FOUNDATION FOR ADMISSIBILITY OF ELECTRONIC EVIDENCE IN TANZANIA[1]

By Zakayo N.Lukumay[2]

Abstract

This article is a modest attempt to investigate the required standards for proper foundation of admissibility of electronic evidence in the courts in Tanzania. For such proper foundation to be laid, the e-evidence should pass through a number of tests as established under section 18 – 20 of the Electronic Transactions Act, 2015as well as judicial pronouncements as discussed in this discourse. These standards range from authenticity, relevance, rules against hearsay, and the best evidence rule. A proponent who fails to meet these tests will not be allowed to rely upon any piece of electronic evidence.

The article recommends that sections 69 and 78 &79 of the Tanzania Evidence Act, 1967 should be amended to introduce words to the effect that the requirement of authentication or identification is a condition precedent to admissibility and it is satisfied by evidence sufficient to support a finding that the matter in question is what its proponent claims. It is further recommended that merged to govern authentication of electronically stored information in the country. A good example in this respect are provisions of the US Federal Rules of Evidence which have been written in a more general manner to accommodate all evidence including evidence in electronic form.

Another provision worth adding to the Law of Evidence Act, 1967 is the one that should allow authentication or identification provided by the Act of Parliament or by other rules prescribed by the highest court in the hierarchy pursuant to statutory authority. The rationale of the proposed amendment is to give legal effect to the efforts by a few pro-active judges seeking to accommodate changes brought about by the ever advancing technologies.

Key Words: *Admissibility, Electronic Evidence, Electronic Transaction, Digital Evidence*

1.0 Introduction

Information and Communication Technologies (ICT) have, over the past few decades, decisively established itself as a general purpose technology—one that affects an entire economy and that it will continue to do so for the foreseeable future.[3]This growth shows that our lives currently depend on the wind of info-technology. We use it for healthcare, transport and most especially for communication. It has made life much easier than it was before, in every sense.

[1]This article was first presented at the Training for Judges, Magistrates, advocates, state attorneys, prosecutors and investigators in Zanzibar on 12th June, 2014 with the following title: "Electronic Evidence in Court Rooms: New Horizons and Evidential Foundation for Admissibility in Tanzania." The paper was reviewed to accommodate changes brought about by the Cyber Crime Act and the Electronic Transactions Act of 2015.

[2]Senior Lecturer at the Law School of Tanzania, an Advocate and an active member of the Tanganyika Law Society.

[3] See Association of Chief Police Officers (ACPO), "Good Practice Guide for Computer-based Electronic Evidence", accessed at http://www.7safe.com/electronic_evidence/ACPO_guidelines_computer_evidence.pdf on 30/04/2014, p. 6. See also Roper, M., (ed), "Managing Public Sector Records: A Study Programme", accessed at www.irmt.org/documents/educ_training/.../IRMT_**electronic**_recs.doc,on 1/05/2014.

There are now several websites that can help one get any product or service simply by the click of a button or mouse or touch pad.[4] It is for this reason, many companies and governments have been forced to digitise volumes of documents in order to reduce costs of storage and make easy transmission of information electronically.[5]

A report by the Tanzania Communication Regulatory Authority (TCRA) shows that internet services in Tanzania commenced from the year 1995. There has been a steady growth of internet users from 3.5million people in 2008 to over about 11 million out of the 32 million Tanzanians with access to mobile phones by the end of 2014.[6]

Conveniences brought by the mobile telephone, resulting from the ever-changing technology, and user-friendly apps offering immense opportunities to the users. These include messaging apps, portals and platforms all managed through Smartphones.[7] With an excess of 1 billion users globally, WhatsApp is the most popular mobile messaging application that enables users to exchange media, texts, video clips and voice calls.

In Tanzania, MIC Tanzania Limited,[8] one of the leading Telecommunication Company popular known as Tigo announced free WhatsApp services for its 10 million subscribers hence making it the first telecom company in the country to offer social media services for free.[9]Partly because WhatsApp is more easily accessible than either Facebook or Twitter to Tanzania's 11 million Internet users.[10]WhatsApp users in Tanzania can access services to hail a taxi, order food delivery, buy movie tickets, play casual games, check in for a flight, send money to friends, access fitness tracker data, book a doctor appointment, get banking statements, pay the water bill, find geo-targeted coupons, recognise music, search for a book, meet strangers around, follow celebrity news, read magazine articles, and even donate to charity - all integrated in a single app.[11]

On the other side, criminals all over the world have utilized these developments for their ill motives. In Tanzania, cybercrimes are on the increase at an alarming rate and the trend shows that these vices are likely to continue to be committed. Police records show that between 2010 and the first quarter of 2013 cyber fraud related

---

[4] Transportation companies like Fastjet, Precision Air and online shopping companies that sell vehicles like autorec, befoward, tradecarviewany many others have online portals where customers can order products and services online.
[5] Reed, C., "The admissibility and Authentication of Computer Evidence – A Confusion of Issues" 5th BILETA Conference, British and Irish Legal Technology Association, http://www.bileta.ac.uk/document%20library/1/the%20admissibility%20and%20authentication%20of%20computer%20evidence%20-%20a%20confusion%20of%20issues.pdf (accessed on 12/07/2015).
[6] See http://www.tanzaniatoday.co.tz/news/how-the-cyber-crime-law-will-affect-e-commerce-in-tanzania(accessed18/9/2015).
[7] See http://allafrica.com/stories/201602170815.html(accessed on 13/04/2015).
[8] MIC stands for Millicom International Cellular
[9] See http://allafrica.com/stories/201602051590.html . (accessed on 28/04/2016)
[10] See http://qz.com/510899/whatsapp-is-now-the-primary-platform-for-political-trash-talk-in-tanzanias-election-campaign/ (accessed on 28/04/2016).
[11]http://allafrica.com/stories/201602170815.html(accessed on 20/12/2015)

losses in banks stood around Tanzania shillings 9.8 billion.[12] It is estimated that 320 people were arrested between July and December 2011, whereas in 2012, 230 people were arrested over the crime.[13] Exim Bank in Arusha became the latest victim with nearly Tanzanian shillings 7 billion being reported to have been stolen from customer's accounts.[14] James[15] reports that financial institutions have been the main victims of cyber fraud and theft losing an estimated $1 billion after hackers[16] broke into the banks' network between 2013 and 2014. On 22nd February, 2016, the customers of NBC Bank at the branch of the University of Dar es Salaam (UDSM) lost nearly Sh100 million to card skimming. The bank statement of one of the victims showed that Tanzanian Shillings 800,000, which was his net salary had been withdrawn from London in Sterling Pounds using MasterCard. [17] The South Africa's Standard Bank, the parent company of Stanbic Bank Tanzania Limited, has also recently fallen victim of an electronic theft after criminals stole up to USD 19 Million by skimming automatic teller machines in far way Japan within a period of three hours.[18]

In response to challenges associated with the advancement of ICT, the Government of Tanzania enacted two important pieces of legislation. They are the Cybercrimes Act of 2015 and the Electronic Transactions Act of 2015. There have so far been a few cases[19] pending in courts arising from violation of the Cyber Crimes Act, particularly section 16 which prohibits publication of false[20] information. In all these cases, evidence to prove or disprove the allegations will certainly be electronic in nature.

Arguably, courts must be prepared to face challenges revolving around admissibility of new forms of evidence brought by the advancement of ICT. Chief Magistrate Judge Grimm of the United States District Court for the District of Maryland in *Lorraine v. Markel American Ins. Co*.[21] also advices that,

---

[12]www.theeastafrican.co.ke/news/Dar-pushes-for-cyber-crime-law-as a fraud icreases-2558/2048142-/ctdd75/-index.html(accessed on 12/01/2016).

[13]*Ibid.*

[14]*Ibid.*

[15] By Bernard James,The Citizen Reporter, accessed at http://www.thecitizen.co.tz/News/national/Banks-under-siege-from-ATM-hackers-/-/1840392/2631726/-/hbbv7bz/-/index.html (accessed on 12/01/2016).

[16]mainly from Eastern Europe, Ukraine, Russia and China.

[17] Bernard James, *op.cit.*

[18] See *The Guardian,* ISSN 0856 – 5422 Issue No. 6656, dated 25th May, 2016.

[19]A few of these suspects are YerickoYohanesNyerere, Mashinda Edwin Mtei and others, Benedict Angelo Ngonyan, Leila Constantine Sinare and 3 others, IsackHabakuki and Bob ChachaWangwe.

[20] Section 16 of the Cybercrime Act, Act No. 14 of 2015 provides that "Any person who publishes information or data presented in a picture, text, symbol or any other form in a computer system knowing that such information or data is false, deceptive, misleading or inaccurate, and with intent to defame, threaten, abuse, insult, or otherwise deceive or mislead the public or concealing commission of an offence, commits an offence, and shall on conviction be liable to a fine of not less than five million shillings or to imprisonment for a term of not less than three years or to both.

[21]Civil Action No.PWG-06-1893.Lorraineinvolved an insurance dispute over the recovery of insurance proceeds after the Plaintiff's boat was struck by lightning. Defendant insurance company paid out under the policy. Plaintiff later discovered that there had been damage to the ship's hull and claimed that he was entitled to an additional $36,000 to fix that damage. Defendant disagreed. Plaintiff filed a claim against his insurance company and the matter went to arbitration. At arbitration, the arbitrator held that some of the damage to the boat's hull had been caused by the lightening but limited the damages to

> [b]ecause it can be expected that electronic evidence will constitute much, if not most, of the evidence used in future motions practice or at trial, counsel should know how to get it right on the first try." It means that the proponent of any piece of electronic evidence should lay a proper foundation for admissibility, failure of which will render the evidence inadmissible.

It is therefore apposite that any person, including prosecutors as well as the defense lawyers, seeking admissibility of electronically generated information, has to lay the evidential foundation for the same before it is accepted in legal proceedings. This paper is modest attempt to present and discuss standards or requirements that should be fulfilled in admissibility of electronic evidence.

2.0 Meaning and Historical Development of Electronic Evidence

2.1 Meaning and Nature of Electronic Evidence

Electronic evidence is defined as data (comprising the output of analogue devices or data in digital format) that is created, manipulated, stored or communicated by any device, computer or computer system or transmitted over a communication system that is relevant to the process of adjudication.[22]According to Mason[23], there is a significant difference between analogue evidence and digital evidence, mainly because evidence that is the product of an analogue device is only stored on a carrier such as paper or a photographic film, or it may not even be recorded, but it can be a continuous reading, such as early versions of radar.

