Presentation, Admissibility and Assessment of Digital and Forensic Evidence in Cybercrime Cases

Jane Okuo Kajuga
Judge

Introduction

Cybercrimes are offenses that are committed through use of technology, where the computer or systems can be the tools for commission of crime, or the target.

Technology can enforce the commission of other offenses - Ordinary offenses increasingly have elements of electronic evidence (Kato Kajubi)

E-fraud – ATM/Mobile money frauds,

Uganda versus Ssentongo and 4 others: Case No 123/2012

Accused stole money from the MTN Mobile money platform FUNDAMO by creating fictitious journals, exiting the money through fake subscribers and access shops

Child pornography: Cyber harassment: Offensive communication (nullified)

Unauthorised access into computers /systems, **Asycuda system (URA)** damaging, altering or modifying data (attacking the integrity of the systems, malicious software, ransomware, DOS attacks)

Cont'd

In everyday transactions, computers are used; Emails are sent, phone conversations are held and recorded, text messages are sent, pictures are taken and stored, documents are shared

CCTV cameras and other digital devices are also used to collect, store and transmit messages that contain evidence relating to crimes.

Every contact with a computer leaves a lot of evidence, some of which is easily detected, others require digital forensic expertise and tools

E-Evidence thus includes:

Data: Electronic representations of data in any form

Data messages: Data generated, sent, received or stored by a computer and includes voices and stored records

Cont'd

Electronic Records: Data stored or recorded on any medium in or by a computer system or other similar device that can be read or perceived by any person or a computer system or other related device and includes a display, printout or other output of that data

Broad spectrum of evidence covered: raw data, photos, files, log data, server logs, network logs, time stamps, IP addresses, videos and images on mobile phones, digital cameras, system access records, email and email logs and headers, security alerts, voice recordings, chats, posts on social media e.g. Facebook, tiktok, WhatsApp, Instagram, you tube clips, any form of electronic communications and information sharing systems e.g. office mails

NB (ever changing and developing sphere)

E-Evidence definition

Evidence generally denotes the means by which an alleged matter, the truth of which is subjected to investigation is proved or disproved. What is used to prove facts in issue, or facts from which facts in issue may be deduced

E-Evidence is aptly defined by Justice Mutonyi Margaret in ***Amongin Jane Frances Okili versus Lucy Akello HCT-02-CV-EP-001-2014)***

> ***" Any probative information stored or transmitted in digital form that a party at a trial or proceeding may use to prove a particular proposition or to persuade court of the truth of an allegation"***

NB Information generated in digital form also included in Electronic transactions Act, 2011

Evolution

Uganda's Evidence Act Cap 6, fashioned on the Indian Evidence Act and British Common law emphasized the best evidence Rule, to avoid admission of forged documents. It required the production of the original where evidence is in writing.

With the advances in technology, the provisions of our law were inadequate to handle the admission of electronic evidence. The Electronic Transactions Act, Computer Misuse Act and Electronic Signatures Act were enacted in 2011.

The volatile nature of e-evidence and its capacity for manipulation requires different standards for its retrieval, storage and admissibility. These standards are tied to the integrity of the computer/System, the persons involved in the retrieval, and the methods of authentication, among others.

Retrieval

Part 3 Computer Misuse Act provides for investigations and procedures

- Preservation orders – Upon court order, IO can secure such order for preservation of information stored on computer/system to prevent its loss or modification (Transcriber information, traffic data)
- Disclosure of preserved data – also by court order; also includes data on the pathways, electronic keys for access
- Production orders: compel any persons to provide data stored/in his possession; Service provider's submitting subscriber information (mobile money transaction statements)

  You must analyse the form in which the data was taken (minus alterations)

The law

S. 5. ETA Legal effect of electronic records

(1)Information shall not be denied legal effect, validity or enforcement solely on the ground that it is wholly or partly in the form of a data message

(3)Where—(a)an act;

(b)a document; or

(c)information

is required to be in writing, produced, recorded or retained, it may be written, produced, recorded or retained in electronic form.

