopen standard to be used as a baseline for verifying anydigital audio data brought for evidence before the court of law. The standard has targeted on the audio evidence data because standards for other digital documents have already been proposed.

## 1.3 Research Objectives

### 1.3.1 Main Objective

The main objective of this study was to propose an open standard for open source tools used for reporting digital audio evidence.

### 1.3.2 Specific Objectives

The specific objectives of this study are;

i. To determine the efficient open-source forensic tools for digital audio analysis.
ii. To evaluate the selected open-source tools for digital audio report formats.
iii. To devisean appropriate open standard for ensuring correlation of audio evidence reports.

## 1.4 Research Questions

The study was expected to answer the following questions

i. What are the most effective open-source forensic tools for audio analysis?
ii. How does the selected open-source forensic tools repot the audio analysis results?
iii. Which open standard can be devised for ensuring the correlation of audio evidence reports?

### 1.5 Significance of the Study

This study will contribute a wider range to the improved quality of working with the digital evidence in the court of law and many other groups by the use of open-source tools. It is going to impact various groups of people in different ways either on a direct or indirect basis.

#### 1.5.1 Law Practitioners

It is aiming at bringing about confidence to individual advocates and private entities dealing with analysis of digital evidence resources brought to be used against the court. This will, therefore,benefit the law practitioners including lawyers, advocates and attorneys at different levels of experiences in their respective fields. Since the Commercial and closed source tools are expensive to acquire most especially for small law firms, it has been difficult for forensic experts to handle the digital-related cases. This study, therefore, will be helpful to them by also maintaining financial feasibility for handling digital-related cases.

#### 1.5.2 Digital Forensic Experts

The study in hand will also be beneficial to all groups of forensic experts including the detectives who will then have the freedom to apply the use of open source tools in processing digital evidence data. Likewise, the implementation of this standard towards the open-source tools is expected to bring a new direction towards improvement in the reporting system which will prove the integrity of such evidence data by eliminating the results mismatch.

### 1.5.3 Academics and Body of knowledge

In a broader sense, the study will contribute to the body of knowledge towards the use of defined formatand also to the group of scholars who will have an interest in conducting further study on the defined field.

## 1.6 Research Scope

The study covered the reporting phase of the digital forensic process, whereby it explained the issue of chain of custody details as the most important concern for any forensic report. It involved the use of open-source analysis tools which provided results for audio data that were made as inputs for the digital forensic format created that included issues of chain of custody. The choice of tools was due to the financial limitations of the commercial forensic tools and according to the study main objective.

## 1.7 Limitations of the Study

i. Limited access to digital audio evidence data from realforensic sample cases that were available in the case records. This was due to ethical issues that were directly linked to the participants' aim of protecting the confidentiality and integrity of the data. This issue was overcome through the use of the emulation method, which involved the use of imitated audio evidence data to represent actual case data.

ii. Limited time for conducting the study towards its completion. The study required a number of experiments from different open source tools as test cases so as to prove the validity of the proposed format for reporting evidence results. This challenge was overcomeby selecting an appropriate

tool to represent the rest of the forensic open source tools, which contained all requirements for the right tool. This tool could, therefore,perform analysis of evidence data in a precise manner.

# CHAPTER TWO

# LITERATURE REVIEW

## 2.1. Overview of Digital Evidence

Digital evidence is defined as information and data of value to an investigation that is stored on, received or transmitted by an electronic device. This evidence can be acquired when electronic devices are seized and secured for examination (NFSTC, 2008). Any information stored electronically is said to be digital since it can be split into a series of zeros (0s) and ones (1s) and the bits are then used to create a match for evidence. The area of digital forensics covers information including Photographs, words, Video Files, Audio files, and spreadsheets. Finding information from this form of storage and exploiting the evidence from it becomes a growing area of science and technology.

The digital forensic process includes a series of actions from the acquisition, identification, analysis and presentation Anson and Bunting(2007), whereby this research mainly focuses on the analysis and presentation parts. The reports from the forensics process are sometimes included with the official investigation report that will be presented to attorneys.

## 2.2. Digital Evidence Analysis

The analysis phase is the most critical aspect of computer forensics because it focuses mainly on performing a critical examination of the obtained data(Kalaimannan and Florida, 2015). It implies validating digital evidence in order to ensure the integrity of the data collected. Digital evidence analysis involves the interpretation of the extracted data with the help of software tools so as to determine

their significance to the case(Daniels & Hart, 2013). It helps in providing correctness of presenting the evidence in court using different hashing algorithms provided by forensic analysis tools(Nelson et al., 2010). Most computer forensic tools, such as ProDiscover, Sleuth kit, X-Ways Forensics, SANS forensic tool, FTK, and Encase provide automated hashing of digitally stored files. Data stored in different media need to have correlation so as to simplify the analysis of the forensic evidence. Event Correlation for Forensic(ECF) software tool is genuinely used for extracting evidence resources from different sources and correlating the events to provide a single output in the report.

### 2.3. Concept of Digital Evidence Reporting and Review

After examining and interpreting the acquired digital data, it is then required to be presented in a legally admissible format before legislative bodies. It is advocated by Daniels and Hart(2004),that it is important to undergo technical and administrative review of the conclusions drawn so as to adhere to the approved reporting policies. The use of software tools is necessary for obtaining a clean and unambiguous report. This means that the reporting phase marks the final process of digital forensics to document the proof of the conclusive evidence of the case in hand(Kalaimannan and Florida, 2015).Before the innovation of forensics software tools from windows, reporting and reviewing phase required manual extraction of examined data to produce a report document. However, the modern forensic process has simplified the task of reporting and documenting the conclusions from the analysis phase by combining the two and automating them. With the rapid growth of science and technology, there have emerged various tools which can perform both analysis and

reporting processes (Nelson et al., 2010). Encase, X-ways forensic tool, ProDiscover and ILook, to mention a few are some of the software tools with a built-in report generator functionality as discussed by Nelson et al.(2010).

## 2.4. Digital Audio Proceedings

Under a study by Omolayeba-Ajileye(2011), digital data is the one comprising the output of the analogue device in a digital format, being created, manipulated, stored and communicated via a computer system. The digital audio data is henceforth in a sound-related format not limited to deleted or backed-up data. This type of data can be stored in CD-ROMS, PDAs or any other portable storage device. In a similar manner, Hurber and Runstein (2018) describe how the analog audio data could be transformed into binary form by the computer processor so that it can produce digital audio data to be kept in a storage device. This means that the analog sound data is then termed as 0s and 1s, made possible by the digital audio processing software which has the ability to import, save audio files and remove pops and hisses from the background noise.

## 2.5. Digital Evidence Admissibility in the Court of Law

With the rapid advancement of technology, a large population is involved in digital transactions and businesses. A scholar from the open university of Tanzania has written a dissertation titled, “Admissibility of electronic evidence in Tanzania; law and practice”. The author clearly stated the significance and legality of electronic evidence to de accepted before the court of law. Makadya (2011) provides an assurance that it is not ethical for one to lose the rightto have their evidence stored electronically. The amendment of the evidence act made in 2015 described that one

could consider anything as a document in the following formats; Human handwriting, typewriting, printing, Photostat, photography, computer data, digital recording and any form of communication. Also, items for representation including in electronic form, by letters, figures, signatures, marks and symbols or more than one of these means, maybe admissible for evidence in any jurisdictions(Makulilo, 2016). In Tanzania, electronic evidence act was brought into validity by the landmark case of Le-Marsh, where a record of bank statement was produced as a computer print-out to show in court how loan interest had been computed. Moreover, Makulilo (2018) has stated clearly in this literature upon the admissibility of all sorts of electronic evidence following the landmark case of Salum Said vs. DPP. The case had faced a great challenge in accepting the evidence brought in the form of video compact disc (VCD), whereby it marked the new start in the high court of Zanzibar for the digital evidence admissibility. In addition to that, Makulilo(2018) perpetuated that, for the VCD to be admissible, it should be qualified with the issues of clarity of picture and sound, accuracy and relevance with litigation. A contrary to the success inadmissibility of the digital evidence, yet Thomson(2013) in his article titled "New challenges for admissibility of digital evidence", has uncovered all the difficulties associated with the authentication of the digital evidence to be used in court. Many fail to understand the proper means to authenticate efficiently their evidence resources. The author has further proposed some important criteria that any evidence should possess including the reliability of the digital recording, integrity and completeness of the data and identity or author of the recording.

## 2.6. Open Source Software Solution for Digital Audio Analysis and Reporting

Many of the common digital forensic analysis tools are developed with commercial interests in mind, for the aim of unwillingness to publish all their source code. The extraction and presentation phases areas discussed by Carrier require tools that process data to extract the important details from it. Such data contained can be of descriptive nature such as date and time accessed. Likewise with the presentation tools which organize the data from an extraction tool into a useful format. Nowadays, with the growth of forensic science, a single tool has the capability to perform both roles. For example, an extraction tool can analyze an audio file and output the time for incidence. An analyst can choose to incorporate two tools to perform the examination of audio data and results can come in a different order depending on the sorting criteria set. (Carrier, 2002 p.6) claims that "if the extraction tools are open source and the investigator has access to the output of this layer, then s/he can verify the output of the presentation tool. Therefore, the presentation tools could remain closed source, but with a published design". Therefore, creating standard techniques of audio data analysis and extraction would not limit a software company's ability to remain competitive. Open-source solution saves well the users who are also developers of the tool and to those who can share the development and maintenance issues. However, the scholars Vlastos & Patel(2016)argue that non-technical users are best served by the closed source manufacturers who make and sell the tools. On the other hand, open-source software becomes the best solution to the small companies and investigative organizations that they too will have their tasks handled systematically with a high level of correctness. By publishing source

code through open source extraction and analysis tools, the digital forensic community can examine and validate the procedures used to produce digital evidence. This helps in reducing error rate since all the bug fixes will be made public(Carrier, 2002). It is possible and easy to make a standard code base which can apply to more than one open-source tool when the bug fixed is of a common nature. Therefore, this motivates vendors to be more willing to participate in an effort to calculate error rates(Carrier, 2003).

## 2.7. Open Source Digital Forensics Analysis Tools

The forensics process is accomplished with a set of scientific guidelines suggested in 1993 called the Daubert standard, which provides admissibility of any scientific testimony(Cino, 2017). The Daubert standard with the help of computer forensic tools enables verifiability of the digital evidence in a way that computer-related cases are put into action according to the strength and ability of the tools to analyze (Smith, 2017). Up to date, forensic scientists perform analysis of digital evidence with the use of commercial tools in faith of reliable results. The Coroner Toolkit (TCT) was the early known open source forensic tool created for UNIX systems, for users with a limited budget to afford the commercial tools. The Coroner toolkit was then extended to support File Allocation Table (FAT) and New Technology File Systems (NTFS) (Sonnekus, 2014) which later was modified into today's known sleuth toolkit. This tool became one of the most popular tools and reliable in use of examination of digital evidence due to its uniqueness in capability compared to other known open source tools.

Moreover, another tool that has gained popularity in its unique functionality is the SANS forensic toolkit(Cervellone & Student, 2015). This is a set of investigative forensic toolkit with the ability to perform analysis of digital data. The SANS forensic toolkit is a powerful open-source made available as a public service to be made as part of a portfolio for any organization(SANS Investigative Forensics Toolkit Documentation, 2017).It is stable software with a unique and very high capacity to support large file-formats including raw data.