The relevant questions as far as a definition of digital evidence is concerned is what is 'digital'? It is worthy to refer to two definitions given by Oxford English Dictionary in this respect. Digital is defined as:

> Relating to or operating with signals or information represented by discrete numeric values of a physical quantity such as voltage or magnetic polarization (commonly representing the digits 0 and 1): designating a signal or information of this kind as opposed to analogue. Relating to or involving the capture, storage or manipulation of images by digital means; (of an image) stored or represented digitally; (of a device) capturing or generating such

---

$14,000. The issue in the district court was whether the arbitrator exceeded his authority by reducing the damages to $14,000. Plaintiff claimed the arbitrator was only authorized to determine whether the ship's hull was damaged as a result of the lightening; Defendant claimed the arbitrator had the authority to reduce the award. Both parties filed motions for summary judgment and both parties attached as exhibits emails that discussed the policy at issue. Neither party, however, supplied any authentication for the emails such that they would be admissible to support a motion for summary judgment. Judge Grimm thus took the opportunity of this case to discuss how electronically stored information can be proffered such that it is admissible into evidence.

[22] See S. Masson, ed, *Electronic Evidence: Disclosure, Discovery & Admissibility,* 2nd edn. (London: LexisNexis Butterworth), p. 22.
[23] *Ibid.*

images. Also in Cinematoger: utilizing this technology in film or television production

Casey[24] defines digital evidence for the purpose of his text in relation to crime as any data stored or transmitted using a computer that support or refute a theory of how an offence occurred or that address critical elements of the offence as instant or *alibi*. Examples of digital data include anything that has been created or stored on a computer, or is made available by way of the Internet, including CDs, DVDs, MP3s and digital broadcast radio.[25]

Digital evidence, by its very nature is invisible to the eye. It is said to be 'digital' because it has been broken down into digits; binary units of ones (1) and zeros (0), that are saved in a computer hard drive and retrieved using a set of instructions called software or code. Therefore the evidence must be developed using tools other than the human eye.[26]

Digital evidence comes from a variety of devices including computing devices (e.g., desktop and laptop computers, digital cameras, music players, Personal Digital Assistants [PDAs], and cellular telephones); network servers (e.g., supporting applications such as Web sites, electronic mail [e-mail], and social networks); and network hardware (e.g., routers found in businesses, homes, and the backbone of the Internet). Information of evidentiary value may be found on digital media such as compact discs (CDs), digital versatile discs (DVDs), floppy disks, thumb drives, hard drives, and memory expansion cards found in digital cameras and mobile phones.[27]

2.3 Sources of Electronic Evidence

The first source of electronic evidence is files created by the computer user. These include documents (e. g, word; file extension of either "doc' or "docx"), text, spreadsheet (e.g., Excel), image, graphics, audio and video files. The files contain metadata (i.e., data about data). Metadata can provide the following kinds of information: the name of the author of the document and the company the document; the owner of the computer; the date and time the document was created, saved and by whom it was saved; any revision made to the document; the date and

[24] E Casey, *Digital Evidence and Computer Evidence: Forensic Science, Computer and the Internet* ,2nd edn.,(London: Elsevier Academic Press) 2004. at 12.
[25] *Ibid*. See also Mason, S., *op. cit*., p. 22.
[26] See S. Mehta, "Cyber forensic and Admissibility of Digital Evidence", accessed at hhttp://www.supremecourtcases.com/index2.php?option=com_content&itemid=135&do_pdf=1&id=22821 on 22nd May, 2014.
[27] G. C Kessler, "Judges' Awareness, Understanding, andApplication of Digital Evidence", A dissertation submitted in partial fulfillment of the requirementsfor the degree of Doctor of PhilosophyinComputing Technology in Education, Graduate School of Computer and Information SciencesNova Southeastern University, 2010, p. 2., see also HosmerC., "Proving the Integrity of Digital Evidencewith Time", *International Journal of Digital Evidence,* Spring 2002, volume 1, Issue 1, p. 1., See also a Manual On Cyber Crime prepared by Data Security Council of India accessed at http://uppolice.up.nic.in/All%20Rules/Cyber%20crime/4-Cyber_Crime_Investigation_Manual.pdf (accessed on 07/06/2014).

time the document was last modified and accessed; and the last time and date the document was printed.[28]

The files of the Windows operating system contain metadata that (i.e., the time events recorded by computers) also may provide valuable information. This was demonstrated in *Jackson v. Microsoft Corporation*[29] where the timestamp data on confidential files in the defendant's possession provided evidence of intellectual property theft. Evidence can also be found on web browsers which users can create files. They may bookmark or added to their favourites folder in the web browser like internet explorer, Mozilla Firefox, Netscape Navigator, and Chrome to mention only a few.[30]

Evidence can also be retrieved from e-mail accounts. Address books in email accounts can include the contacts of the suspect. Other pertinent information relevant to a criminal or a civil case under investigation can be retrieved from e-mails in the inbox, sent, delete, draft, and spam for folders of an account, which reveal the content of communications and the person with whom the suspect was communicating.[31]

Another source of electronically stored information is files protected by computer users. There are many different ways in which a user can protect his or her files. An individual can modify files or folders within the computer to look like something else, he or she can add a password to the file or folder and /or encrypt it to ensure that no one will be able to see what is in the file or folder. An individual can also make the file or folder invisible.[32]

The last source of information which may have value evidentially is a file created by the computer. These include event logs, history files, cookies, temporary files, and spooler files.[33] Event logs automatically record events that occur within a computer to provide an audit trail that can be used to monitor, understand, and diagnose activities and problems within the system. The operating system also collects data about the websites visited by a user.

In *United States v. Tucker*,[34]computer forensics investigators found important electronic evidence of the crime- namely, deleted Internet cache files showing that Tucker had visited child pornography websites – on the suspect's hard drive. In a murder case, for example, Internet cache files can provide evidence on the web searches. Cookies are files created by websites that are stored on a user's computer

[28] See an Article entitled "Where Is the Electronic Evidence and Which Tools Can We Use to Find It?" accessed at*samples.jbpub.com/9781449600723/00723_CH07_Maras.pdf* on 28/05/2014.
[29]Civil Action No. 00-1457 (JGP)
[30]*Ibid*. See also Mason, S., *op.cit*., pp. 6-17.
[31] *Ibid*.
[32]*Ibid*.
[33] Mason, S., *op.cit*., p. 10, 62.
[34]150 F. Supp. 2d 1263 (D. Utah 2001).

hard drive when he or she visits that particular website. As such, by viewing cookies, the investigator can determine which websites the user has visited. Certain cookies are used by websites to gather information about an individual's activities, interests, and preferences. Others are used to store credit card information, user names and passwords. Some cookies do both.[35]

Temporary files can be created by the computer without the knowledge of the user. Operating system, for example, collects and hides certain information from the user, a good example being unsaved documents.[36]

Spooler files are created by the operating system and are stored in the computer hard drive. These are files that the user sends to the printer. As a default setting, most Microsoft Windows operating systems have print jobs "spool". These copies can be recovered and could provide vital evidence in the case under investigation.[37]

Evidence can also be retrieved from telecommunication devices like mobile phones. Evidentiary information like names and number of contacts; calls made, received, and missed; date, time, and duration of calls; text messages and messages with a combination of text, images, videos, and sound (MMS), can be found in mobile phones. With the increased storage capacity and their use in sending e-mails, taking photographs, downloading music, sending instant messages, recording and playing videos, opening application files,(e.g. like documents, spreadsheets, and presentations), and browsing the Internet, mobile phones have become a mine of evidentiary information relevant to a criminal or civil case. Smart phones, may even store global positioning system (GPS) coordinates when photographs are taken, along with the time and date when the photo was created. Additionally, mobile phones may contain GPS navigation system. Therefore, an investigator can pull up the GPS history and any addresses programmed into the GPS and determine which places an offender visited.[38]

Once digital evidence has been identified and obtained, it should be analyzed and a comprehensive report prepared by a specialist, known as a cyber or computer forensic expert. The involvement of this person at every stage of acquisition of digital evidence who will detail all the procedures involved in the process is very vital in order to give the same high probative value.

[35] Mason, S., *op.cit*., p. 10
[36] *Ibid*, p.61.
[37] *Ibid*.
[38] See "Cyber crime Investigation Manual" prepared by Data Security Council of India accessed at http://uppolice.up.nic.in/All%20Rules/Cyber%20crime/4-Cyber_Crime_Investigation_Manual.pdf (accessed on 07/06/2014).

3.0 Challenges Associated with Admissibility of Electronic Evidence

3.1 Overview

The web dictionary defines admissibility as 'capable of being or bound to be admitted in a court of law.'[39]It is a concept in the law of evidence that determines whether or not evidence can be received by the court.[40]According to Blacks Law Dictionary, to be admissbile, evidence must be relevant and to be relevant it must tend to establish material proposition. While admissible facts must be relevant, not all relevant facts are admissible. A fact may be relevant but inadmissible if it is excluded by law for certain reasons. Admissibility is a question of law, while relevance is a question of fact, logic and common sense.[41]

This section devotes a discussion on challenges in admissibility of electronic evidence. These challenges revolve around first, authenticity, second, mechanisms for ascertaining reliability of the equipment that generated, store or transmitted a piece of evidence, weight attached to digital evidence and fourth, limited knowledge of adjudicators in fairly and properly applying the laid down tests/standards to digital evidence.

3.2 Authenticity

A serious concern with respect to digital evidence in digital format revolves around its ubiquitous nature, in that it appears in almost every case in one form or another[42] and it may change formats depending on the software used.[43] A document created in Microsoft Word and later opened in Word Pad is a good example. The document will not show all the features it had when created in Microsoft word. Furthermore, the increasing dangers to the integrity, availability, confidentiality, authenticity, and authorship of electronic documents, associated with actions of hackers, crackers, re-mailers, corporate frauds, and cybercrimes in general, have caused a great deal of concern regarding the risks and constraints for judicial admissibility of electronic evidence.[44]

It is for this reason that the Association of Chief Police Officers[45] pointed out in relation to the nature of computer – based evidence that:

Computer-based electronic evidence is, by its very nature, fragile. It can be altered, damaged, or destroyed by improper handling or improper examination. For this reason, special precautions should be taken to document, collect, preserve and

[39]See http://www.dictionary.com/browse/admissibility. (accessed on 13/01/2016).
[40]Seehttp://legal-dictionary.thefreedictionary.com/admissibility (accessed on 13/01/2016).
[41]See Abiodun, A., "The Evidence Act of 2011: An Appraisal" Being A Paper Presented at the Ogun State Bar and Bench Forum, On Thursday, 11th July, 2013 At The June 12 CulturalCentre, Abeokuta

[42]*Ibid*.
[43] Mason, S., *op.cit*., pp. 84&85.
[44] See the ITU Report on Assessment of Electronic Evidence, http://www.itu.int/en/ITU-D/Projects/ITU-EC-ACP/HIPCAR/Documents/FINAL%20DOCUMENTS/ENGLISH%20DOCS/e-evidence_assessment.pdf(accessed on 16/05/2014).
[45] See the ACPO, *op.cit*, p. 6.

examine this type of evidence. Failure to do so may render it unusable or lead to an inaccurate conclusion.