The law

Section 7 Authenticity of data message

(1)Where a law requires information to be presented or retained in its original form, the requirement is fulfilled by a data message if—

(a)the integrity of the information from the time when it was first generated in its final form as a data message or otherwise has passed assessment in terms of subsection (2); and

(b)that information is capable of being displayed or produced to the person to whom it is to be presented.

This introduces the parameters of admissibility; integrity of the e-evidence (has it been changed or altered?), and its authenticity (is the document what it Purports to be). These shall be pursued later, after the parameter of relevance

Relevance

Section 4 - Evidence Act

Evidence may be given in any suit or proceeding of the existence or nonexistence of every fact in issue and of such other facts as are hereafter declared to be relevant, and of no others.

What constitutes relevant facts are covered in Part II of the Act, and include:

#Existence of course of business

#facts on whether acts were intentional or accidental

#Facts showing the existence of state of mind, body, feeling

#Facts that enable courts to determine amount

#Facts constituting motive or preparation for any fact in issue or relevant fact

#Facts forming part of the same transaction

NB The e-evidence must pass the test of relevance to the issues being investigated by the court.

Cont'd

In criminal proceedings, the admissibility and reliability of e-evidence may be challenged on several grounds suggesting alteration or lack of reliability:

#the method and medium of storage

#the retrieval process, its integrity and legality

the content

#the form of the evidence

#the origin of the data

Therefore, the party seeking to introduce the e-evidence must lay a proper foundation justifying its admissibility.

NB: THIS IS THE PROBLEM AREA

Laying the foundation

This is often overlooked until it becomes a problem. Often elicits objections on grounds that no foundation has been laid warranting the admission of the evidence. It should be remembered that where the court does not admit the evidence, it is useless to the case.

NB

1. Evidence received and marked for identification are not exhibits and cannot be relied upon !!!

2. Until the evidence is admitted you cannot lead evidence of the substantive content of the same !!!

3. The evidence can only be offered into evidence as an exhibit after you have laid the foundation

Laying foundation

Laid through the witness who has first-hand information about the evidence. Recall that hearsay evidence remains inadmissible even for e-evidence. Select the right witness to tender, as you would in an ordinary case involving documents or other exhibits.

#Provide the context between the witness and the item

#Where the witness is an expert, introduce his experience and qualifications to speak to his competence.. The best practice is for the expert witness to carry his credentials with him for the court to inspect

In the **Amongin case** (Supra) the party sought to rely on CD recordings made from a mobile phone. The court in resolving an objection on authenticity observed that the person who recorded the CD should have sworn an affidavit, or if an independent professional witness who recorded the proceedings had testified

Cont'd

#Look for sufficient preliminary evidence of the authenticity, relevance and integrity of the e-evidence sought to be tendered in the foundation being laid

NB The foundation laid will depend on the nature of the evidence.

Section 8 (2) ETA: A person seeking to introduce a data message or an electronic record in legal proceeding has the burden of proving its authenticity by evidence capable of supporting a finding that the electronic record is what the person claims it to be.

(3)Subject to subsection (2), where the best evidence rule is applicable in respect of an electronic record, the rule is fulfilled upon proof of the authenticity of the electronic records system in or by which the data was recorded or stored.

Section 8 (5) ETA

The authenticity of the electronic records system in which an electronic record is recorded or stored shall, in the absence of evidence to the contrary, be presumed where—

(a)there is evidence that supports a finding that at all 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 the electronic record and there are no other reasonable grounds to doubt the integrity of the electronic records system;

(Call Systems administrators, IT personnel, regular users of the system with access rights)

Security of the system- its strength, its renown, security features, access restriction, capacity of persons to alter, records of alteration etc)

No requirement for authentication certificate in ETA as Kenya

Cont'd

(b)it is established 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; or

(c)it is established that the 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.