In contrast to that, the Sleuth Kit also is an efficient open source software performing automated examination of digital forensic evidence. It is highly defined by its advantage of having ease of use and minimum error rate. In addition to this, the Sleuth tool has a reporting functionality digital audio data (Nelson et al., 2010).

### 2.7.1 SANS Investigative Forensic Tool Workstation

The SANS Investigative Forensic Toolkit (SIFT) is an Ubuntu-based VMware image with forensic tools pre-installed. It is very powerful software which was first discovered for incidence response and later released for public. SANS is an open-source environment available to be accessed freely for digital forensic incidences. Experts widely prefer to use it due to its unique capabilities making it closely equal to the standard commercial tools such as EnCase and FTK. According to Ghazinour, Vakharia, Kannaji, & Satyakumar( 2017), the SANS forensic toolkit is highly featured with the following:

- Support for multiple data formats (raw,fat12/16/32,NTFS,UFS,HFS,ext 2/3/4)
- Performs live analysis

- Quick analysis and reporting functionality
- High protection against malware
- Supports expert witness
- Multiplatform support

However, the SANS Investigative toolkit allows the integration with other forensic tools such as the sleuth kit and autopsy to provide a set of valid analysis and outputs.

### 2.7.2 Encase

The EnCase software developed by the guidance software group (Software, 2018), is one of the leading software tool for performing a variety of computer forensic services. It is a commercial tool that can be accessed from the product vendor. Since its founding up to present, over 20,000 experts worldwide rely on this tool to complete the task of investigation at all phases (Ambhire, 2012), resulting in effective E-Discoveries. The EnCase tool covers the entire investigation lifecycle from the collection of electronic evidence, analyzing to the reporting level (Ghazinour et al., 2017). EnCase is characterized by the following features according to the Guidance Software group.

- Support for multiple file system formats (NTFS, FAT, UFS)
- Processing multiple disk image (Raw, VMware, Safeback)
- Remote data collection and processing
- Producing large scale forensic reports in HTML or RTF
- Memory acquisition
- Password recovery

- Uses keyword, metadata and hash values to collect data
- Limited to Windows, AIX Linux, Solaris OS

Together with the good quality features of the product, on the other hand it is difficult to use and requires more training for users before performing effective analysis. Searching is also made difficult and might be confusing and log files for a particular session are not available (Ambhire, 2012).

### 2.7.3 AccessData Forensic Toolkit (FTK)

The Forensic Toolkit is a product developed by AccessData group and integrated by the forensic acquisition and analysis program. It is a proprietary software tool available in the market. With the help of FTK imager, the tool is able to create disk images and previewing without changing the original data (Bariki et al., 2014). The FTK is widely used and as popular as the EnCase tool due to its capability to process data while maintaining the integrity of the original data. It is characterized by the following features adopted from the review done by Ambhire, (2012).

- Supports multiple file system formats (FAT,ex2/3,NTFS)
- Reads multiple disk image formats (Raw,SMART,SafeBack,EnCase0.1)
- Generates reports in different forms (HTML,XML,RTF)
- Allow for keyword search
- Creates hash values for any file (MD5)
- Performs email analysis
- Ease of use during the analysis process

In a contrast to the mentioned features, the FTK tool lacks compatibility to other Operating System software except the MAC OS, also takes long time to import forensic image hence affects the processing speed and lastly, it has minimum features for customization compared to other tools (Ambhire, 2012).

### 2.7.4 Sleuth Toolkit and Autopsy Browser

The Sleuth toolkit is an open-source forensic tool developed independently by Brian Carrierwhich was an advancement of the Coroners toolkit(Carrier, 2002). It is well known by investigators in the 21$^{st}$ century by enabling them to identify and recover evidence from forensic images acquired during incidents or on live systems. The sleuth kit works on windows OS, Linux, OS X and other UNIX systems. This tool works on a command-line environment, requiring the investigator to be of more knowledge. However, it can be used alongside with the Autopsy forensic browser which provides a frontend graphical user interface. Autopsy tool performs digital case management at all levels, the following being some of its features(Brno, 2018).

- File system analysis (NTFS,FAT12/16/32, Ext2/3/4,ExFAT)
- Keyword search
- Email analysis
- Hashing for any file (MD5&SHA-1)
- Report generation (HTML, Xls, Excel)
- Email and web artifacts analysis

Moreover, the autopsy has an additional advantage that it allows customization of the tool according to the investigators' intentions example, the reporting infrastructure of the tool allows editing of the existing module and replacing it with a customized one to suit the specific behavior (Brno, 2018).

### 2.7.5 Digital Forensics Framework (DFF)

The digital forensic framework is both an investigation tool and also an open source development platform for performing digital forensics assessments. It is used by different law enforcement agencies, education institutions, digital forensic researchers and private companies worldwide (Ghazinour et al., 2017). The DFF is built on a dedicated Application Programming Interface (API) and is available in three options, DFF free, DFF Pro and DFF Live. The DFF free requires no payments but lacks technical support for end-users. Digital forensic framework is featured by performing cryptographic hashing, automatic extraction of data, performing live and static analysis, scripting, batching capabilities and reading standard forensic file formats.

### 2.7.6 Pro-Discover

This is an integrated forensic tool which works on windows platform on collection, management and analysis of digital data. Pro-Discover is a commercial forensic platform that allows investigators to perform live analysis on systems (Bariki et al., 2014). This tool supports numerous features such as performing keyword search, MD5 hashing of files, disk imaging, support for different file systems including FAT 12/16/32 and generation of quality reports from the analysis done by the tool, to be

presented in legal proceedings (Ghazinour et al., 2017). However, the survey done on both commercial and open-source tools did not cover all available tools in the field but rather, some of the commonly used tools with the capability to produce a forensic report after analyzing the evidence data.

## 2.8. Related Works

A study carried out byBariki, Hashmi, & Baggili (2014) in the Middle East, defined a standard for reporting digital evidence items in computer forensic tools. The authors focused on developing a standard that could be used on the reports generated by computer forensic tools. The study employed an incremental procedure to develop a standard for reporting evidence items. The authors surveyed three commercial forensic tools namely ProDiscover, Encase and AccessData tool that perform various forensic procedures including reporting. In this study, the authors examined each tool's reporting function so as to obtain important requirements for evidence data. Reporting was tasted through an XML schemer was defined for the proposed format which would, therefore, perform as a merger for reports from commercial tools. The authors gathered opinions from the digital forensic community and also reviewed the report identical details from the analysis made by the three commercial tools, to obtain basic requirements for the forensic reporting standard. The study scope was limited to the reporting phase and commercial tools so as to give space for further studies.

In s similar manner, another study conducted by (Mohammed, 2016) generated a framework which could solve the problem of analyzing big and heterogeneous digital evidence data. The author reviewed the big data acquisition analytics, data

clustering algorithms, data reduction process with hashes and data correlation. The study revealed the challenge existing in the forensic field including the problem of analyzing big heterogeneous data. A novel framework proposed covered three core areas including the data volume, heterogeneous data and investigator cognitive load of understanding the relationship existing between the artifacts. The framework solved the problem of data volume through the use of metadata, the problem of heterogeneous data resources through semantic web anthologies and also the use of artificial intelligence models for automatic identification and correlation of the artifacts for investigators. Through the use of artificial intelligence models, the investigators could easily understand the nature and existing relationship of artifacts. The study concluded that through the proposed framework, the forensic process on examination and analysis phase would integrate big data from heterogeneous sources which is a problem for many investigators using various forensic tools. Nevertheless, this study did not capture the remaining phases of the forensic process including the forensic reportfrom the analysis of big heterogeneous data.

Furthermore,Carrier, (2003) conducted a study on digital forensics examination and analysis tools using abstraction layers to determine proper tools and errors engaged in the digital forensic data analysis process. This study covered the issue of layers of abstraction which were described as a means of analyzing large data in a more manageable form. The researcher described the requirements for analysis tools of digital evidence data and explained the application of abstraction layers as a means of identifying errors in the process of analyzing digital evidence data

Ratnasari, Devi and Prayudi, Yudi and Sugiantoro, (2018)defined an XML approach for the solution of chain of custody reports for digital evidence. In this study, the authors presented an application that could provide documentation of chain of custody evidence by the use of XML. The application was developed to cover the needs of different file types from electronic evidence sources. It was built through Java language and cross-platform complaint and the main chain of custody fields were defined and included as part of modules in the application. The application involved a number of experiments by case scenario, which was conducted so as to produce secured documented reports produced for chain of custody. Inputs to the experiment included data from the case scenario which were the evidence that was directly reported to police and the ones found in storage devices such as Flash Drives. The acquisition process was done through multiple forensic tools including Encase, FTK, and XRY and Wireshark and the MD5 values were recorded.In case of any integrity change, the report produced after using this chain of custody application could be noticed through the difference in MD5 values before and after documentation. The authors majored in this study to the chain of custody section of digital forensic being a part of reporting the analysis of evidence data since the forensic reporting phase requires a high level of data integrity and security. It was seen of great need to have a precise and unambiguous report that could be used in the court and also by non-forensic experts. Therefore the study concluded that, in any cyber-related case,the process of digital forensic analysis requires a precise report document form of chain of custody which explains the whole process from evidence acquisition to presentation.  However, the study evolved around the chain

of custody element of digital evidence since it is the most critical area which proves the integrity of the evidence data

## 2.9. Research Gap

Despite all the studies conducted concerning the digital evidenceprocess in different phases, yet there is hardly a study that covers the issue of correlation and uniformity of digital evidence reports generated from analysis of evidence data from different open-source tools. Furthermore, the studies from previous researchers failed to reveal the issue of open source tools as a solution to digital forensic analysis by identifying the important and verifiable tool features that are required to make them reliable for use. Moreover, the previous studies failed to capture the digital audio evidence types in solving ambiguity in reporting the analysis results. This brings about the need to conduct a study that can cover issues of correlation of reporting documents on digital audio evidence data. It is expected that this study will bridge the currently existing gap towards new areas of study which were not put into consideration.

# CHAPTER THREE

# METHODOLOGY

## 3.1. Introduction

This section of the research has presented the methodology which was used for the proposed study. It has stated the data collection methods used, software toolsapplied, research approach and the emulation setup for the experiment.

In this study, a mixed approach was used to address the research questions. The mixed approach involves a hybrid setting of both computer experiment and quantitative research. It has been proven by (Daniel, 2004) who argues that the research approach can either be qualitative, quantitative or mixed (qualitative and quantitative) approach depending on the nature of the study.

## 3.2. Research Strategy

The study has used the emulation process to capture results for the proposed solution. The choice of this strategy has been influenced by the nature of research objective three (3) and its related question Saunders et al. (2009). The strategy has modeled the inputs to the real selected open-source tools so as to obtain results that help to achieve the third objective. Also, documentary review was used as a strategy for determining the best open source tools and quality and acceptable reporting formats.

### 3.3. Emulation Process

The emulationmethod uses a computer to imitate the operating real environment of a system. Since it is a powerful and intuitive technique, simulation can be used for complex systems to process experiments (Douglas, 2015). Emulation best fits the study due to tightening ethical conditions of accessing the real inputs to test the applicability of the proposed standard (Mchaney, 2009).

### 3.4. Study Settings

This study was specifically based on the selected open-source tools to implement and compare the validity and integrity of the captured audio data from the evidence source.The researcher used a sound recorder that helped to capture the audio data; and storage devices such as flash disc and CDs which helped in preserving the obtained digital audio data. These storage devices were then used as evidence sources, forinputting data in the open-source forensic tools so as to observe the analysis and reports produced by each.