The challenge to triers of facts revolves around trust or genuineness of the media which stores the information, like a CD, memory stick or even a hard drive. Errors abound in all forms of information communication systems. Examples may include corruption of data,[46] loss of data, interference with data and errors in the interpretation and analysis of evidence. Because of this problem, Mason advises that the correctness of the information stored in any computer system and media should always be ascertained before a conclusion is reached.[47]

Profile pages on social network sites raise authentication issues analogous to those raised by photographs, and videos, as well as several types of metadata, some of which are not publicly visible.[48]The key issue in social media is typically one of authorship- who authored/posted the alleged document in question? As Pendleton[49] correctly points out, anyone is free to create a profile page using whatever name of choice. Therefore, the mere existence of a profile page in someone's name does not necessarily reflect that the purported creator had anything to do with its creation. Such postings do not require a unique user name and password.[50]

3.3 Judges' Awareness on Standards of Admissibility of Digital Evidence

In Lazarus Mirisho's case, for example, issues raised by the Defence were whether in Tanzania courts are well equipped to handle electronic evidence in view of absence of rules and procedures for the admissibility of such evidence. The Defendant's Counsel doubted the ability of courts, in the absence of any express statutory enactment.

In the case of *Rep. v. Sweetbert Godian@Kashaga & Another*[51] the prosecution did not tell the court how conspiracy could be done between the accused persons via other means of communication other than them meeting physically. The court also did not acknowledge that, conspiracy is possible without physical meeting. With regard to the second count of forgery, the prosecution had adduced evidence that the second accused had logged in 8 times in different accounts of the client including that of the first accused. It seems that the prosecution did not show how this was possible given that the electronic transfer was affected at the headquarters of the bank. But again

[46] Introduction of a 'trojan horse' is one of the causes of corruption of data in the computer or computer system.
[47] See Mason, S., *op.cit*., p. 7.
[48] Ibid.
[49] A. Pendleton, "Admissibility of Electronic Evidence: A New Evidentiary Frontier", http://mnbenchbar.com/2013/10/admissibility-of-electronic-evidence/, (accessed on 15/05/2014).
[50]Recently Jamii Forum posted the following story with the following Swahili title: "Mbungewamoshivijijinicyrilchamiakanushauzushidhidiyake, asemaileniakauntfeki." The unofficial translation of this title can be "The Member of Parliament – Moshi Rural Cyril Chami denies false information against him, saying the account used is fake". Headings like these tend to show that not all stories, images or conversations found in online social media are authentic.(See http://www.jamiiforums.com/jukwaa-la-siasa/589546-mbunge-wa-moshi-vijijini-cyril-chami-akanusha-uzushi-dhidi-yake-asema-ile-ni-akaunt-feki.html).
[51]Criminal Case No 68 of 2009.

the court seems to have agreed with the accused person's defence that he could not have affected the said transfer because he was not at the headquarters. This shows that the court did not pay regard to the fact that transfer of funds can be affected electronically without physically being present at the bank.

It should be viewed, additional evidence would have been necessary to convince the court that the accused persons did commit the offences electronically, which did not require any physical meeting or actual transfer of money in cash form. These bits of evidence could be, for example phone communications between the suspects if any and expert evidence to show how it is possible to create the fake password to affect transfer.

Rep.v. James Elineema@kangalu&3 others,[52] the offences with which the accused persons were charged were similar to the case above. The same observations were made by the court when deciding on whether the accuse persons were guilty of the offence of conspiracy or not. It seems the prosecution and the court expected the suspects to meet physically and conspire. In the second count of forgery, the electronic evidence was disregarded by both the prosecution and the court. A neutral e-expert was necessary to show how the 1st and 2nd accused persons' accounts were credited in electronic means. This was possible through audit trails, but the challenge is what if the accused person, using some technical knowhow deleted the information? This is where the need for a forensic expert comes in. He is able to show how the accused person deleted some information and this would raise a lot of suspicions, justifying, as it is viewed, a conviction based on circumstantial evidence.

The danger with electronic evidence is that it can be applied to convict an innocent person. Mason[53] presented several examples of this complex situation, including: a judge is presented with network server logs showing a cyber intruder coming from a particular Internet Protocol (IP) address. Internet Service Provider (ISP) records show that the IP address in question was assigned to a computer system at a particular residence at the time of the incident. This information could be used to improperly identify an individual as a wrongdoer; a judge is presented with call history and service provider records showing that one mobile telephone was used to place a call to another mobile phone. The court and a jury might erroneously believe that this evidence conclusively proves that the owners of the two telephones actually had a conversation.

Metadata in a Microsoft Word document include the name of the person who ostensibly registered the product. Unless that information is deliberately deleted or

[52]Criminal Case No. 200/2010.
[53] Mason, S., *op.cit.,* p. 50.

altered, the name will appear in every document generated by the Office application. A judge might erroneously conclude that the metadata in a given document conclusively proves that the named person is the actual author.[54]

In view of the complexity and the nature of electronic evidence, it is argued that training should be conducted to all stakeholders in the justice sector like judges, magistrates, prosecutors, advocates, investigators to mention only a few. In line with this recommendation, one forum[55] observed that:

Given the reliance of societies worldwide on information and communication technologies, judges and prosecutors must be prepared to deal with cybercrime and electronic evidence. While in many countries, law enforcement authorities have been able to strengthen their capacities to investigate cybercrime and secure electronic evidence, this seems to have been less the case for judges and prosecutors. Experience suggests that in most cases, judges and prosecutors encounter difficulties in coping with the new realities of the cyber world.[56]

The forum urged that particular efforts are required to enable judges and prosecutors to prosecute and adjudicate cybercrime and make use of electronic evidence through training, networking and specialization.

In *Lazarus Mirisho Mafie and Another v. Odilo Gasper Kilenga,*[57] for example, the issues raised by the Defence was whether in Tanzania courts are well equipped to handle electronic evidence in view of absence of rules and procedures for the admissibility of such evidence. The Defendant's Counsel doubted the ability of courts, in the absence of any express statutory enactment. In this case, parties decided to settle the dispute out of court as the plaintiff could not meet the standards required for admissibility of a print-out of an email.[58]

3. 4 Proof of Reliability of Equipment

Reliability is the capacity of a digital object to stand for the facts to which it purports to attest, which, in turn, is linked to ensuring sufficient procedural and technical attributes (including a combination of preventative measures, such as to prevent unauthorized amendments and changes, and verification measures to provide for a degree of assurance as to the identity of users and manipulated) are in place and working to provide for a degree of assurance that the digital object can be deemed to be reliable. In essence, reliability is associated with the degree of control exercised over the procedures that permit the data to be created. It is not absolute. The other

[54] *Ibid.*
[55] See the Council of Europe Report on "Cybercrime Training for judges and prosecutors: A Concept" http://www.coe.int/t/DGHL/cooperation/LisbonNetwork/meetings/Autre/2079_train_concept_4_provisional_8oct09_en.pdf, p. 4. (accessed on 20/06/2016).
[56] *Ibid.*
[57] Commercial Case No. 10 of 2008 (Unreported).
[58] An Interview conducted with Justice Makaramba on phone on 16th May, 2014.

challenging aspect as far as admissibility of electronic evidence is whether electronic evidence is reliable.

A number of jurisdictions peg reliability on the equipment that produced an electronic record. In *R v Shephard,*[59] Lord Griffith observed that:

> Computers vary immensely in their complexity and in the operations they perform. The nature of evidence to discharge the burden of showing that there has been no improper use of the computer and that it was operating properly will inevitably vary from case to case.

The question that this case raises is how to prove reliability of digital evidence. Lord Griffith in the cited case was of the view that the burden can be discharged by calling a witness who is familiar with the operation of the computer in the sense of knowing what the computer is required to do and who can say that it is doing it properly[60]. It is also advised that lawyers must look at digital guidance from forensic specialists.

4.0 Admissibility of Electronic Evidence in Tanzania

4:1 The Position before 2015

Before the amendment of this Act in 2007 and 2015, it was doubtful if electronic evidence was admissible in both civil and criminal cases. It was for this reason that Nsekela, J., (as he then was) observed in *Trust Bank of Tanzania v. Le-Marsh Enterpsrises Ltd. and Two Others,*[61]that, in absence of the law which guides the admission of e-evidence, the court will find ways of dispensing justice even in very difficult circumstance for legal guidance. On the need for the court to march according to technological changes, he reiterated that the law must keep abreast of technological changes as it affects the way of doing business and therefore the court has a duty to take into account technological changes that affects the business worldwide.

Drawing lessons from UK, Nsekela, J., (as he then was) amended the definition of banker's book to include its counterpart in electronic version and the print out may be admitted in evidence subject to the same safeguards provided for under sections 78 and 79 of the Tanzania Evidence Act of 1967. He, however, was of the view that it would have been much better if the position was clarified beyond all doubt by legislation rather than judicial intervention. After eight years of such a piece of advice, the Legislature in 2007 made amendments to the Evidence Act, 1967 to

[59][1993] AC 380, [1993] 1 AII ER 225 (spelt Shepherd in AII ER), [1993] Crim LR 295, HL.
[60][1993] AC 380 at 387. See Connolly v Lancashire Country Council [1994] RTR 79, QBD, where the prosecution elected to produce evidence that a weighbridge was working properly, but failed to demonstrate the computer was functioning properly at the material time.
[61]Commercial Case No.4 of 2000 (Unreported).

provide for admissibility of computer print-out in evidence as part of banker's books and electronic evidence to prove criminal charges.

Section 40A of the Evidence Act of 1967 was amended[62] to provide for admissibility of computer generated evidence in criminal cases as follows:

> In any criminal proceedings-
>
> a) An information retrieved from computer systems, networks or servers; or
>
> b) The records obtained through surveillance of means of preservation of information including facsimile machines, electronic transmission and communication facilities; or
>
> c) The audio or video recording of acts or behaviors or conversation of persons charged, shall be admissible in evidence.