EG **CCTV Records (example of Kamyuka alleged murder case for CCTV and Flash disc extraction) : Press recordings ; clips or posts by independent persons**

S. 8 (6)

For the purposes of determining whether an electronic record is admissible under this section, evidence may be presented in respect of set standards, 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.

(Use illicit enrichment case example to elaborate production of payment records from Public Service for illicit; and MTN standards on retrieval and archival of data)

Recall S 7 (2)- authenticity shall be assessed by determining if the information is complete and unaltered, except for the addition of an endorsement and any change which arises in the normal course of communication or storage or display

(Use example of payment records for two officers mixed up headings or titling)

Amongin case

“The proponent of e-evidence must lay a foundation which makes the evidence reliable. The foundation includes;

#Reliability of the equipment used

#manner in which basic data is initially entered

#method of storing the data and precautions taken to prevent alteration/ loss

#reliability of computer program used to process data

Measures taken to verify accuracy of the program

#Software used to preserve data in its original form

Cont'd

#Competence of the person who accessed the data

#Independent third party should be able to examine

(Use example of Namuli on third-party verification of system data and extracts

Also of Abacus)

Legality of the retrieval of e-evidence

Always consider the provisions of the law on search and seizure and retrieval of the evidence – specific laws have different provisions

See: Criminal Procedure Code Act, Police Act, Customs Laws e.g. Tax Procedures Code Act, EACCMA, Anti-corruption Act, IG Act

Computer Misuse Act, 2011

S. 28 Searches and seizures

(1)Where a Magistrate is satisfied by information given by a police officer that there are reasonable grounds for believing—

(a)that an offence under this Act has been or is about to be committed in any premises; and

(b)that evidence that such an offence has been or is about to be committed is in those premises,the Magistrate may issue a warrant authorising a police officer to enter and search the premises, using such reasonable force as is necessary.

(2)An authorised officer may seize any computer system or take any samples or copies of applications or data—

(a)that is concerned in or is on reasonable grounds believed to be concerned in the commission or suspected commission of an offence, whether within Uganda or elsewhere;

(b)that may afford evidence of the commission or suspected commission of an offence, whether within Uganda or elsewhere; or

(c)that is intended to be used or is on reasonable grounds believed to be intended to be used in the commission of an offence

Cont'd

(3)A computer system referred to in subsection (2) may be seized or samples or copies of applications or data may be taken, **only by virtue of a search warrant.**

Gaster Mugoya versus Uganda

CACA 223/2021

The Judge was criticized for having wrongly admitted and heavily relied on the prosecution's electronic evidence and exhibits that were illegally seized, illegally extracted without a search warrant, fabricated and unauthentic and without the prosecution disclosing the software tool used by the experts, ENCASE and the mirror images analysed.

Judgement

"We agree with the learned trial judge that the seizure of the items upon suspicion could have been lawful. However, the items were supposed to be returned within 72 hours under section 28 (8) of the Computer Misuse Act. They were not.

Secondly, upon seizing the computers, flash disks, external hard disk et cetera were obtained yet there was not a right to search the items for information without a warrant from a magistrate"

Since the offenses charged fell under the Computer Misuse Act, the laws on warrants and return within 72 hours as set out under that law applied, and not the EACCMA.

The appeal succeeded on the two grounds which related to e-evidence

Case example

Kakonge Umar versus Uganda :

CACA 99/2018

Appeal was on the ground that the evidence from a recorder was inadmissible as it was secondary evidence and should not have been relied on. The device on which it was recorded was not tendered, instead a CD was presented of the same.

Court did not fault the admission of the recording, instead held that it was unclear, incomprehensible, and equivocal, not self-explanatory. The meaning of futali was unclear, it could mean two different things in the context of the case.

.