Digital audio data analysis requires software that is a digital forensic tool to receive and process the audio data of known format and characteristics. The audio datawas used as input to the experimentand obtain a final report document with the defined format. depicts the laboratory setup that was used in the study. Figure 3.1 depicts the emulation setup for conducting the digital audio data analysis so as to examine the multiple report formats that a tool is capable of producing producing.

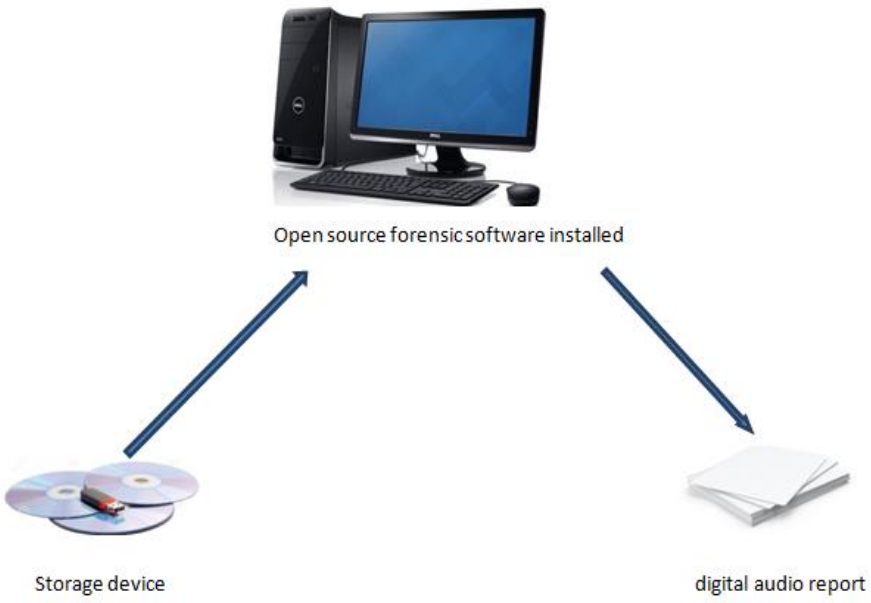


**Figure 3.1: Emulation Experiment Setup**

**Source**: (Researcher,2019)

### 3.5Research Approach

The study used a mixed approach to produce a hybrid setting of both quantitative and qualitative research methods so as to address the research questions. It worked by deploying the existing standards and proposing a format that would work for the open source tools. This was due to time constraints in the accomplishment of the study as well as limited financial sustainability to support it.

The following procedures were used towards achieving the specific objectives.

i. The researcher went through a literature review, to obtain the most commonly used and effective open-source tools. Here, data was obtained from the e-Library and resulted in a valid set of results. This approach helped in achieving the first specific objective.

ii. The researcher tested the efficiency of the identified open source tools in achievement of the second objective so as to observe the mismatch of audio reports produced. After analysis done by the selected tools, the results were produced and the report formats verified the difference in report formats.

iii. Lastly, from a survey of studies done by different scholars, the researcher generated an XML schema with defined criteria that finally stood as an agreed standard to be used with open source tools identified on the first objective. The defined criteria were derived from the recommended fields which are important to be inclusive for any forensic report by maintaining a chain of custody. Thisenabledthe implementation of the third objective.

### 3.6 Population

This part represents a group of individuals, objects or items from which a sample was taken for measurement. For this particular study, the targeted population was a group of law practitioners including the police force, lawyers, advocates and forensic investigators. This is because, according to their area of profession, they would pose key information about existing digital crime scenarios and how they are handled. The number of employed staff was from various areas of work including the high court of Tanzania at Dodoma region, the central police station and some private law firms such as Rweyengeza Company, Nyangarika Company and the Wasonga's. The population reached was a total of 60 people in total.

### 3.7 Sampling Frame

This defines the elements of the population sample that was selected for the study. The sample frame for this study was a number of the permanently employed people in a particular institution.

#### 3.7.1 Sampling Method

This part explains the plan, techniques and procedures used by the researcher to obtain a sample from the defined population. Usually, the sampling processis done before data is collected. The researcher used a non-probability method during the identification of the sample. In the non-probability sampling process, the organizers of the inquiry purposively chose the particular units of the universe for constituting a sample on the basis that the small mass that is to be selected out of a huge one would be typical or representative of the whole.

Purposive sampling was used to select a group of professionals including lawyers, detectives, state attorneys and forensic experts. A purposive or judgmental sampling enables the researcher to use his judgment to select elements of the population that will best answer the research question(s).Due to time constraints and limited knowledge of the population, the researcher decided to use the non-probability design to ease the project. The other reason for selecting purposive is to obtain a group of people that the researcher expected to be reliable for the study according to each respondent's profession.

### 3.7.2 Sample Size

This represents the specific number of elements selected to represent the entire population. The study involved a sample size of 41 respondents whereby 12 people were state attorneys, 23 advocates, 2 ICT officers from the high court and 4 detectives (Table 3.1).

**Table 3.1 Sample Size**

| S/N | Type of Respondent | Actual Sample Drawn | Sampling Technique |
|---|---|---|---|
| 1 | State Attorneys | 12 | Non Probability (Purposive Sampling) |
| 2 | Advocates | 23 | Non Probability (Purposive Sampling) |
| 3 | ICT officers | 2 | Non Probability (Purposive Sampling) |
| 4 | Detectives | 4 | Non Probability (Purposive Sampling) |
| | **TOTAL** | **41** | |

## 3.8 Data Collection Methods

i. **Observation technique**

Through the computer simulation, the researcher observed how the software tools conduct criminal profiling so as to obtain digital audio reports in formats pertaining toa particular tool.

ii. **Documentary Review**

Secondary data was collected from previous researches, journals, reports and books related to the study. The aim was to verify the existence of the report heterogeneity problem and determine the best open source tools mostly used for digital audio analysis.

iii. **Questionnaires**

Structured questionnaires were administered to detectives, state attorneys and individual advocates from different law firms. The goal of this primary data obtained was to verify the existence lack of implementation of a common open report standard. The sample of the questions that were asked to these groups of respondents are indicated in appendix 1

### 3.9 Data Analysis

The study adopted both qualitative and quantitative data analysis techniques. A descriptive analysis was used to analyze quantitative data obtained from questionnaires supplied to different respondents. The sum, percentages of responses were calculated and exported into excel forplotting tables, histograms and pie charts. In addition, document analysis was used to report the findings from works of literature for objectives one and three, and supplement the quantitative results.

### 3.10 Ethical Issues

The researcher asked for permission from the University of Dodoma administration to visit targeted areasduringthe data collection stage. Also, to ensure confidentiality and privacy the respondents' names were not reported anywhere in this study. In addition, the discussions of the findings in this study were derived from the obtained

results from literature, questionnaires, and simulation. Lastly, all of the relevant literature materials that were surveyed were acknowledged in the reference section.

### 3.11 Reliability and Validity

A set of audio data was recorded and used in the experiment to represent actual digital audio data from a cybercrime case scenario. To prove the validity of the study, a number of audio recordings were evaluated through the laboratory experiment and analysis results were produced from the selected open-source tools. The experiment was repeated 4 times and the average of the results was recorded this approach helped in providing a set of reliable results.

### 3.12 Chapter Summary

This chapter has presented the research strategy that was adopted to answer the research questions. Emulation settings and tools that were used have also been discussed in detail. In addition, data collection, analysis methods, tools and techniques, ethical issues, and reliability and validity pertaining to this study have been presented. The next chapter will discuss in details the findings related to each research objective under investigation

# CHAPTER FOUR

# RESULTS AND FINDINGS

## 4.1. Introduction

This chapter presents the findings of the study in relation to the research questions under investigation.The chapter is organized into three parts. The first part presents results with respect to the first research objective in determining open-source forensic tools for digital audio analysis; the second partpresents the results with respect to the computer experiment which aimed at observing different report formats produced from the selected open source tools. The last part presents the findings ofthe devised open standard for reporting the digital audio evidence results by open source tools.All of the findings attempt to answer the associated research questions set out in the introductory chapter.

## 4.2. Determination of Efficient Open-Source Forensic Tools

In the process of determining the efficient open-source tools, the researcher went through a grave survey on different digital forensic analysis tools available for conducting the investigation process. The study involved both commercial and open-source tools that are available and of most use in the market. The process was made possible through the list of available forensic tools and technique catalog provided by the NIST. The goal of this catalog is to provide an ease searchable means for obtaining the tools by calling out the parameters of the desired tool.

### 4.2.1 Mandatory Features for Digital Forensic Tools

With the increase in the importance of digital forensic investigation, numerous software tools have emerged in the market to support the process. For this reason, an investigator should be well informed about the type and appropriate tool to be used for a particular task. Tool selection comes as a great challenge, whereby examiners would need a typology for quantifiable characters for the right tool selection (Kiper & Ph, 2019). The use of unreliable tools for performing analysis of digital audio data may lead to unreliable results and hence jeopardize the whole forensic investigation process. With respect to the main purpose of this study, the tools which were to be selected had to be considered fit for creating forensic reports. Providing a list of tools and picking one from them helps the investigator to simplify the process. SANS institute describes some characteristics of a powerful forensic tool (Cervellone & Student, 2015).

The researcher conducted a systematic literature reviewby analyzing different forensic tools including both commercial and open-source, to obtain the critical features of effective forensic tools in general. To obtain a relevant choice of tool to be used in the study, the researcher evaluated the processing and analyzing capability of open source tools through the existing NIST Computer Forensic tools and techniques catalog which describes the tools by their functionality. The following sub-sections provide mandatory functionalities of a good digital forensic tool.

### 4.3. Selection of Digital Forensic Analysis Tool

The process of selecting the right tool to be used in performing analysis could not be such an easy task without any professional considerations to support the choices of tools. However, the investigators ought to make proper decisions on the type of tool which could match the technical intentions of the tasks to be carried out. Right decisions upon the tool type to be used are accomplished through a series of critical testing and reviewing each tool's performance in analysis. But then, reviewing every tool's functionality was almost impractical considering the scope and time limit for the study. There exists a forensic tool catalog ontology proposed by the National Institute of Standards (NIST CFTC), (Grigaliunas, Toldinas, & Venckauskas, 2017). This technique was introduced and put into practice by NIST so as to ease the tool selection process by organizing 29 forensic functionalities powered by filterable fields based on technical parameters (NIST, 2017), (Kiper & Ph, 2019).However the NIST technique was observed to be too general example, parameters listed in functionality could mean forensic processes instead. To assist the process of specific digital forensic tool selection, this study adopted the ease-to-use typology created by Kiper & Ph, (2019) that facilitated the selection of digital forensic tools based on user-specified attributes.

However, a number of requirements have been adopted from NIST and some requirements are derived from other authors to complete the list of requirements in this research. The literature review found that requirements from NIST research are a standardized approach for disk imaging tools testing. The NIST requirements for forensic tools were also recommended by other authors such as Byers (2008),

Wilsdon & Slay (2014) and Carrier (2002). In accordance with the general objective of this study that was to propose a format that would work with open source tools in the reporting phase, the selection of tools naturally relied on the open-source tools rather than the commercial software tools.

The following factors were considered in order to support the easy selection of open source tools to be used in testing the analysis of the digital audio data, based on the ISO/IEC 9126 standard of qualities of good software as summarized in the Figure 4.1.