Sections 78A and 78B were also amended by the same Act to provide for admissibility of bankers books in electronic form as follows:

> **78A. – (1)** "Banker's books" include ledgers, cash books, account books and any other records used in the ordinary business of the bank or financial institution, whether the records are in written form or a data message kept on an information system including, but not limited to computers and storage devices, magnetic tape, micro-film, video or computer display screen or any other form of mechanical or electronic data retrieval mechanism.
>
> **78B. – (1)** A printout of any entry in the books of a bank on micro-film,
>
> computer, information system, magnetic tape or any other form of mechanical or electronic data retrieval mechanism obtained by a mechanical or other process which in itself ensures the accuracy of such print out, and when such print out is supported by a proof stipulated under subsection (2) of section 78 that it was made in the usual and ordinary course of business, and that the book is in the custody of the bank, it shall be received in evidence under this Act.
>
> (2) Any entry in any banker's book shall be deemed to be primary evidence of such entry and any such banker's book shall be deemed to be a "document" for the purposes of subsection (1) of section 64.

In 2007, Lukumay and Mollel[63] argued in respect of these amendments that they were not adequate for the following reasons: First, there are various provisions in the

[62] See the Written Laws (Miscellaneous Amendments) Act [Act No.15 of 2007].

Law of Evidence Act that remain untouched and which have been impacted by ICT in one way or another. Sections 68 and 69 which provides for authentication of documentary evidence are good examples. Second, the amendments did not touch other pieces of legislation that mention documents which may also have evidentiary value. Third, the amendment did not address on the thorny issue of authentication. In other words, it did not have mechanisms for authentication of digital evidence.[64]

Another development towards giving legal recognition to documents in electronic form was the enactment of the Finance Act, 2009. The Act amends several pieces of tax legislation to provide for the recognition of electronic documents for various purposes including evidence, filing or lodgement by a taxpayer and service by the Tanzania Revenue Authority. These changes anticipate a move towards the greater use of electronic communication for tax communications. E-filing, for example, is explicitly stated as a strategic initiative in the TRA's Third Corporate Plan (2008/09 – 2012/13).[65]

The inadequacy of the Evidence Act to regulate in evidence in electronic form in civil cases was addressed by Makaramba J. in *Lazarus Mirisho Mafie and Another v. Odilo Gasper Kilenga*[66]and Nyangarika J., in *Exim Bank (T) Ltd v. Kilimanjaro Coffee Company Limited.*[67]The issue in Lazarus case was whether or not electronic documents/records may be admitted as evidence in proceedings of civil nature. The Defendant's Counsel contended that e-mails, being electronic evidence are not admissible in evidence in civil proceedings. The Court, agreeing with this contention pointed out that the admissibility of electronic evidence in civil proceedings is not yet part of our laws. There is a dearth of statutory provisions and case law on admissibility of electronic evidence in civil proceedings generally.

Makaramba J., in Lazurus case is of the view that:

> Our Evidence Act, 1967 however does not contain any express provision on authentication and identification of electronically stored information as is the case with the Kenyan Evidence Act or the United States Federal Rules of Evidence. The underlying concept under the Evidence Act, 1967 is relevancy of evidence to the facts in issue.

He further observed that the first task of the Court was to examine the existing provisions in our law on admissibility of documentary evidence and construe them broadly if possible in order to establish a set of rules to guide admissibility of

---

[63] A. Mollel& Z. Lukumay, *Electronic Transactions and the Law of Evidence in Tanzania,* Iringa University College, p. 92.
[64] The Article will later examine if these concerns have adequately been addressed in the new Cyber Crime Act and Electronic Transactions Act both of 2015.
[65] See http://www.pwc.com/en_TZ/tz/pdf/finance-act-update-2009.pdf. (accessed on 20/12/2015)
[66] Commercial Case No. 10 of 2008 (Unreported). It was also noted in this case that the piece meal approach to legislating the law on admissibility of electronic evidence in Tanzania is unsatisfactory.
[67] Commercial Case No. 29 of 2011 (Unreported).

electronically stored information generated for use in court of law as evidence in civil proceedings.

Although the above statement, the Judge was of the different view that the Law of Evidence Act before it was amended by the Electronic Transactions Act of 2015 sufficed to cover electronically generated information without requiring the intervention of the Parliament. This view is apparently contrary to the one expressed by Mason[68] that evidence in digital format ought to be subject to a more rigorous mechanism than would normally be associated with extant on physical media. The two forms of document, physical and digital, cannot be compared like-for-like because the criteria by which a document in digital format must be tested will differ, by its very nature, to that of physical document.[69]

Despite Judge Makaramba's view on the inadequacy of the current rules of evidence in civil proceedings, he pointed out that:

> A novel legal issue as it obviously creates some challenges to courts which necessarily call for judicial innovation as it holds a stake in the development of the law in so far as the admissibility of electronic evidence in civil proceedings is concerned…The main task for this Court presently is therefore to develop the law a step further by setting out guiding standards for recognizing admissibility of electronically stored evidence in civil proceedings.

From this quotation, Justice Makaramba seems to have agreed with the fact that the law of Evidence Act of Tanzania lacks the guidelines in relation to admissibility of electronic evidence. The Judge in this case lamented on the inadequacy and the unavailability of case law to guide him in the following words:

> The e-mail the Plaintiffs sought to be admitted as evidence to support their claim is central to the preliminary objection. This Court however is being called upon to consider the admissibility of electronic evidence in civil proceedings generally, which admittedly is not yet covered under our laws of evidence or civil procedure. There is however some limited sphere in admissibility of electronic evidence in certain specified matters in civil proceedings as well as in criminal proceedings. This Court therefore in dealing with the matter before is doing so without the benefit of any express enactment on admissibility of electronic evidence generally in other civil proceedings, and without any precedent from our courts on admissibility of e-mail to fall back on.

The Judge further observed that:

[68] Mason, S., *op.cit.*, p. 23.
[69] *Ibid.*

> It must be appreciated however, that in this country, aside from certain restrictive amendments to the law of evidence, and the decision of this Court in the case of *The Trust Bank of Tanzania v. Le-Marsh Enterpsrises Ltd. and two Others*, Commercial Case No.4 of 2000 (Unreported), which dealt with the issue "*whether or not a computer print-out is a banker's book under the Evidence Act, 1967*, there is dearth of statutory provisions and case law on admissibility of electronic evidence in civil proceedings generally.

It is for this reason therefore that he intervened, after quoting a decision by Lord Denning in *Packer v. Packer*[70] by extending the definition of a 'document' in section 3 of the Tanzania Evidence Act, 1967[71] to include an e-mail in the following words:

> In the present case, the duty of this Court is to "*construe*" the words in the existing laws and then to "*extend*" that construction to cover electronically stored information. The idea is not as the Plaintiffs' Counsel would wish this Court to do to extend to civil proceedings rules on admissibility of electronic evidence developed for criminal proceedings, but to construe the term "*document*" in section 3 of the Tanzania Evidence Act, 1967 [Cap.6 RE 2002] to encompass an e-mail for purposes of admissibility in civil proceedings.[72]

It is viewed; the Judge undertook in this case a task which the Parliament had already done in the Finance Act of 2009. This law extended the definition of the term "document" to include a document in electronic form. The Judge ought only to have taken judicial notice of this law and point out the fact that an 'e-mail' is an electronic document and therefore falls within the definition in the above mentioned law.

Adopting the requirements that should be met in so far as admissibility of electronically generated evidence laid down in Loraine's case Makaramba J., in Lazurus case is of the view that:

> as for standards on relevancy and hearsay, the existing rules of evidence suffice. The rules to be developed by courts are for setting out prior requirements to be met before an electronically generated document can be admitted in evidence in civil proceedings. This is where opinion given by Judge Grim in *Jack R. Loraine and Beverly Mack v. Markel American Insurance Company* Civil Action No. PWG-06-1893 becomes relevant

In Lorraine's case, Magistrate Grimm observed that, electronic evidence "comes in multiple evidentiary 'flavors, 'including e-mail, website ESI (electronically stored information), internet postings, digital photographs, and computer-generated documents and data files. According to Judge Magistrate Grimm, electronic evidence

[70][1954] P 15 (if we never do anything which has never been done before, we shall not get anywhere. The law will stand still whilst the rest of the world goes on: and that will be bad for both.
[71] [Cap. 6 R.E. 2002].
[72]See Lazaro Mirisho's Case.

can be lumped under the umbrella term of ESI. Whether ESI is admissible into evidence is determined by a collection of evidence rules that present themselves like a series of hurdles to be cleared by the proponent of the evidence. These rules are:

> (1) is the ESI relevant as determined by Rule 401 (does it have any tendency to make some fact that is of consequence to the litigation more or less probable than it otherwise would be); (2) if relevant under 401, is it authentic as required by Rule 901(a) (can the proponent show that the ESI is what it purports to be); (3) if the ESI is offered for its substantive truth, is it hearsay as defined by Rule 801, and if so, is it covered by an applicable exception (Rules 803, 804 and 807); (4) is the form of the ESI that is being offered as evidence an original or duplicate under the original writing rule, or if not, is there admissible secondary evidence to prove the content of the ESI (Rules 1001-1008); and (5) is the probative value of the ESI substantially outweighed by the danger of unfair prejudice or one of the other factors identified by Rule 403, such that it should be excluded despite its relevance.

Following the decision in Loraine's case, Justice Makaramba propounded rules that should guide the court in Tanzania in admitting electronically stored information, including emails in form of questions as follows:

> first, is the e-mail relevant as determined under the Evidence Act, 1967 [Cap.6 R.E. 2002] (does it have any tendency to make some fact that is of consequence to the litigation more or less probable than it otherwise would be); second, if relevant under the Evidence Act, 1967 [Cap.6 R.E. 2002] as amended is it authentic in the sense that, can the proponent show that the e-mail is what it purports to be; third, if the e-mail is offered for its substantive truth, is it hearsay as defined under the rules in the Evidence Act, [Cap.6 R.E. 2002] as amended and if so, is it covered by an applicable exceptions to the hearsay rules under the Evidence Act, 1967 [Cap.6 R.E. 2002] as amended; fourth, is the e-mail that is being offered as evidence an original or duplicate under the original writing rule, if not, is there admissible secondary evidence to prove the content of the e-mail; and fifth, is the probative value of the e-mail substantially outweighed by the danger of unfair prejudice or other identified harm.

From the above decisions, the five standards that a party seeking admissibility of electronically generated evidence must comply revolve around relevance, authenticity, original rule, rule against hearsay and unfair prejudice. These standards as adopted into Tanzanian legal system by Justice Makaramba in Lazarus case that act as the set of court rules for guiding any court in determining the admissibility of electronically stored information (ESI), which is not limited to e-

mails only, but may encompass other forms of electronic evidence such as computer print outs, website messages only to mention a few. Failure to clear any of these evidentiary hurdles means that the evidence will not be admissible.