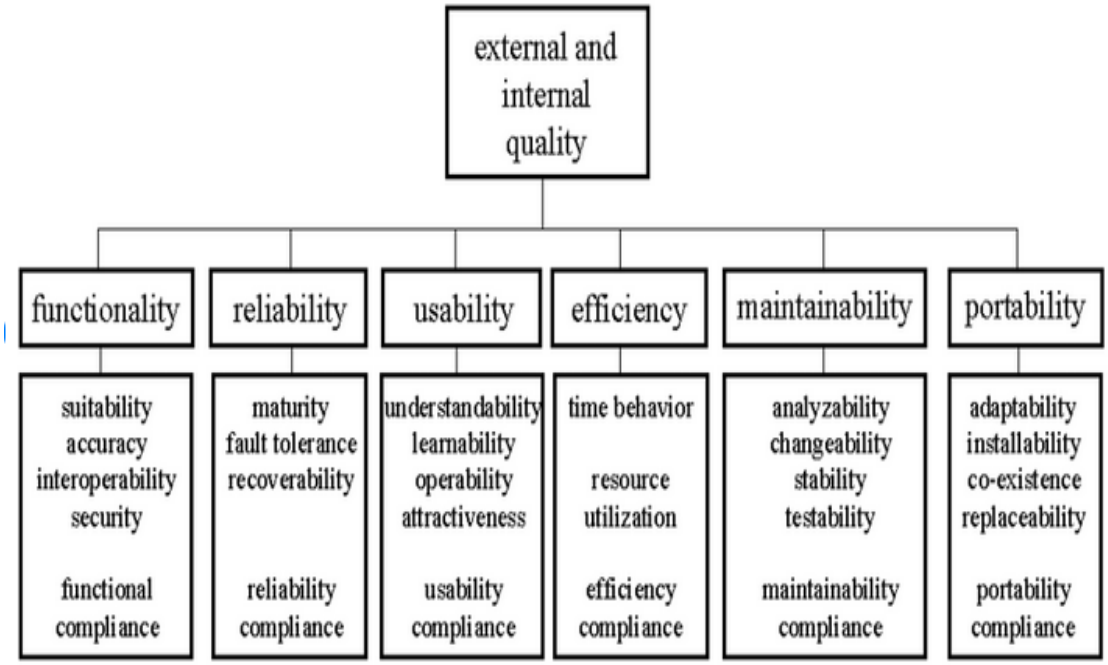


**Figure 4.1: External and Internal Quality Attributes.**

**Source:** Adopted from Dugalic (2012)

### 4.3.1. Functionality

For any software product to be qualified for use, it is expected to maintain every aspect of its performance including accuracy, time, interoperability and security. All of the tools under study were viewed as acceptable tools but to justify this, the researcher with the help of other authors such as Brno (2018) and Ghazinour, Vakharia, Kannaji, & Satyakumar (2017), picked the open-source tools SANS Investigative toolkit and the Autopsy. These tools were proven to have the ability to perform analysis of digital forensic data at nearly all phases of the forensic process. This, therefore, qualified the tools to be used in testing the reporting format suggested in this study.

### 4.3.2. Usability

This is an area of contention which determines the amount of time that an expert is expected to use in learning and understanding to use the software tool. It defines the ability of the user to work with the tool without reviewing its source code, software package or background processes that run hand in hand with the tool. The tools have to present data in a clear format that the investigator should be able to interpret the results correctly. For the case of this study, the researcher adopted the tool rating method by Kiper & Ph, (2019) in the study titled Developing a Practical Typology for Selecting Digital Forensics Tools to obtain the tools which do not require much of expertise in the whole process of examining the evidence data. Together with this, the study also obtained a review of tool descriptions which are provided timely by the www.forensicswiki.org/wiki/Tools. From the analysis made, the study concluded

that the list of appropriate and easy to use open-source tools are Autopsy and SANS investigative toolkit.

### 4.3.3. Reliability

Software reliability defines the possibility of the tool to perform its functions in a free-of-failure state during the analysis of evidence data. Within this criterion, issues of robustness and ability of the tools to perform the desired task within time and with minimum error rate were a focal point of consideration. The researcher picked the tools with maximum capacity to perform multiple tasks, in order to ease the analysis process and also avoiding the use of different tools in performing the forensic process. This was so as to minimize the task of testing the proposed standard in Chapter 5. The viable tools selected for this study were the Autopsy, which was found to have the highest performance and an all in one open-source tool together with the SANS investigative toolkit, which was proven as a very powerful open-source tool that allows integration with other tools (Ghazinour et al., 2017), (Brno, 2018).

### 4.3.4. Portability

The forensic analysis software tools examined under portability were those which were having a multi-platform support and those which were easy to install with minimum number of compatibility requirements. The open-source tools Autopsy and Digital forensic framework contained these features hence suggested as most portable tools that can fit for forensic examination.

The maintainability and efficiency, as suggested by the ISO/IEC 9126 standard, falls within the functionality and usability qualities of good software through their internal attributes. The tool selection process has been summarized in Table

**Table 4.1: Selection of Digital Forensic Analysis Tool**

| CRITERIA | SIFT | AUTOPSY | DFF |
|---|---|---|---|
| **Functionality** | √ | √ | √ |
| **Usability** | √ | √ | √ |
| **Reliability** | √ | √ | √ |
| **Portability** | √ | √ | √ |

According to the survey done on open source tool selection, the results summarized that the tools that could be used during analysis and testing of the proposed format were, therefore, SANS Investigative toolkit and the Autopsy.

Together with the literature review done, the researcher also conducted unstructured interviews with detectives, advocates and state attorneys so as to validate the existence and use of different software tools in the forensic process, corresponding to the research question one. The interviews were aimed at proving the fact that the forensic process has now adopted the use of software tools in processing and presenting digital evidence data in the courtroom. An interview guide was prepared and conducted with 12 state attorneys, 23 advocates, 2 ICT officers from the high court and 4 detectives, making a total of 41 respondents. The population was characterized by the period of experience of respondents in the field of expertise, to obtain reliable answers to the interview questions. The demographic character of the

population was sufficient as it had the ability to satisfy the purpose of this research question since a large portion of respondents included the law practicing experts (Landeta, Barrutia, & Lertxundi, 2011).

### 4.4. Reporting Formats for Digital Audio Analysis by the Autopsy

The Autopsy forensic browser was selected as a tool to be used to analyze a set of digital audio data. A current version of autopsy 4.2.0 was downloaded into a local machine and installed from its official site http://sleuthkit.org/autopsy/download.php. The software was then automatically made accessible to run from the local computer's desktop or start menu. A flash disk containing different audio data was analyzedandthe final report produced was in three different formats including the HTML, Excel and Basic file format. The Figure 4.2 shows the autopsyuser interface after installation on a windows platform.

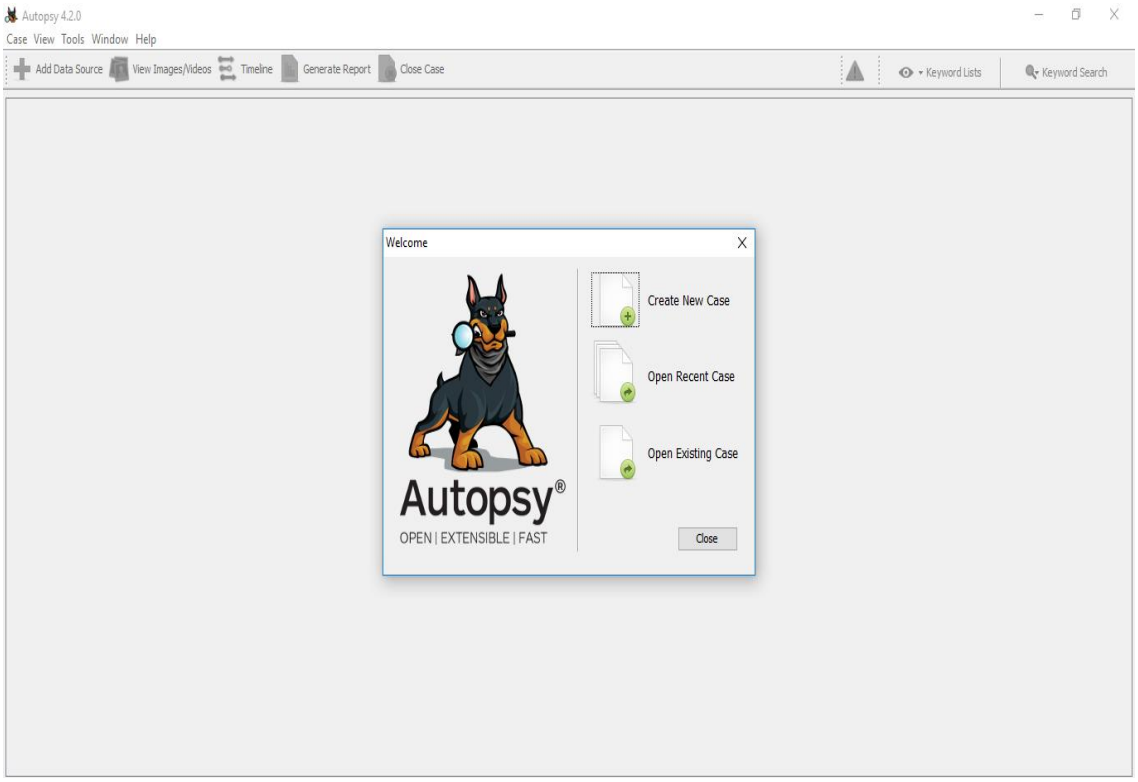


**Figure 4.2: The Autopsy Forensic Browser Interface**

**Source**: (Researcher,2019)

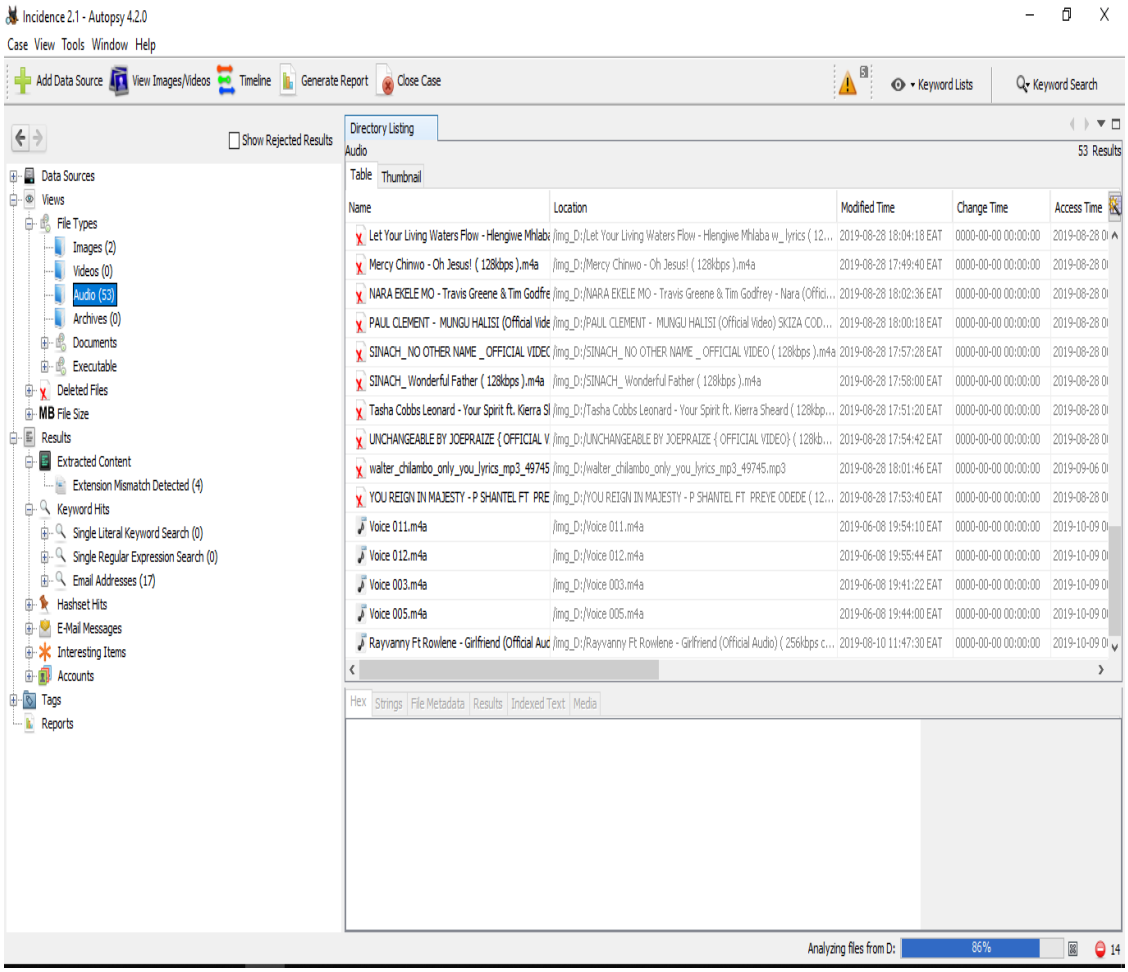


**Figure 4.3: Audio Analyses with Autopsy Forensic Browser**

**Source:** (Researcher,2019)

After the analysis process as demonstrated in Figure 4.3, the forensic report was requested in at least three formats which would give details on the analyzed evidence. The reporting module contains seven different formats for presenting the results obtained from the analysis done. The existence of more than one format gives the investigator a wider chance of choice of report depending on use.Figure 4.4 shows the options available in the reporting module.

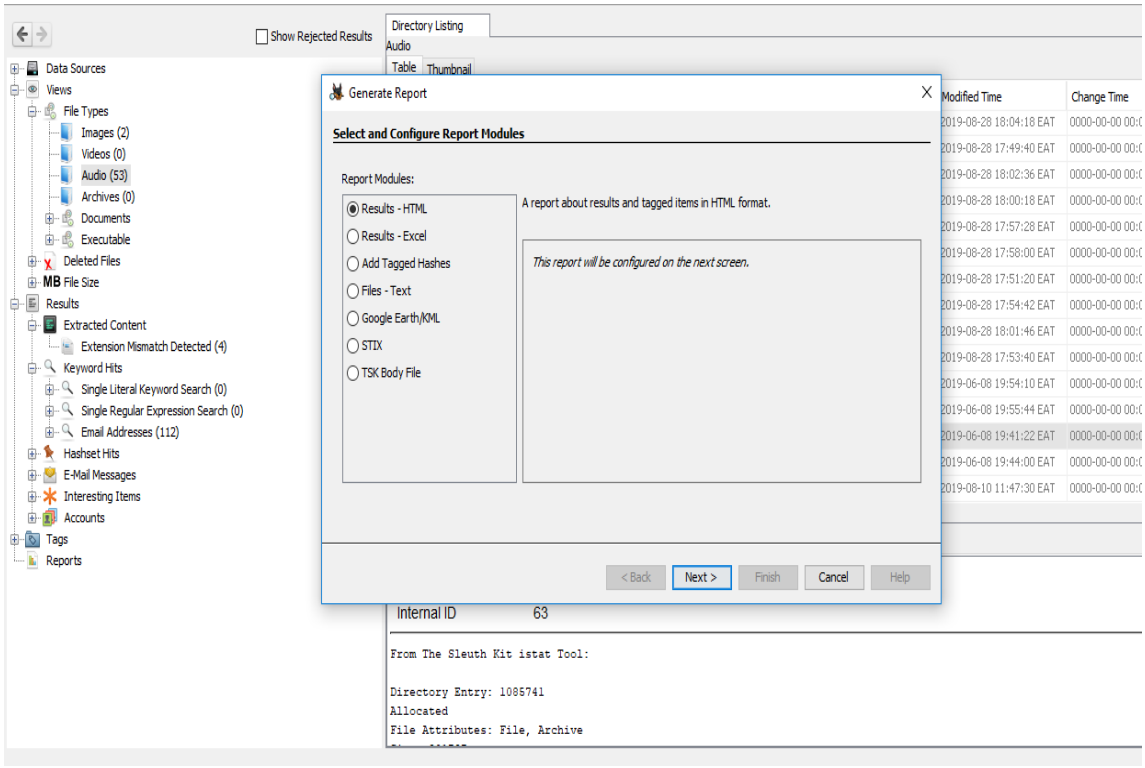


**Figure 4.4: Reporting Module of the Autopsy Forensic Browser**

The reporting module finally produced three different outputs pertaining to the digital audio input. The results were presented in HTML, Excel and Basic file format reports as presented in Figure , Figure 4.6 and Figure 4.7.