4.2 The Position After 2015

4.2.1 Overview

As pointed out earlier in this article, the Parliament of Tanzania enacted two pieces of legislation that are relevant to this discussion. The first one is the Cybercrime Act of 2015 and the second one is the Electronic Transactions Act of 2015. Apparently, while ETA borrowed heavily from UNCITRAL Model Law on Electronic Commerce, Cybercrime Act does the same from the African Union Convention on Cyber Security and Personal Data of June 2014. Under Article 25,[73] the Convention requires member states to adopt legislation to combat cybercrime.

The Cybercrime Act aims at making provisions for criminalizing offences related to computer systems and Information Communication Technologies and to provide for investigation, collection, and use of electronic evidence[74] and for matters related therewith. The crimes include illegal Access, illegal interception, illegal data interference, data espionage, illegal system interference, illegal device, computer-related forgery, computer-related fraud, child abuse and identity related crimes, among others.[75]Apparently, the enactment of the Cybercrime Act is a response to the difficulties faced in prosecution of crimes committed through the use of computers and computer networks. The Act was not meant to prevent the exchange and drafting of information but to protect people from abuse, such as online fraud.

The Electronic Transactions Act, 2015 provides for the legal recognition of electronic transactions, e-government services, the use of ICT in collection of evidence, admissibility of electronic evidence, facilitation of secure electronic signature and other related issues. Recognition of electronic transactions, admissibility of electronic evidence and recognition of electronic contracts have been long waited because prior to the Electronic Transactions Act, electronic transactions, electronic contracts or were not recognized under the laws in Tanzania.

---

[73] Article 25 of the Convention provides that "each State Party to the convention shall adopt such legislative and/or measures as it deems effective by considering as substantive criminal offences acts which affect the confidentiality, integrity availability and survival of information and communication technology system, the data they process and the underlying network infrastructure, as well as effective procedural measures to pursue and prosecute offenders. State Parties shall take into consideration the choice of language that is used in international best practices.

[74] Part IV of the Act contains provisions in relation to search and seizure. See sections 31-38.

[75] Part II of the Act contains 25 provisions on various offences and penalties – sections 4-5 illegal access, remaining and interception; section 7 – illegal data interference; sections 8-12 data espionage, illegal system interference, illegal device, computer-related forgery and computer-related fraud; section 13 – computer pornography; section 14 – pornography; section 15 – identity crimes; section. 16 – publication of false information; sections 17 – 19 – racist and xenophobic material, racist and xenophobic motivated insult, and genocide and crimes against humanity; s. 20 – unsolicited messages; sections 20-21 – disclosure of details of investigation and obstruction of investigation; section 23 – cyberbullying; section 24 – violation of intellectual property rights.

In other words, the Act sought to create conducive environment in which persons can lawfully transaction business in cyberspace and enforce their rights in the civil courts should the need to do arises. It is not within the scope of this paper to give a critical analysis of the two pieces of legislation. Of relevance to this paper is the fact that electronic evidence has now received legal recognition. In other words, information created, manipulated, stored or communicated electronically can now be used to prove or disprove a matter in court.

4.2.2 Definition of Terms Related to Electronically Generated or Stored Information

S. 3 of the Electronic Transactions Act of 2015 defines data as any information presented in an electronic form. S. 64 (2) defines electronic evidence as electronic evidence" means any data or information stored in electronic form or electronic media or retrieved from a computer system, which can be presented as evidence. Section 42 of the Act amends the definition of the term 'document' under section 3 of the Evidence Act to include computer data and every recording upon any tangible thing, any form of communication or representation including electronic form. "Electronic record" means a record stored in an electronic form;

The same section 3 of the Electronic Transactions Act defines "electronic signature" as data, including an electronic sound, symbol or process, executed or adopted to identify a party, to indicate that party's approval or intention in respect of the information contained in the electronic communication and which is attached to or logically associated with such electronic communication;

Of interest in this part is the definition of the term 'document'. The issue that may be posed is whether this definition is wide enough to cover the modern means of generating, storing and transmitting evidence in electronic form. To be specific, does this definition cover all hand-held devices like phones, ATM machines, tablets and any other electronic devices that can store, process, transmit or retrieve information in electronic form? Will this provision encompass statements from telecommunication companies showing records of call logs, text messages, WhatsApp chats, receipts or records of cash withdrawals and other transactions from ATM machines, internet banking, online product purchases, on-line bill payments, of utility bills, flight bookings and tickets, and other online transaction records?

Solace is found in the definition of 'data' and 'data message' under s. 3 of the Electronic Transactions Act of 2015. While data is defined as 'any information presented in an electronic form', data message is defined '… data generated, communicated, received or stored by electronic, magnetic optical or other means in a computer system or for transmission from one computer system to another.' With these definitions, the courts should now accept information recorded in any device

as evidence to prove or disprove any contentious matter and the same should not be rejected for a simple reason that it is in electronic format and not there is any print-out to that effect. The challenge is how to prove its authenticity. The later part of this article is devoted to this discussion.

It is, however, my view that the definition of the term 'document' which appears in a myriad of legislation should be extended to cover and include any device by means of which information is recorded, stored or retrievable including computer output.[76]

4.2.3 Legal Recognition of Data Messages

Similar to UNCITRAL Model Law on Electronic Commerce, Electronic Transactions Act adopts the functional equivalent approach in the course of elimination of obstacles arising from legal requirements as to writing, signatures, originals and retention of data messages. It is for this reason that s. 4 provides that "a data message shall not be denied legal effect, validity or enforceability on the ground that it is in electronic format." With this provision, data messages have been given functional equivalence to paper documents.

In order remove obstacles facing electronic records, various provisions of the Evidence Act of 1967 have been amended. Section 42 of the Act amends section19 of the Evidence Act by inserting the word 'electronic' immediately after the word 'oral'. Section 44 amends section 34 of the Evidence Act by inserting the word 'electronic' immediately after the word 'written'. Section 44 amends section 34B of the Evidence Act by inserting the words 'or electronic' between the words 'written' and 'statements' wherever they appear in that section.

4.2.4 Requirements of writing, signature, original and retention of data messages

In much the same line as Articles 6, 7 and 8 of the UNCITRAL Model Law on Electronic Commerce, sections 5, 6, 7 and 9 of the Electronic Transactions Act of 2015 introduces various provisions on how data messages will fulfil the legal requirements of writing, signature, original and retention. On the requirement of writing, section 5 of ETA provides that, where a law requires information or transaction to be in a prescribed non-electronic form or in writing, such requirement shall be met by an information or a transaction entered in electronic form that is - (a) organized in the same or substantially the same way as the prescribed non-electronic form; (b) accessible to the other person for subsequent reference; and (c) capable to be retained by the other person. (2) Subsection (1) shall apply whether the requirement is in a form of an obligation or where the law only provides consequences for the information which is not in writing.

[76] See section 258 of the Nigerian Evidence Act of 2011.

In respect with the requirement as to signature, section 6 (1) where a law requires the signature of a person to be entered, that requirement shall be met by a secure electronic signature made under this Act. (2) The requirement for an electronic signature made under subsection (1) shall be met if- (a) the method is used to identify the person and to indicate the intention of that person in relation with the information communicated; and (b) at the time the method was used, that method was reliable and appropriate for the purposes for which the information was communicated. 3) Parties to a contract may agree to use a particular method of electronic signature as they deem appropriate unless it is otherwise provided by law.

The law does not dictate the method of signing a document in electronic form. This leaves a party wishing to prove that he/she signed a document electronically to use any method to identify the signatory and that the method is reliable and appropriate. Sections 7 and 8 provides for secured electronic signature. It is deemed to be secure if is unique, can be identify the signatory, is created and affixed to the electronic communication, is under the control of the person who signs it and is created and linked to the electronic communication to which it relates in a manner such that any changes in the electronic communication would be revealed.

In my strong view, the law this provision is not very clear as it does not state categorically the manner in which an electronic signature can be created, secured or controlled and which authority has the mandate of issuing it. This is open to each electronic system to create its own system of electronic signature and claim it to be secure.

In *Dodsal Hydrocabons and Power [Tanzania PVT LTD & 3 Others v. Hasmukh Bhagwanji Masrani*,[77] pleadings were struck out for containing scanned signatures which were held not to be recognised in our Laws despite a party having submitted an affidavit which was likewise held to have contained scanned signature instead of originals on its verification clauses. The principal officer of the claimants company signed the pleadings in Saud Arabia and an objection was raised. Although the matter is now on appeal, it is a well-established principle that the object of signature and verification is to fix upon a party responsibility and guarantee of good faith. Conversely, in England, electronic signature is said to include, typing a name into a document; an email address; clicking the 'I accept' icon; PIN; biodynamic signature; scanned signature and digital signature.[78]

On retention requirement, section 9 (1) provides that where a written law requires that certain information or document be retained or kept, that requirement is deemed to have been met by electronic record keeping provided that the information contained in that record is in electronic form. The electronic record is

[77]Commercial Case NO. 42 of 2011[HC][Makaramba, J][Unreported] at 20.
[78]Abiodun, A., *op.cit.*, p. 25.

retained or kept in a format in which it was generated, sent or received, or in a format which can be demonstrated to represent that information accurately; and such electronic record is retained or kept in a form that enables the identification of the origin and destination of an electronic record or electronic communication and the date and time when it was first generated, sent, received or retained.

4.2.5 Admissibility of Electronic Evidence

Section 40A of the Tanzania Evidence Act of 1967 provides for admissibility of electronic evidence in respect of criminal cases and sections 78A and 78B to accommodate bankers' books in electronic form. Apparently, these provisions should now be read together with section 46 of the Electronic Transactions Act of 2015 introduces the new section 64A in Evidence Act which provides that in any proceedings, electronic evidence shall be admissible and its weight shall be determined in the manner prescribed under section 18 of the Electronic Transaction Act, 2015.

5.2 Foundational Requirements

5.2.1 Overview

The adversarial system requires that every proponent of any piece of evidence must lay a proper foundation before it is admissible to prove or disprove any fact in issue. As we will see in this study, Judges have held correctly to my view that failure to lay the foundation for admissibility of electronically generated evidence is a serious procedural that flaw in any proceedings.

The purpose of this section, therefore, is to explore standards that may be used in laying such a foundation. There are five foundational rules that a party seeking admissibility of electronically generated evidence must comply. These are relevance, authenticity, original rule, rule against hearsay and unfair prejudice.