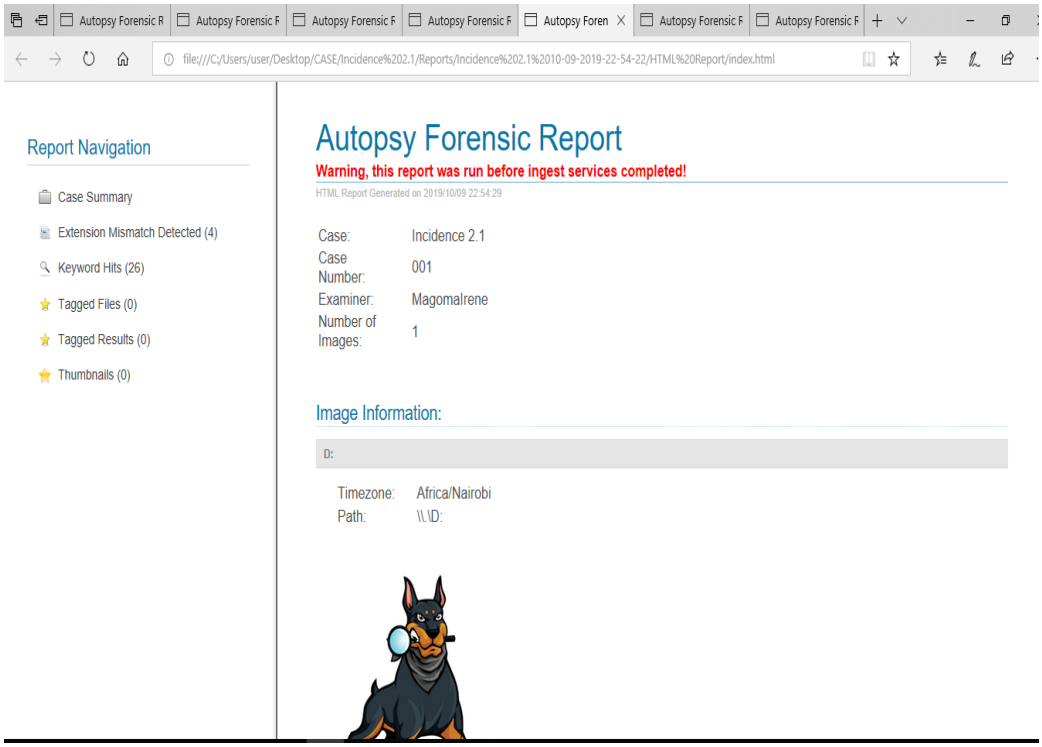


**Figure 4.5: HTML Report from Autopsy Forensic Browser**

```
Ebezina _ Preye ( 128kbps ).m4a .m4a    r       yes     2019-08-28 00:00:00 EAT 2019-08-28 17:47:22 EAT 2019-08-28 17:47:48 EAT 4441165 189     8a63d1dd3b4dd52089ba3a3e
Ebony - Date Your Father Official Video ( 128kbps ).mp3 .mp3    r       yes     2019-09-06 00:00:00 EAT 2019-08-28 17:47:46 EAT 2019-08-28 17:48:04 EAT 3256158 195
Excess Love - Mercy Chinwo (Official Video) ( 256kbps cbr ).mp3 .mp3    r       yes     2019-09-06 00:00:00 EAT 2019-08-28 17:57:59 EAT 2019-08-28 17:59:06 EAT 1269209
God of everything by Viwe Nikita ( 128kbps ).m4a        .m4a    r       yes     2019-08-28 00:00:00 EAT 2019-08-28 17:52:38 EAT 2019-08-28 17:53:10 EAT 5826908 206
I STILL BELIEVE ( 128kbps ).m4a .m4a    r       yes     2019-08-28 00:00:00 EAT 2019-08-28 17:45:29 EAT 2019-08-28 17:45:50 EAT 4002432 210     ff3217f435c320ef1b7f2591
Innoss'B - Yo Pe (Official Video) ( 128kbps ).m4a       .m4a    r       yes     2019-08-28 00:00:00 EAT 2019-08-28 17:43:23 EAT 2019-08-28 17:43:48 EAT 4471444 215
Intentional video lyrics by Travis Greene ( 128kbps ).m4a       .m4a    r       yes     2019-08-28 00:00:00 EAT 2019-08-28 17:48:04 EAT 2019-08-28 17:48:24 EAT 3453911
joel_lwaga_feat._chris_shalom_umejua_kunifurahisha_official_video_mp3_35616.mp3 .mp3    r       yes     2019-09-06 00:00:00 EAT 2019-08-28 18:01:45 EAT 2019-08-28 18:02
Let Your Living Waters Flow - Hlengiwe Mhlaba w_ lyrics ( 128kbps ).m4a .m4a    r       yes     2019-08-28 00:00:00 EAT 2019-08-28 18:03:53 EAT 2019-08-28 18:04:18 EAT
Mercy Chinwo - Oh Jesus! ( 128kbps ).m4a        .m4a    r       yes     2019-08-28 00:00:00 EAT 2019-08-28 17:49:04 EAT 2019-08-28 17:49:40 EAT 6572472 241     2d923d2b
NARA EKELE MO - Travis Greene & Tim Godfrey - Nara (Official Video) ( 128kbps ).m4a     .m4a    r       yes     2019-08-28 00:00:00 EAT 2019-08-28 18:02:11 EAT 2019-08-
PAUL CLEMENT -  MUNGU HALISI (Official Video) SKIZA CODE 7473184 ( 128kbps ).m4a        .m4a    r       yes     2019-08-28 00:00:00 EAT 2019-08-28 17:59:53 EAT 2019-08-
SINACH_ NO OTHER NAME _ OFFICIAL VIDEO ( 128kbps ).m4a  .m4a    r       yes     2019-08-28 00:00:00 EAT 2019-08-28 17:56:56 EAT 2019-08-28 17:57:28 EAT 5644397 1085703
SINACH_ Wonderful Father ( 128kbps ).m4a        .m4a    r       yes     2019-08-28 00:00:00 EAT 2019-08-28 17:57:27 EAT 2019-08-28 17:58:00 EAT 6021378 1085708 62e832f0
Tasha Cobbs Leonard - Your Spirit ft. Kierra Sheard ( 128kbps ).m4a     .m4a    r       yes     2019-08-28 00:00:00 EAT 2019-08-28 17:50:38 EAT 2019-08-28 17:51:20 EAT
UNCHANGEABLE BY JOEPRAIZE { OFFICIAL VIDEO} ( 128kbps ).m4a     .m4a    r       yes     2019-08-28 00:00:00 EAT 2019-08-28 17:54:09 EAT 2019-08-28 17:54:42 EAT 6255925
walter_chilambo_only_you_lyrics_mp3_49745.mp3   .mp3    r       yes     2019-09-06 00:00:00 EAT 2019-08-28 18:01:24 EAT 2019-08-28 18:01:46 EAT 3975397 1085726 289f7ea0
YOU REIGN IN MAJESTY - P SHANTEL FT  PREYE ODEDE ( 128kbps ).m4a        .m4a    r       yes     2019-08-28 00:00:00 EAT 2019-08-28 17:53:08 EAT 2019-08-28 17:53:40 EAT
SPECS PRINTER.docx      .docx   r       yes     2019-09-06 00:00:00 EAT 2019-09-06 08:23:36 EAT 2019-09-06 08:20:32 EAT 15732   1085735 d3ad4ba2fd54bdb3ceca3406c6d03241
Voice 011.m4a   .m4a    r               2019-10-09 00:00:00 EAT 2019-10-09 19:00:39 EAT 2019-06-08 19:54:10 EAT 544297  1085737 8ad4f990a013634cc468e4f9e5fe1c82
Voice 012.m4a   .m4a    r               2019-10-09 00:00:00 EAT 2019-10-09 19:00:46 EAT 2019-06-08 19:55:44 EAT 1289231 1085739 65fef9d2fb6ebd9f45fdc44a83303b80
Voice 003.m4a   .m4a    r               2019-10-09 00:00:00 EAT 2019-10-09 19:00:49 EAT 2019-06-08 19:41:22 EAT 801797  1085741 7c33b2ad9fc7aa28ccf169dcd56ad616
Voice 005.m4a   .m4a    r               2019-10-09 00:00:00 EAT 2019-10-09 19:00:50 EAT 2019-06-08 19:44:00 EAT 447080  1085743 9ce2c2dc981dbcc3a181c7b354dde671
Rayvanny Ft Rowlene - Girlfriend (Official Audio) ( 256kbps cbr ).mp3   .mp3    r               2019-10-09 00:00:00 EAT 2019-10-09 19:06:16 EAT 2019-08-10 11:47:30 EAT
Iren Proposal 4...docx  .docx   r       yes     2019-10-09 00:00:00 EAT 2019-10-09 19:10:53 EAT 2019-04-08 08:46:08 EAT 215610  1085753 b48e6e5c3bba64d5724f2e4813af828c
$MBR            v               0000-00-00 00:00:00     0000-00-00 00:00:00     0000-00-00 00:00:00     512     502791187       ce9aeeb09e4378bd9a7fcd302f7b957b
$FAT1           v               0000-00-00 00:00:00     0000-00-00 00:00:00     0000-00-00 00:00:00     7856128 502791188       231d6a255dbf2a37ae60b01b959dc1dc
$FAT2           v               0000-00-00 00:00:00     0000-00-00 00:00:00     0000-00-00 00:00:00     7856128 502791189       231d6a255dbf2a37ae60b01b959dc1dc
3BC1875^.^^^    .^^^    r       yes     0000-00-00 00:00:00     0000-00-00 00:00:00     0000-00-00 00:00:00     33554432        68573971        5db2ed0dcd0ac28f6b55da77
3BC9075^.^^^    .^^^    r       yes     0000-00-00 00:00:00     0000-00-00 00:00:00     0000-00-00 00:00:00     33554432        68575651        5db2ed0dcd0ac28f6b55da77
3BC0875^.^^^    .^^^    r       yes     0000-00-00 00:00:00     0000-00-00 00:00:00     0000-00-00 00:00:00     33554432        68577363        5db2ed0dcd0ac28f6b55da77
3BC1075^.^^^    .^^^    r       yes     0000-00-00 00:00:00     0000-00-00 00:00:00     0000-00-00 00:00:00     33554432        68577427        5db2ed0dcd0ac28f6b55da77
3BC2075^.^^^    .^^^    r       yes     0000-00-00 00:00:00     0000-00-00 00:00:00     0000-00-00 00:00:00     33554432        68577436        5db2ed0dcd0ac28f6b55da77
og^0^^^^.^^^    .^^^    r       yes     1985-08-12 00:00:00 EAT 0000-00-00 00:00:00     0000-00-00 00:00:00     410648576       77802483        b6df57e2eb65df518732b549
SETUP.CFG       .CFG    r       yes     2015-07-10 00:00:00 EAT 2015-07-10 17:01:16 EAT 2015-07-10 17:01:16 EAT 5390    112718118       96ce5ecd469f69313a67084c5d8f7d6e
IMAGIN~0.DLL    .DLL    r       yes     2015-07-10 00:00:00 EAT 2015-07-10 17:01:16 EAT 2015-07-10 17:01:16 EAT 214368  112718627       512992a9264b7b1a9f28c810b74a8486
```

**Figure 4.6: Text File Report from TheAutopsy Forensic Browser**

| | A | B | C | D | E | F |
|---|---|---|---|---|---|---|
| 1 | Summary | | | | | |
| 2 | | | | | | |
| 3 | Case Name: | Incidence 2.1 | | | | |
| 4 | Case Number: | 001 | | | | |
| 5 | Examiner: | MagomaIrene | | | | |
| 6 | Number of Images: | 1 | | | | |
| 7 | | | | | | |
| 8 | | | | | | |
| 9 | | | | | | |
| 10 | | | | | | |
| 11 | | | | | | |

**Figure 4.7 Excel Report Format from Autopsy Forensic Browser**

### 4.5. Standardization Format for Reporting Digital Evidence Data

It has been proven by different authors such asBariki, Hashmi, & Baggili (2014) that the existence and use of more than one tool in performing analysis in the forensics process has eased the task for examiners although on the other hand causing mismatch of results. This was viewed as a major problem especially to the small law practitioners who have limited access to commercial all-in-one tools. This has therefore hindered the proper handling of digital-related cases. To minimize the problem, this study proposed a format that is to be adhered to during the presentation of digital audio data.In this study, the researcher used the criteria of the ISO/IEC 27037 standard which tells important details of a proper tool and that of Bariki, Hashmi, & Baggili (2014)who created a format for commercial tools and tested it on the Encase tool. List of important criteria that a forensic report requires include the details on the chain of custody. Chain of custody is the most critical and important aspect when handling any evidence item for presentation in the court by ensuring the originality of evidence data. Just like it is handled with other categories of physical crime, chain of custody also applies in the digital related crimes. There is no a common standard across the world for presenting a report on the crime as every country differs with how they need the evidence to be documented(Ratnasari, Devi and Prayudi, Yudi and Sugiantoro, 2018) However, any report on digital evidence data should at least contain the “5Ws and 1H” information on Who, What, When, Where, Why and How, meaning a person who handles the evidences, type of evidence collected time of analysis, method or tool used in analysis and storage

location (Bariki et al., 2014 &Ratnasari, Devi and Prayudi, Yudi and Sugiantoro, 2018).

The following were the list of criteria that defined the standardization format.

i. **Name:** This describes the name of the forensic examiner who is responsible for running the analysis of the evidence data
ii. **File Type:** This defines the type of data that was examined by the tool used during the analysis process
iii. **Date:** This part determines when the digital audio data was examined
iv. **Altered:** Thispart will reveal whether there was some missing data when handled for analysis. If the evidednce data was altered, it defines also the date of alteration
v. **Deleted:**This field represents all necessary information for the evidence data whether deleted or not, and if yes, date of deletion
vi. **File Size:** This part contains the details on the size of the data file that was processed
vii. **Hash Value:** This part describes the hash function calculated so as to prove the integrity of the data
viii. **Full path:** This provides the full address path of file to enable traceability.
ix. **Tool:** this part will define the type of tool that was used during the analysis process.

The defined criteria were then used to determine the correctness of the evidence report which contains all the important details representing the entire chain of custody details. Together with the definition of the important details for chain of

custody in the forensic report, the researcher devised an XML schemer which carries the defined criteria. The XML language was used due to its unique feature extensibility and flexibility and that it can be used crossplatform.

The schemer contains three distinct classes, thet are Case information, Evidence information and the Investigator's details. The Case information carries a brief summary of the case including the following elements; case name and number, date of receiving the case, name of the tool used and the investigator. The (tns:investigatorDetails) on the Investigator element, retrives the investigator details from the Investigator class.

The EvidenceItemInformation class, carries the defined elements that are a proposed standard for reporting audio forensic evidence. The last part is the investigator class, which carries investigator's name, address, phone number, email and investigator's comments.The Figure 4.8 is a screenshot of the proposed reporting format, expressed in an XML schemer

```
−<xsd:schema elementFormDefault="qualified" targetNamespace="http://xml.netbeans.org/schema/forensicReportXmlSchema">
  −<xsd:element name="DigitalEvidenceItem">
    −<xsd:complexType>
      −<xsd:sequence>
        −<xsd:element name="CaseInformation">
          −<xsd:complexType>
            −<xsd:sequence>
                <xsd:element name="CaseNumber" type="xsd:int"/>
                <xsd:element name="CaseName" type="xsd:string"/>
                <xsd:element name="CaseDescription" type="xsd:string"/>
                <xsd:element name="ReportCreatedDate" type="xsd:dateTime"/>
                <xsd:element name="ForensicToolNameAndVersion" type="xsd:string"/>
                <xsd:element name="Investigator" type="tns:InvestigatorsDetails"/>
              </xsd:sequence>
            </xsd:complexType>
          </xsd:element>
        −<xsd:element name="EvidenceItemInformation">
          −<xsd:complexType>
            −<xsd:sequence>
                <xsd:element name="FileName" type="xsd:string"/>
                <xsd:element name="FileType" type="xsd:string"/>
                <xsd:element name="DateReceived" type="xsd:dateTime"/>
                <xsd:element name="IsAltered" type="xsd:boolean"/>
                <xsd:element name="DateAltered" type="xsd:dateTime"/>
                <xsd:element name="IsDeleted" type="xsd:boolean"/>
                <xsd:element name="DateDeleted" type="xsd:dateTime"/>
                <xsd:element name="FileSize" type="xsd:string"/>
                <xsd:element name="HashValue" type="xsd:string"/>
                <xsd:element name="FullPath" type="xsd:string"/>
                <xsd:element name="ToolName" type="xsd:string"/>
              </xsd:sequence>
            </xsd:complexType>
          </xsd:element>
        </xsd:sequence>
      </xsd:complexType>
    </xsd:element>
  −<xsd:complexType name="InvestigatorsDetails">
    −<xsd:sequence>
        <xsd:element name="Name" type="xsd:string"/>
        <xsd:element name="Agency" type="xsd:string"/>
        <xsd:element name="Address" type="xsd:string"/>
        <xsd:element name="Phone" type="xsd:string"/>
        <xsd:element name="Fax" type="xsd:string"/>
        <xsd:element name="Email" type="xsd:string"/>
        <xsd:element name="Comments" type="xsd:string"/>
      </xsd:sequence>
    </xsd:complexType>
  </xsd:schema>
```

**Figure 4.8 XML Schemer for the Proposed Format**

# CHAPTER FIVE

# DISCUSSION OF THE RESULTS

## 5.1. Introduction

This chapter concentrates on the discussion of the findings as presented in chapter four. The discussion is aligned with respect to the specific objectives of this study and aiming to answer research questions.

## 5.2. Digital Forensic Analysis Tools Selection Results

With respect to objective one which aimed at determing a proper set of tools that would assist in the process of testing the proposed standardization format of reports presentation. The researcher conducted a study of different exiting tools both off the shelf and commercial tools that are commonly used in the process of analyzing digital evidence data by the forensic experts. The survey of both types was done for the interest of gaining general features for a good quality tool since most of them have recurring features. Different characteristics and capabilities of the tools were examined in order to verify the selection process. With a guidance of criteria defined by the ISO/IEC 9126 standard of good qualities of software tools, the selection process was made. The study found that upon the available tools, it was useful to select the open-source tools so as to ease the accessibility of these tools in achieving the last objective. The researcher picked the autopsy browser among the tools, which would perform analysis of audio data, and thereafter produce a report of a standardized format.

However, upon the tool selection process, it was also necessary to verify the applicability of more than one tool by forensic examiners during the analysis process of digital data. This was aimed at proving the existence of none uniformity of digital audio evidence results in the final report formation. The researcher conducted a survey through interviews with a defined expertise population which proved the existence and use of these tools.

### 5.2.1. The Working Experience of Respondents

The researcher examined the period of the work experience of all respondents who were to take part in this study; the aim was to understand their awareness on the software tools. The results were summarized in Table 5.1.

**Table 5.1: Respondents Working Experience**

| Years of experience | Respondents | Percentage (%) |
|---|---|---|
| Less than 1 year | 4 | 10 |
| Between 1 and 5 years | 23 | 56 |
| Above 5 years | 14 | 34 |
| Total | 41 | 100 |

A plot for Table that described the period of working experience of the respondents was depicted in a pie chart in Figure so as to provide an easy clear presentation. The results show that 10% of the total population had less than 1 year of working experience, which represented 4 people, while 56% of the population which was 23 respondents had worked in the field for between 1 and 5 years. The rest of the population which covered 34% that was 14 people, were more experienced in the field having worked for above 5 years in their professions.

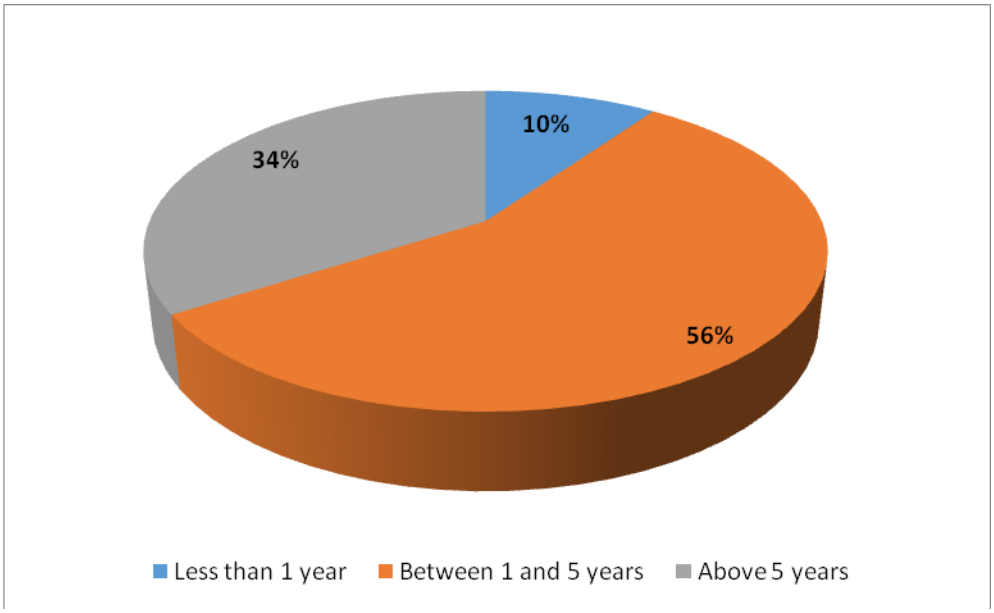


**Figure 5.1: Working Experiences of Respondents**

### 5.2.2. The Use of More Than One Forensic Tool for Analysis

Analysis was done on the use of more than one digital forensic analysis tool for processing evidence data, the results obtained were then graphically presented as follows

**Table 5.2: Response for Application of More Than One Digital Forensic Analysis Tool**

| Response | Frequency(N) | Percentage (%) |
|---|---|---|
| Strongly agree | 10 | 24 |
| Agree | 26 | 63 |
| Neutral | 4 | 10 |
| Disagree | 1 | 3 |
| Strongly disagree | 0 | 0 |
| Total | 41 | 100 |

The results upon the application of more than one digital forensic tool to analyze digital evidence data represented in Table 5.2 show that 24%, that was 10 respondents strongly agreed to the fact that digital forensics analysis is conducted by more than one tool and 63% of the population which is equal to 26 people also agreed upon this fact. However, 10% of the respondents that were a total of 4 people were not aware of the application and use of these tools while 3% that is one person and none disagreed with this. From this analysis, it is vivid that there is an existence of use of more than one digital forensic analysis tool in the investigation process; hence resulting in non-uniform reports produced which becomes ambiguous during the presentation of evidence data in the courtroom. This makes it difficult to prove the integrity of the evidence data when brought for justification. The results were depicted graphically as in Figure 5.2.

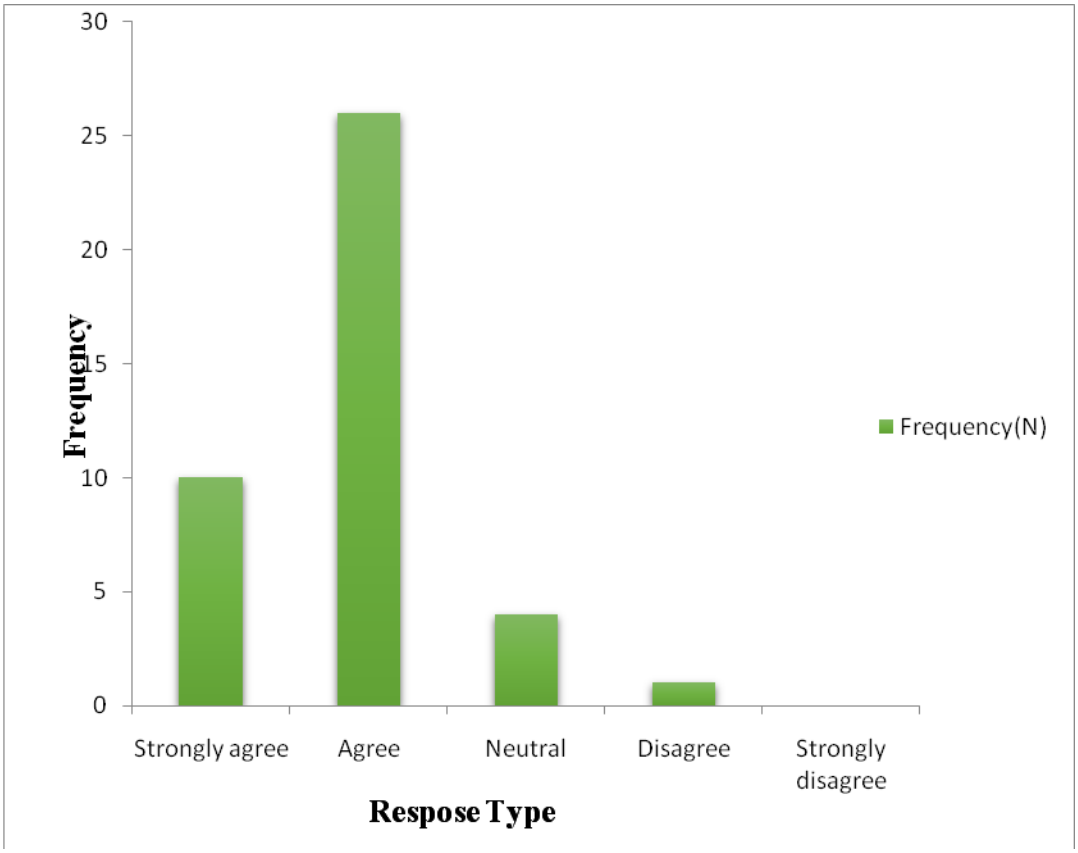


**Figure 5.2. Response for Application of More Than One Forensic Tool**

From the above analysis, the study indicates that the tools which were fit for the analysis process during the testing of the proposed standard were the SIFT and autopsy. From this result, the researcher picked the autopsy forensic browser which works in coordination with the sleuth kit. Since both tools had the same capabilities, the researcher had to select one between the two, so as to run data analysis.

This analysis made, therefore, answered the research que

stion one which required determining the effective and most used tools, and later selecting an open-source out of the reviewed tools. With the help of responses from different groups of people, the researcher was able to verify the results obtained from

the literature review done.

### 5.3. Testing the Autopsy tool for ReportingDigital Audio Analysis.

The computer experiment involved the use of a storage device; that was a flash disc, voice recorder and desktop computer installed the selected analysis software tool. The researcher acquired audio data through a voice recorder. The data was then stored in a flash drive and later analyzed through the autopsy forensic browser installed in a desktop Computer. The specifications of devices involved in the experiment were as follows.

#### i. Sound Recorder

An application from a Samsung S6 mobile phone 32 GB internal storage

#### ii. Flash Disk

A SanDisk flash with 16 GB storage capacity

#### iii. Desktop Computer

RAM 4 GB

Processor Intel Core i5

Windows 10/64bits OS

#### iv. The Autopsy Forensic Browser

The autopsy Version 4.2.0, an extension of the Sleuth kit.

Inorder to perform testing, the researcher recorded a set of four different audio data and stored them in an external flash drive. The audio data were used as inputs

imitated from real data. Forensic analysis was done for the audio inputs through the autopsy forensic browser. The aim was to examine the analysis done and the output produced in the autopsy reporting module. The analysis results proved the differences in output formats whereby the HTML report provided a user-friendly view of the results including the case name, type, investigator information, tool type and evidence information. The excel report only produced a summary of the case information. It produced the case name, case number, investigators name and the number of files. The basic file format displaed a number of evidence items which were ambiguous in their presentation.Theoutputs were produced by the selected forensic tool, and the results were recorded and presented. From the analysis made, the researcher concluded the Autopsy browser with the help of the Slethkit, produce a reports in different formats for the audio evidence data. Although the HTML format is seento have a graphical user interface, yet it does not carry all necessary details of the data. This therefore raises a need for a defined format that would carry all needed details for a digital audio forensic case.

### 5.4. A Standardization Format for Reporting Digital Evidence Data

With respect to the second objective, the studyrequired proposing a format that would be a standard for all reporting documents needed to present evidence data in the court. The researcher, in order to answer the second research question, made a thorough survey to obtain the needs for a forensic report. Through a documentary review, the researcher revealed the critical features of an authentic report that it requires all necessary chain of custody elements. The digital chain of custody requires information about the evidence data from its acquisition to presentation

state in order to easily identify any alteration which would result in loss of integrity. From a survey by other scholars, the researcher study formed a defined list of important fields that should be contained in a forensic report.