5.2.2 Relevance

The first requirement for admissibility is that the evidence must be relevance. In this requirement, the proponent of electronically generated evidence must offer proof that it is relevant to the proceedings before the court. "Relevant evidence" means evidence having any tendency to make the existence of any fact that is of consequence to the determination of the action more probable or less probable than it would be without the evidence. According to Grimm J., in Loraine, there is a distinction between the admissibility of evidence and the weight to which it is entitled in the eyes of the fact finder and that to be relevant, evidence does not have

to carry any particular weight: "it is sufficient if it has 'any tendency' to prove or disprove a consequential fact in the litigation.[79]

5.2.3 Authenticity

5.2.3.1 Overview

If evidence is not relevant, the inquiry ends, as evidence that is not relevant is never admissible. The second requirement of authenticity should be considered. To be admissible, the evidence must be authentic. In an American case of Lorraine, Justice Grim refused to allow either party to offer emails in evidence in support of their summary judgment motions due to non-compliance with the rules of authentication. He found that they failed to meet any of the standards for admission under the Federal rules of evidence. In that case, the emails were not authenticated but simply attached to their pleadings as exhibits, as has been the common practice. Even though neither party directly challenged the admissibility of the other's emails evidence, the court was not in a position to consider emails, because there were no basis provided by the parties for admissibility or authentication.

Similarly, in Lazarus case, Justice Makaramba concluded that plaintiffs have not been able to cross the hurdle of proving the authenticity of the e-mail they are seeking to produce in evidence. An interview with him revealed that parties in Lazurus case decided to settle the dispute out of court.[80] The assumption that can be drawn from this scenario is that it is very hard to meet the established standards. As stated above, the most difficult hurdle to meet is that which revolves around authentication of digital evidence.

In Arusha, the High Court rejected admissibility of flash disc into evidence for the reason that the procedure for admissibility of electronically generated evidence have not been complied with. In *R. v. Deodata and Another*, Criminal Number 209 of 2010 a Resident Magistrate at the Resident Magistrate Court of Dar es Salaama at Kisutu denied phone call records admissibility due to the fact that the proponent did not lay a proper foundation for admissibility of a computer printout bearing such call records. In *R. v. Gwajima,* the Kisutu Resident Magistrate's court refused to accept as an exhibit a CD – Video-taped allegedly showing how the leader of Glory of Christ of Tanzania Church insulted Polycarp Cardinal Pengo because the Prosecution failed to bring the person who video-recorded the CD.[81]

From the above analysis, the most difficult hurdle to cross is that which requires electronic evidence to be authenticated before it is admitted in evidence. It is for this

[79] See p. 27 of Loraine.
[80] An Interview conducted with Justice Makaramba on phone on 16th May, 2014.
[81] See Daily News, ISSN 0856-3812, No. 11, 675, dated 28/04/2016.

reason this section delves into a discussion on how to comply with authentication requirement in order for electronically generated records to be admissible in Court.

5.2.3.2 Meaning of Authentication

Authentication is the process of determining whether the evidence is trustworthy.[82] The term 'trustworthiness' is often used to describe that a thing deserves, or is entitled to, trust or confidence. As Hearther[83] puts it, there are two qualitative dimensions to the concept of trustworthiness.[84] These are reliability and authenticity. Reliability is meant to demonstrate the record is capable of standing for the facts to which it attests, and authenticity means the record is what it claims to be. The purpose of best evidence rule is to increase the probability of the trustworthiness of the document by reducing the opportunity for the deliberate or inadvertent alteration of the document.[85]

The UK Association of Chief Police Officers[86] stated the nature of electronic evidence in the following words:

> Computer-based electronic evidence is, by its very nature, fragile. It can be altered, damaged, or destroyed by improper handling or improper examination. For this reason, special precautions should be taken to document, collect, preserve and examine this type of evidence. Failure to do so may render it unusable or lead to an inaccurate conclusion.

It is for this reason that the requirement to authenticate electronic evidence is usually the most difficult to overcome as courts seek to determine its admissibility. The term 'authentic" from which the term authentication stems is defined by Black's Law Dictionary as 'genuine; true; real; pure; reliable; trustworthy; having the character and authority of an original; duly vested with all necessary formalities and legally attested to be competent, credible and reliable as evidence'.

The term "authentic" as pointed out by Mason is used to describe whether a document or data is genuine. Authenticity can only exist if the three elements are in place. These are reliability, integrity and usability. Mason suggests further that:

> As such authenticity is an implicit value derived or presumed from the presence of the explicit elements that characterize the other three characteristics. A presumption of authenticity is an inference that is drawn

[82] Casey, E., *Digital Evidence and Computer Crime: Forensic Science, Computers and the Interne*, 2nd ed., Elsevier: New York, 2004, p. 172.
[83] Heather MacNeil Trusting Records Legal, Historical and Diplomatic Perspectives (2000), p xi; see Livia lacovino Recordkeeping, Ethics and Law (2006) p 41, for further comments about 'trustworthiness'.
[84] *Ibid*.
[85] Mason, *op.cit*, p. 62.
[86] See the ACPO, *op.cit*, p. 6.

from known facts about the manner in which record has been created, handled, and maintained.

5.2.3.3 Judicial Requirements for Authentication

Judicial requirements for authentication of any type of evidence is not new in Tanzania. In an old case of *Gerald Ngaiza v. Issa Ibrahim*[87] it was held that paper evidence without proof of source and authenticity should not be admitted. The same position was also in *Hussein v. Republic*.[88] On the manner to authenticate a document it was held in *Nicholas Alfred Kiyabo v. Republic*[89] that when a person is seen writing or signing a document it is not necessary to call for a handwriting expert or someone acquainted with the person's signature. The witnesses who saw the appellant signing the document was held to be sufficient. These decisions demonstrate the need for any person wishing to rely on any kind of evidence to lay a proper foundation for its admissibility.

The Makaramba J., in Lazurus case is of the view that:

> Our Evidence Act, 1967 however does not contain any express provision on authentication and identification of electronically stored information as is the case with the Kenyan Evidence Act or the United States Federal Rules of Evidence. The underlying concept under the Evidence Act, 1967 is relevancy of evidence to the facts in issue.

According to Makaramba J., authentication of electronically stored information may require greater scrutiny than that required for the authentication of "*hard copy*" documents but this does not mean abandoning the existing rules of evidence when doing so. This is based on the fact that electronic documents or records that are merely stored in a computer raise no computer-specific authentication issues.

In Lazarus case, Makaramba J., directed that the party seeking electronically generated evidence must provide authenticating facts for the e-mail and other evidence that the party wish to proffer in support of its case but not simply to attach the exhibits. Absence of authentication strips the e-mails of any evidentiary value because the court cannot consider them as evidentiary facts. The Plaintiff has to cure the evidentiary deficiencies. The Plaintiffs' Counsel needs to plan which method or methods of authentication that will be most effective, and prepare the necessary formulation, whether through testimony, affidavit, admission or stipulation. The proffering Counsel needs also to be specific in presenting the authenticating facts and, if authenticity is challenged, should cite authority to support the method selected.

---

[87] *Gerald Ngaiza v. Issa Ibrahim,* (1974) LRT n.13[HC].
[88] *D. Hussein v. Republic*, [1975] LRT n. 45.
[89](1987) TLR 59 (HC).

The requirement to authenticate electronic evidence was also pointed out by Nyangarika J., in Exim in the following words:

> It must be born in mind that electronic evidence must be authenticated because of the potential for unauthorized transaction or of the processing of such evidence. There is also a need to know the history, source and custody of such kind of evidence.

Judge Grimm in Lorraine's case also recognized that authentication of electronically stored information may require greater scrutiny than for the authentication of 'hard copy' documents. In his words:

> Given the pervasiveness today of electronically prepared and stored records as opposed to the manually prepared records of the past, counsel must be prepared to recognize and appropriately deal with the evidentiary issues associated with the admissibility of electronically generated and stored evidence.

In an English case of *R v. Robson and Harris,*[90] it was observed, inter alia, that a person producing a record as evidence must describe its provenance and history so as to satisfy the judge that there is a prima facie case that the evidence is authentic.

5.2.3.4 Authentication under the Law of Evidence Act, 1967

In Tanzania, the general rule is that no writing can be admitted in evidence, unless its execution and genuiness is proved. Sections 69 – 75 of the Law of Evidence Act provide for proof of the execution of the document. Authentication is achieved by way of proof of signatures under section 69 which provides that:

> if a document is alleged to be signed or to have been written wholly or in part by any person, the signature or the handwriting of so much of the document as is alleged to be in that person's handwriting must be proved to be in his handwriting.

The section requires that the signature of the person who is alleged to have signed or made the document, must be proved. There are several modes of proving a signature or writing. These are: by calling a person who signed or wrote a document; by calling a person in whose presence the document was signed or written, by calling a handwriting expert, by calling a person acquired with the handwriting of the person by whom the document is supposed to be signed or written, by comparing in court the disputed signature or writing with some admitted signature or writing, by proof of admission by the person who is alleged to have signed or written the document that the signed or wrote it, by the statement of the deceased

[90] *R v. Robson and Harris,* [1993] All ER 225.

professional scribe made in the ordinary course of business that the signature on the document is that of a particular person. In this respect, a signature is proved to have been made at the request of a person by some other person, e. g., by the scribe who signed on behalf of the executants and lastly by other circumstantial evidence.

Section 78 and 79 provides for rules to authenticate records in bankers' books. It provides that:

> S. 78-(1) A copy of any entry in a banker's book shall not be received in evidence under this Act unless it first proved that the book was at the time of the making of the entry one of the ordinary books of the bank and that the entry was made in the usual and ordinary course of business and that the book is in the custody or control of the bank.
>
> (2) Such proof under subsection (1) may be given by a partner or officer of the bank and may be given orally or by an affidavit sworn before any commissioner for oaths or person authorized to take affidavits.
>
> S. 78B (1) a printout of any entry in the books of a bank on micro-film, computer, information system, magnetic tape or any other form of mechanical or electronic data retrieval mechanism obtained by a mechanical or other process which in itself ensures the accuracy of such print out, and when such print out is supported by a proof stipulated under subsection (2) of section 78 that it was made in the usual and ordinary course of business, and that the book is in the custody of the bank, it shall be received in evidence under this Act.
>
> (2) Any entry in any banker's book shall be deemed to be primary evidence of such entry and any such banker's book shall be deemed to be a "document" for the purposes of subsection (1) of section 64.
>
> 79.-(1) A copy of an entry in a banker's book shall not be received in evidence under this Act unless it be further proved that the copy has been examined with the original entry and is correct. (2) Such proof shall be given by some person who, has examined the copy with the original entry, and may be given either orally or by an affidavit sworn before any commissioner for oaths or person authorized to take affidavits.

Having found that the standards on authenticating banking records were not sufficient, Nyangarika J., in *Exim Bank (T) Ltd v. Kilimanjaro Coffee Company Limited (citation)* filled the *lacuna* by adopting the guidelines governing authentication of such print outs pertaining in India. In this respect the Judge directed that for purposes of authentication, electronic evidence or electronic generated information in the form of print outs under ss 78 and 79 have to be accompanied by; first, a

certificate to the effect that it is a print out of such an entry by the accountant or branch manager of the relevant bank and second, a certificate by a person in charge of a computer system containing a brief description of the computer system and particulars of the safeguards adopted by the system to ensure that first, data is entered or any other operation performed only by authorized persons, second, all safeguards were adopted to prevent and detect unauthorized changes of data, third, the safeguards are available to retrieve data that is lost due to systems failure or any other reasons, fourth, the manner in which data is transferred from the system to removable media like floppies, disks, copies or other electronic magnetic data storage devices, fifth, the mode of identification of such data storage devices, sixth, the safeguards to prevent and detect any tempering with the system and, lastly, any other facts which will vouch for the integrity and accuracy of the system.

The Judge went further to state that there is a need for further certificate from the person in charge of the computer system to the effect that to the best of his knowledge and belief, such computer system, operated properly at the material time when he was provided with all the relevant data and print out in question represent correctly or is appropriately derived from the relevant data.

The judge appeared to have amended the law of evidence Act to incorporate the Indian guidelines on authentication of computer print outs from banker's books and having applied them to the case at hand, he ruled the Plaintiff did not lay a foundation for admissibility of the same in the following words:

> However, in the present case, no evidence was led the plaintiff's counsel or PW1 to show that the print outs statements originated from the Plaintiff's bankers book and that the bankers book was at the time of making of the entry one of the ordinary books of the plaintiff's bank. Furthermore, there is no proof that the entry was made in the usual course of business of the plaintiff's bank and that the book is still in the custody or control of the plaintiff bank.
>
> Furthermore, no evidence was led by Plaintiff counsel or PW1 to show that the print outs statements were examined with the original entry and are correct.
>
> There is also not certificate of Accountant or Manager and by a person in charge of the Computer System containing a brief description of the Computer system and particularly from where the prints outs statement were retrieved for purposes of authenticity showing that the print outs statements were not tempered with and are correct in every respect.

The above standards as assimilated by Nyangarika, J., into our means Tanzania legal system appear to be restrictive to banks records. It is argued here that the same standards or rules should be made applicable to all types of an electronically generated document.

5.2.3.5 ***Authentication under the Electronic Transactions Act of 2015***

Under section 64A of the Evidence Act, the weight, admissibility and authenticity of an electronic piece of evidence will be determined upon a proffer fulfilling the requirements under section 18 of the Electronic Transactions Act of 2015.Section 18 (1) places electronic evidence in the same level as paper based evidence. S. 18(2) provides for factors to be considered in determining the admissibility and the weight of electronic data messages. These are: first, reliability of the manner in which the data message was generated, stored or communicated; two, the reliability of the manner in which the integrity of the data message was maintained; three, the manner in which its origin at or was identified and lastly, any other factor that may be relevant in assessing the weight of evidence.

S. 18(3) provides for factors to be presumed in respect of authenticity of an electronic records system. In other words, in order to determine whether an electronic record is authentic or not, the proponent should comply with the following requirements : first, he/she has to tender evidence that supports a finding that at all the material times the computer system or other similar device was operating properly or if it was not, the fact of its not operating properly did not affect the integrity of an electronic record and that there are no other reasonable grounds on which to doubt the authenticity of the electronic record system.

Second, he/she must establish that the electronic record was recorded or stored by a party to the proceedings who is adverse in interest to the party seeking to introduce it. Third, he/she must establish that an electronic record was recorded or stored in the usual and ordinary course of business by a person who is not a party to the proceedings and who did not record or store it under the control of the party seeking to introduce the record.

On the nature of evidence required under the above provisions, s. 18(4) provides that:

> For purposes of determining whether an electronic record is admissible under this section, an evidence may be presented in respect of any set standard, procedure, usage or practice on how electronic records are to be recorded or stored, with regard to the type of business or endeavours that used, recorded or stored the electronic record and the nature and purpose of the electronic record. (Emphasis added**)**

The proponent of the evidence must establish a chain of custody. Questions that are likely to be asked during the trial are: Who originally entered the information into the computer? What type of skill level did they have, and was the data validated? Once the data was entered, was it manipulated before being placed into a database? After data entry, how was the data maintained and who had access to it? Counsel's failure to adequately anticipate likely evidentiary challenges can prove costly.

The above provision seems to be silent on the nature of evidence required to prove the fact that the computer system or other similar device was operating properly and if it was not, then evidence to the effect that its being not operational at the material time did not affect the integrity of an electronic record. It simply says 'evidence' in respect of any set standard as far as recording or storage of electronic records is concerned. It is argued here that the law should dictate the nature of the evidence to authenticate an electronic record. The requirement that the electronic records must have been created by a person who is not a party to the proceedings leaves also much to be desired. In most cases, electronic records with evidential value are created by persons who later may be parties to the proceedings. It means therefore that electronic records can be denied admissibility simply because they were made by the party to the matter or proceedings.

The author is impressed by the wording of section 65A and 65B of the Indian Evidence Act of 1872. Section 65A provides that the contents of electronic records may be proved in accordance with the provisions of section 65B. Section 65B provides as follows:

> (1) Notwithstanding anything contained in this Act, any information contained in an electronic record which is printed on a paper, stored, recorded or copied in optical or magnetic media produced by a computer (hereinafter referred to as the computer output) shall be deemed to be also a document, if the conditions mentioned in this section are satisfied in relation to the information and computer in question and shall be admissible in any proceedings, without further proof or production of the original, as evidence of any contents of the original or of any fact stated therein or which direct evidence would be admissible.
>
> (2) The conditions referred to in sub-section (1) in respect of a computer output shall be the following, namely:
>
> > (a) the computer output containing the information was produced by the computer during the period over which the computer was used regularly to store or process information for the purposes of any activities regularly carried on over that period by the person having lawful control over the use of the computer;

(b) during the said period, information of the kind contained in the electronic record or of the kind from which the information so contained is derived was regularly fed into the computer in the ordinary course of the said activities;

(c) throughout the materiel part of the said period, the computer was operating properly or, if not, then in respect of any period in which it was not operating properly or was out of operation during that part of the period, was not such as to affect the electronic record or the accuracy of its contents; and

(d) the information contained in the electronic record reproduces or is derived from such information fed into the computer in the ordinary course of the said activities.

(3) Where over any period, the functions of storing or processing information for the purposes of any activities of any regularly carried on over that period as mentioned in clause (a) of sub-section (2) was regularly performed by computer, whether-

(a) by a combination of computers operating over that period; or

(b) by different computers operating in succession over that period; or

(c) by different combinations of computers operating in succession over that period; or

(d) in any other manner involving the successive operation over that period, in whatever order, of one or more computers and one or more combinations of computers.

All the computers used for that purpose during that period shall be treated for the purposes of this section as constituting a single computer; and references in this section to a computer shall be construed accordingly.

(4) In any proceedings where it is desired to give a statement in evidence by virtue of this section, a certificate doing any of the following things, that is to say,

(a) Identifying the electronic record containing the statement and describing the manner in which it was produced;

(b) giving such particulars of any device involved in the production of that electronic record as may be appropriate for the purpose of showing that the electronic record was produced by a computer;

(c) dealing with any of the matters to which the conditions mentioned in sub-section (2) relate, and purporting to be signed by a person

occupying a responsible official position in relation to the operation of the relevant device or the management of the relevant activities (whichever is appropriate) shall be evidence of any matter stated in the certificate; and for the purpose of this sub-section it shall be sufficient for a matter to be stated to the best of the knowledge and belief of the person stating it.

(5) For the purposes of this section,-

(a) Information shall be taken to be supplied to a computer if it is supplied thereto in any appropriate form and whether it is so supplied directly or (with or without human intervention) by means of any appropriate equipment;

(b) whether in the course of activities carried on by any official, information is supplied with a view to its being stored or processed for the purposes of those activities by a computer operated otherwise than in the course of those activities, that information, if duly supplied to that computer, shall be taken to be supplied to it in the course of those activities;

(c) a computer output shall be taken to have been produced by a computer whether it was produced by it directly or (with or without human intervention) by means of any appropriate equipment.

In a nutshell, section 65B of the Indian Evidence Act states four conditions upon which electronic records should fulfil before being admitted into evidence. These are: first, that the statement sought to be tendered was produced by the computer a period when it was in regular use; second, that during that period of regular use, information of the kind contained in the document or statement was supplied to the computer; third, that the computer was operating properly during that period of regular use; and fourth that the information contained in the statement was supplied to the computer in the ordinary course of its normal use.

Section 65B(4) requires that the party who seeks to tender a computer generated statement or document shall file a certificate to identify the document or statement, describe the manner of its production and also to state the particulars of the device used in the production of the document. The Certificate must be signed by a person occupying a responsible position in relation to the operation of the relevant device or the management of the relevant activities. A number of countries like Kenya and Nigeria[91] have similar provisions in their evidence acts.

[91] Under the Nigeria Evidence Act of 2011, the four conditions for admissibility of computer-generated evidence under Section 84(2) are that: the statement sought to be tendered was produced by the computer during a period when it was in regular use; during that period of regular use, information of the kind contained in the document or statement was supplied to the computer; the computer was operating properly during that period of regular use; and the information contained in the statement was supplied to the computer in the ordinary course of its normal use. Further, Section 84(4) requires that the party

In a recent Indian case of *Anvar P.V. v. P.K. Basheer and Others*[92] the Supreme Court it was held that secondary data in CD/DVD/Pen Drive are not admissible without a certificate under section 65 B (4) of Indian Evidence Act in view of the fact that electronic records is more susceptible to tampering, alteration, transposition, excision and that without such safeguards, the whole trial based on proof of electronic records can lead to travesty of justice.

In *US v. Briscoe*[93] the federal court stated that a proper foundation for computer records is generally established if the party presenting the computer records provides sufficient facts to warrant a finding that records are trustworthy and the opposing party is afforded an opportunity to inquire into the accuracy thereof and how the records were maintained and produced.