The results from a survey done by the researcher was a set of criteria expressed in an XML schemer which represents the necessary chain of custody elements for reporting digital audio evidence data. The elements defined for the standardization format are the file name, date, altered, file size, hash value, full file path, hash value and tool name. A compinatioin of these details, describes a chain of custody which was discussed in the Chapter 4 that it is the basic element for a digital report. This therefore,answered the the third objective which required a format for reporting the digital audio evidence data.

# CHAPTER SIX

# SUMMARY, CONCLUSION AND RECOMMENDATION

## 6.0 Introduction

This chapter carries a summary for the study, conclusions based on the findings presented and discussed in chapter five; recommendations and areas that may need further research.

## 6.1 Summary of the Study

The motive for this study was to propose a reporting format for digital audio evidence data that is analyzed by open source tools. The study went by three objectives, which were respectively answered by three research questions namely; (i) What are the most effective open-source forensic tools for audio analysis? (ii) How does the selected open-source forensic tools repot the audio analysis results? and (iii) Which open standard can be devised for ensuring the correlation of audio evidence reports.The study has applied an emulation computer experiment design and documentary review techniques to collect both the quantitative and qualitative data for achieving the mentioned objectives. The analysis made towards achieving each study objective were as follows;

Questionnaires were provided to a sampled portion of law practicing bodies and other professionals, towards proving the applicability of forensic software tools. This went hand in hand with a study of different tools used in the market, whereby the results answered the first research question. A majority of the population agreed to the availability and use of different forensic tools for the analysis process. From a critical

literature review, a tool selection was made, and the autopsy browser was agreed to be used during the computer experiment.

Secondly, the selected Autopsy browser for sleuth toolkit was tested through analyses of different audio data to produce reports in accordance to the existing reporting modules. A set of four different audio data was run through analysis by this tool and different reports were created for each. Although the tool carries seven different reporting styles, the researcher concentrated on three major reporting styles of this tool that supported audio data including the HTML, Excel and Text File. Results from the analysis was that a single audio data could proiduce three different reports which do not fully match in their contents. This practice helped to answer the second research question.

Again, through literature review, the researcher identified the features of a good report. From a group of other scholars, it was identified that any digital forensic report should not miss the digital chain of custody items of who, what, why, when, where and how. Therefore, a standard for audio forensic report was derived from those features. The final output was an XML format which contains the defined criteria for a standard digital audio evidence report. This went and answered the third research question.

## 6.2 Conclusion

Based on the study findings and analysis made the conclusions discussed hereunder are pertinent.

i. The forensic tools available in the market perform analysis of digital data .the researcher observed that most of the tools are designed for performing file, memory and network analysis rather than multimedia. A majority of tools

especially the open-source has definite support for performing analysis of media data and this is due to latency in multimedia related crimes reported.

ii. In Tanzania, many people are not aware of the importance and power of cyber act which serves the purpose of digital-related crimes. Due to his, the researcher experienced hardship in obtaining clear details and sample cases which involve digital audio evidence since the cases of this nature are merely reported.

## 6.3 Recommendations

Based on the study results and conclusion made, the study recommends the following.

First, to the law practitioners and legal-related bodies, it is necessary to promote the use of forensic tools in analyzing digital related crimes. This will help them to obtain a smart business process as the cases will be handled at the highest level of integrity of the evidence data. This will ensure little or close to no occurrence of fraud.

Secondly, to the group of cyber investigators and legal bodies, it is quite important to define and formalize a common way of presenting the final data analyzed by any type of tool both commercial and open source. The proposed format from the study can be considered and adopted by the legal framework in reporting evidence data in the courtroom.

Lastly, the researcher recommends the use of the sleuth kit together with autopsy forensic browser open-source tools in the practice of investigation for digital audio data. This is because it is user friendly and has strong capability close to the trusted commercial tools.

## 6.4 Future Work

Together with the study conclusion and recommendations made, still there is a need for conducting further research on the following, as related to the study.

i. Further research should be done on the digital forensic tools, to determine the key framework for digital forensic analysis process. It is important to determine a common forensic framework since it is a baseline for practicing any digital-related investigation.

ii. Moreover, here is a need for study for other classes of cybercrime dominant in Tanzania such as network fraud to mitigate security issues especially on social media.

iii. Future scholars can go further in implementing and testing the proposed reporting standard in the open source tools since it is designed in an XML format which is extensible and portable to embade in any other tool.

## REFERENCES


Ambhire, V. R. (2012). *Digital Forensic Tools*, *2*(3), 392–398.

Anson, S., & Bunting, S. (2007). *Mastering Windows Network Forensics and Investigation*. sybex.

Baggili, I. (2010). *Digital forensic and cyber crime*. .Abu Dhabi United arabs emirates: springer.

Bariki, H., Hashmi, M., & Baggili, I. (2014). D*efining a Standard for Reporting Digital Evidence Items in Computer Forensic Tools Defining a Standard for Reporting Digital Evidence Items*, (October 2010). https://doi.org/10.1007/978-3-642-19513-6

Brenner, S. W. (2001). State Cybercrime Legislation in the United States of America: A Survey. *Richmond Journal of Law and Technology*, *7*(3). Retrieved from http://scholarship.richmond.edu/jolt%0Ahttp://scholarship.richmond.edu/jolt/vol7/iss3/4%0Ahttp://www.richmond.edu/jolt/v7i3/article2.html.

Brno, S. (2018). *Tool for forensic analyses of digital traces.*

Byers, D. (2008). Disk Imaging Evaluation: Encase 6 . 8 / LINEN 6 . 1, (October).

Carrier, B. (2002). Open Source Digital Forensics Tools. *Analysis*, (October 2002), 1–11. Retrieved from http://www.digital-evidence.org/papers/opensrc_legal.pdf

Carrier, B. (2003). Defining digital forensic examination and analysis tools using abstraction layers. *International Journal of Digital Evidence*, *1*(4), 1–12. https://doi.org/10.1017/CBO9781107415324.004

Cervellone, A., & Student, G. (2015). *A Comparison of Computer Forensic Tools*: An Open-Source Evaluation, 1–30.

Cino, J. G. (2017). An uncivil action: *criminalizing*, 651–709. council of europe cybercrime project. (2016). The state of cybercrime legislation in Africa – an overview Introduction: Why should countries of Africa legislation on cybercrime and electronic evidence? adopt A legal framework on cybercrime and electronic evidence: what is required?, (May 2015), 1–9.

Daniels, D. J., & Hart, S. V. (2013). Forensic Examination of Digital Evidence: A Guide for Law Enforcement.

Douglas, K. (2015). Digital computing , modelling and simulation Kirsty Douglas Working paper Final, (April). european commission. (2017). EU cybersecurity initiatives.

Ghazinour, K., Vakharia, D. M., Kannaji, K. C., & Satyakumar, R. (2017). A Study on Digital Forensic Tools. *2017 IEEE International Conference on Power, Control, Signals and Instrumentation Engineering (ICPCSI)*, 3136–3142.

Grigaliunas, S., Toldinas, J., & Venckauskas, A. (2017). An Ontology-Based Transformation Model for the Digital Forensics Domain, 78–82.

Hanson, S. (2014). Computer Forensics: Investigations of the Future.

Huber, D., & Runstein, R. (2018). Digital Audio Technology.*Modern Recording Techniques*, 195-217. https://doi.org/10.4324/9781315666952-6

Ips, M. (2018). Electronic Evidence: Collection , Preservation and Appreciation Outline of My Presentation.

Kalaimannan, E., & Florida, W. (2015). Smart Device Forensics - Acquisition , Analysis and Interpretation of Digital Evidences, 838–839. https://doi.org/10.1109/CSCI.2015.58

Kashililah, T. (2015). Tanzania Cybercrimes Act, 2015. *May-2015*, *96*(14), 25–26. Retrieved from https://rsf.org/sites/default/files/the_cyber_crime_act_2015.pdf

Kiper, J. R. R., & Ph, D. (2019). *Information Security Reading Room Pick a Tool , the Right Tool*: Developing a Practical Typology for Selecting.

L.Ramadhani, A. (2017). computerization of judiciary.

Landeta, J., Barrutia, J., & Lertxundi, A. (2011). Technological Forecasting & Social Change Hybrid Delphi: A methodology to facilitate contribution from experts in professional contexts. *Technological Forecasting & Social Change*, *78*(9), 1629–1641. https://doi.org/10.1016/j.techfore.2011.03.009

Lunker, M. (2009). Cyber Laws: A Global Perspective. *Manishl@ India. Com*.

Makadya, B. H. (2011). *MKANDYA_B*. Open University of Tanzania.

Makulilo, B. A. (2016). *The admissibility of electronic evidence in Tanzania*: new rules and case law, *13*.

Makulilo, B. A. B. (2018). *The admissibility and authentication of digital evidence in Zanzibar under the new Evidence Act*, *15*(3).

Mchaney, R. (2009). *Understanding Computer Simulation*.

Mohammed, H. (2016). *An Automated Approach for Digital Forensic Analysis of Heterogeneous Big Data An Automated Approach for Digital Big Data*, *11*.

Nelson, B., Philips, A., & Steuart, C. (2010). *Guide to computer forensics and investigations* (3rd ed.).

NFSTC. (2008). *A Simplified Guide To Digital Evidence*. Largo, Florida 33777.

Nfuka, E. N., Sanga, C., & Mshangi, M. (2014). *The Rapid Growth of Cybercrimes Affecting Information Systems in the Global: Is this a Myth or Reality in Tanzania?*, *3*(2), 182–199.

NICE. (2018). *National Institute for Health and Care Excellence Evidence Standards Framework For Digital*, (December), 1–29.

Norden, S. (2013). How the Internet has Changed the Face of crime. *Gateway Journalism Review*, *41*, 20. Retrieved from http://search.proquest.com/docview/890514694?accountid=14549%5Cnhttp://hl5yy6xn2p.search.serialssolutions.com/?genre=article&sid=ProQ:&atitle=How+the+Internet+has+Changed+the+Definition+of+%22Journalist%22&title=Gateway+Journalism+Review&issn=&date=2011-0

Omolayeba-Ajileye, A. (2011). *Admissability of electronic evidence in civil and criminal proceedings*, 1–32.

Ratnasari, Devi and Prayudi, Yudi and Sugiantoro, B. (2018). XML Approach for the Solution of Chain of Custody of Digital Evidence. *International Journal of Computer Applications*, *179*, 20–25.

SANS Investigative Forensics Toolkit Documentation. (2017).

Smith, J. (2017). *Criminal Evidence: Expert Testimony*, *702*(August), 1–56.

Sonnekus, M. H. (2014). *And Proprietary Digital of the requirements for the degree of by*, (December).

Thomson, B. L. L. (2013). Mobile Devices, *9*(3).

Vlastos, E., & Patel, A. (2016). *An open source forensic tool to visualize digital evidence*, (May). https://doi.org/10.1016/j.csi.2007.03.003

Wilsdon, T., & Slay, J. (2014). *Validation of Forensic Computing Software Utilizing Black Box Testing Techniques Validation of Forensic Computing Software Utilizing Black Box Testing Techniques*, (February).

# APPENDICES

## Appendix 1: Questionnaire

1. What department are you working from?
2. For how long have you worked in this field?
3. Are you aware of the use of software tools in processing digital evidence data?
4. Do you practice the use of multiple tools in processing a single case?
5. Do you face any difficulties in presenting digital results in the court?
6. If yes, which ways do you use to overcome the difficulties in reporting style?
7. Is there any standard way of reporting the analysis results in court for evidence?