In *Kubor v Dickson*[94] the Supreme Court of Nigeria examined the provisions of Sections 84, 34(1)(b) and 258 of the Evidence Act 2011 regarding the concept of a 'document' and the admissibility of electronic evidence. In the leading judgment, the court stated the following:

There is no evidence on record to show that the appellants in tendering exhibits "D" and "L" satisfied any of the above conditions. In fact they did not as the documents were tendered and admitted from the bar. No witness testified before tendering the documents so there was no opportunity to lay the necessary foundations for their admission as e-documents under section 84 of the Evidence Act, 2011. No wonder therefore that the lower court held at page 838 of the record thus:-

> 'A party that seeks to tender in evidence computer generated document needs to do more than just tendering same from the bar. Evidence in relation to the use of the computer must be called to establish the conditions set out under section 84(2) of the Evidence Act 2011.'

I agree entirely with the above conclusion. Since the appellants never fulfilled the pre-condition laid down by law, Exhibits "D" and "L" were inadmissible as computer generated evidence."

The appellants' appeal was accordingly dismissed.

---

which seeks to tender a computer-generated statement or document shall file a certificate: identifying the document or statement; describing the manner of its production; stating the specifications of the device used in the production of the document; and signed by a person occupying a responsible position in relation to the operation of the relevant device or the management of the relevant activities.

[92] [MANU/SC/0834/2014].

[93] 896 f.2d 1476 at page 1494-95 (7th Cir.1990).

[94] (2014) 4 NWLR Pt 1345, pages 534-594 accessed at http://www.lexology.com/library/detail.aspx?g=f16ede4c-f04a-40a7-96c3-e6a4899f3cf0.

This is also the spirit behind the decision by Nyangarika J., in *Exim's case*.[95] Our law should also have similar wordings and it is at this point that I strongly urge the Parliament to amend this provision accordingly. Otherwise, it will be very difficult for any piece of electronic evidence to be admissible into evidence in Tanzania.

5.2.4 The Hearsay Rule

The third requirement for admissibility of electronic evidence is subject to the hearsay rule. Therefore, a document, electronic or otherwise, is not admissible to prove the truth of its contents unless it falls within one of the exceptions to the hearsay rule. Hearsay is an out-of-court statement offered in court to prove the truth of the matter asserted by the out-of-court declarant. It is offered into evidence through the testimony of a witness to that statement or through a written account by the declarant. The hearsay rule excludes such evidence because it possesses the testimonial dangers of perception, memory, sincerity, and ambiguity that cannot be tested through oath and cross-examination.[96]

There are five separate questions that must be answered: First, does the evidence constitute a statement; second, was the statement made by a "declarant"; third, is the statement being offered to prove the truth of its contents; fourth, is the statement excluded from the definition of hearsay; and lastly, if the statement is hearsay, is it covered by one of the exceptions to the hearsay rule. It is critical to conduct a proper hearsay analysis by considering each of the above questions.[97]

The second question that must be answered in the hearsay analysis is that a "writing" or "spoken utterance" cannot be a "statement" under the hearsay rule unless it is made by a "declarant", that is, a person who makes a statement. The key to understanding the hearsay rule is to appreciate that it only applies to intentionally assertive verbal or non-verbal conduct, and its goal is to guard against the risks associated with testimonial evidence: perception, memory, sincerity and narration. Cases involving electronic evidence often raise the issue of whether electronic writings constitute "statements."

The third question that must be answered in determining if evidence is hearsay is whether the statement is offered to prove its substantive truth, or for some other purpose. Once it has been determined whether evidence falls into the definition of hearsay because it is a statement, uttered by a declarant, and offered for its substantive truth, the final step in assessing whether it is hearsay is to see if it is excluded from the definition of hearsay. Judge Grim commented that given the near universal use of electronic means of communication, it is not surprising that statements contained in electronically made or stored evidence often have been

[95] Commercial Case No. 29 of 2011 (Unreported).
[96] Paul R. Rice, ***Electronic Evidence: Law And Practice***, 262 (Aba Publishing 2005)

[97] *Lorraine* case.

found to qualify as admissions by a party opponent if offered against that party citing **Siddiqui case**, 235 F.3d at 1323 (ruling that e-mail authored by defendant was not hearsay).

5.2.5 The original writing rule

The third requirement to be fulfilled in respect with admissibility of electronic evidence is that of original. Any proponent of an electronic evidence must determine whether the original writing rule is applicable, and if so, the Counsel must be prepared to introduce an original, a duplicate original, or be able to demonstrate that one of the permitted forms of secondary evidence is admissible. The original writing rule has particular applicability to electronically prepared or stored writings, recordings or photographs. When the contents of any electronic evidence are at issue, the proponent is required to prove its content by presenting the original, being the best evidence. In absence of the original, the proffer is allowed to present a duplicate under the secondary evidence rules. The challenge as far as electronic records are concerned is what amount to original or duplicate?

Justice Makaramba is of the view that the definitions of "*writings, recordings and photographs*" in the Tanzania Evidence Act include evidence that is electronically generated and stored. Traditionally the rule requiring the original centered upon accumulations of data and expressions affecting legal relations set forth in words and figures. This meant that the rule was one essentially related to writings. Present day techniques have expanded methods of storing data, yet the essential form that the information ultimately assumes for useable purposes is words and figures.

The U.N. Model law contains the following provision:

> Article 9: Admissibility of evidential value of a data record (1) In any legal proceedings, nothing in the application of the rules of evidence shall apply so as to prevent the admission of a data record in evidence
>
> > (a) on the grounds that it is a data record; or,
> > (b) if it is the best evidence that the person adducing it could reasonably be expected to obtain, on the grounds that it is not an original document.
>
> (2) Information presented in the form of a data record shall be given due evidential weight. In assessing the evidential weight of a data record, regard shall be had to the reliability of the manner in which the data record was generated, stored or communicated, to the reliability of the manner in which the information was authenticated and to any other relevant factor.

As pointed out earlier this article, section 4 of the Electronic Transactions Act of 2015 has recognized documents in electronic form and that they should not be denied admissibility simply because they are in electronic form. With this provision, data messages have been given functional equivalence to writing in tangible format and their authenticity and weight are subjected to the conditions under sections 18 of the same Act as discussed above.

According to the provisions above, if four main criteria are fulfilled, any information contained in an electronic record which is printed on paper, stored, recorded or copied in an optical or magnetic media, produced by a computer is deemed to be a document and becomes admissible in proceedings without further proof or production of the original.

In Botswana under the Electronic Records (Evidence) Act, 2014, is a bit more elaborate on the requirement of original in respect of electronic records/evidence. Section 7 provides that the best evidence rule in respect of an electronic record shall be satisfied on proof of the integrity of the electronic records system in or by which the data contained in the electronic record was recorded or stored; or if the electronic record contains an electronic signature that was added when the electronic records was first generated in its final form and that can be used to verify that the electronic record has not been changed since that time.

5.2.6 The need to balance its probative value against the potential for unfair prejudice, or other harm

According to Judge Grim, when a lawyer analyses the admissibility of electronic evidence, he or she should consider whether it would unfairly prejudice the party against whom it is offered, confuse or mislead the jury (or assessors in this part of the world), unduly delay the trial of the case, or interject collateral matters into the case. Courts are particularly likely to consider whether the admission of electronic evidence would be unduly prejudicial in the following circumstances: first, when the evidence would contain offensive or highly derogatory language that may provoke an emotional response; second, when analysing computer animations, to determine if there is a substantial risk for mistaking them for the actual events in the litigation; third, when considering the admissibility of summaries of voluminous electronic writings, recordings or photographs and lastly, in circumstances when the court is concerned as to the reliability or accuracy of the information that is contained within the electronic evidence.

6.0 Conclusion

This paper aimed at investigating the required standards for proper foundation of admissibility of electronic evidence in the courts in Tanzania. This type of evidence

emanates from electronically stored information, a few examples of which are emails, website data and postings, online social media and mobile phone calls, text messages as well as GPS data.

It was found in this paper that electronic evidence is now admissible in courts of law to prove or to disprove any issue in courts of law in both criminal and civil proceedings subject to laying a proper foundation. For such proper foundation to be laid, the e-evidence should pass through a number of tests as established under section 18–20 of the Electronic Transactions Act, 2015as well as judicial pronouncements as discussed in this discourse. In essence, these rules range from authenticity, relevance, rules against hearsay, and the best evidence rule. A proponent who fails to meet these tests will not be allowed to rely upon any piece of electronic evidence.

It was observed that the most important hurdle that presents difficulties in meeting is authentication. Authenticating electronic evidence at trial requires preparation from the discovery phase onwards. The challenge presented by the law revolves around this requirement - 'to prove reliability of the equipment and mode of entering data'. The lesson learnt is that the foundation for admissibility of electronic evidence ought to begin way back before litigation is contemplated. It implies that businesses and individuals should maintain a clear procedure and policy on handling electronic evidence as the same is a potential mine in litigation.

It was further observed that section 69 of the Tanzanian Evidence Act, 1967 contains rules for authentication of documents. This does not cover other types of evidence as discussed in this paper. It was also found out that while sections 78 and 79 of the Tanzania Evidence Act of 1967 contain rules in respect of authentication of bankers' books, section 69 provides for authentication of handwriting and signatures. It is argued here that this distinction is not necessary when it comes to authentication of computer print outs or electronically stored information generally.

7.0 Recommendations

In view of the complexity of electronic evidence, it is recommended that continuous legal education should be conducted for judges, magistrates, advocates, prosecutors and investigators. If the need arises, cyber forensic experts should be used in case the court needs to get an independent opinion on any matter involving modern technologies.

The study recommends that section 69 of the Tanzania Evidence Act of 1967 should be amended to introduce words to the effect that the requirement of authentication or identification is a condition precedent to admissibility and it is satisfied by

evidence sufficient to support a finding that the matter in question is what its proponent claims. The study further proposes an amendment to this provision to the effect that any person seeking admissibility of any type of evidence should lead evidence describing a process or system used to produce a result and showing that the process or system produces an accurate result.

Another provision worth adding to the Law of Evidence Act, 1967 is the one that should allow authentication or identification provided by the Act of Parliament or by other rules prescribed by the highest court in the hierarchy pursuant to statutory authority. The rationale of the proposed amendment is to give legal effect to the efforts by a few pro-active judges seeking to accommodate changes brought about by the ever advancing technologies.

It is recommended that sections 69 and 78 &79 merged to govern authentication of electronically stored information in the country. A good example in this respect are provisions of the US Federal Rules of Evidence which have been written in a more general manner to accommodate all evidence including evidence in electronic form.