Kakonge cont'd

"We note that since the invention of the first practical sound recording and reproduction device by Thomas Edison in 1877, such devices have become commonplace and are used worldwide. The process through which those devices come to record sound is reliable. Such devices include the audio recording device on which the conversation between PW 2 and the appellant were initially recorded as well as the compact Disc on which the audio was transferred to"

"The traditional distinction between primary and secondary evidence has been modified in relation to electronic information. The law now recognises that electronic information may be relied on notwithstanding that the device on which that information was originally recorded was not exhibited in the trial court." See S 7

Cont'd

"...what exists now is a classification of electronic information into authentic and nonauthentic electronic information. Where the information passes the authenticity assessment laid down in S 7 (2) it may be relied upon by a court"

The said assessment is made against the following criteria; whether the information has remained complete and unaltered except for addition of endorsement and or any other change that may occur in the normal course of communication, **and** the authenticity is assessed having regard to all other relevant circumstances

Cont'd

"In the post-Electronic Transactions Act era, 2011, it is no longer open to frustrate the admission of e-information merely because the relevant recording device has not been tendered in court"

"Having said so, we are of the considered view that in addition to the reliability test referred to, the e evidence must be clear, unequivocal and self explanatory"

In **Dr Peter Musoke Gukiina versus Sudhir Ruparelia** and others HCCS 2/2019, the judge overruled an objection that the video had been edited and admitted. It was of a TV program. Changes in normal editing are expected and S 8 (1)(c) ETA forbids denial on basis that the evidence is not in its original form

Cont'd

<u>Dian GF International Ltd versus DAMCO logistics Uganda Ltd and another</u>

<u>HCCS 161/2010</u>

An e mail introduced in evidence was attacked for non authentication, it could not be verified whether it was sent or delivered.

The judge relied on an article

"E mail evidence preservation, how to balance the obligation and the High Cost: Lex Electronica, Vol 14 n 2" on how e mails can be authenticated

(See Extract next slide)

Emails cont'd

E-mails are composed of a "header" and "body". While the body of the email contains the individual text composed by the sender, the header listing the sender's name and address, the recipient's user name and address, the transmission date and time and the subject matter of the mailing. If email is produced by a party from the party's files and on its face purports to have been sent by that party, these circumstances alone may suffice to establish authenticity. Authentication should be made through a knowledgeable witness who can identify the authorship as well as the documents appearance, contents, substance, internal patterns, or other distinctive characteristics. Given that most emails contained certain identifying markers, such as the address from which they were sent, the name of the sender, or the company name, that information, coupled with their production during discovery, should be enough to satisfy the authentication requirements.

Cont’d

“The requirement of originality for paper document is applied differently in email evidence. If data are stored in a computer or similar device, any printout readable by sight, shown to reflect the data accurately, is deemed as “original”.

To admit emails into evidence, the proponent must show the origin and integrity of emails. He must show who or what originated the email and whether the content is complete in the form intended, free from error or fabrication. In discovery, the proponent needs to prove that the hard copy of the email evidence is consistent with the one in the computer and includes all the information held in the electronic document.”

Social media evidence

May consist of posts, chats, images profiles

May be private or public (privacy laws)

Must be authentic, must be relevant and properly retrieved

Specialised social media investigation strategies may be applicable,

Full profile and meta data information –Time stamps, IP addresses,

Eliminate the chance that any other person could be responsible for the post or chat. Prove account ownership usually by meta data, witness accounts, consistent profiles

(Use example of Ministry of Education case-WhatsAppp communications extracted from phone)

Evidential weight

Once the e-evidence is admitted, the court must determine the probative value or evidential weight to attach to it.

Section 8 (4) ETA

When assessing the above, the court shall have regard to;

The reliability of the manner in which the message was generated, stored or communicated

The reliability of its maintenance

how the originator of the record was identified

(**Give an example of the DTB bank case of Uganda versus Kirumira and how he was identified)**

Case

Dr Stella Nyanzi versus Uganda

HC Cr Appeal 79/2019

In the case before the lower trial court the digital footprint and thus the domicile in Uganda of the device allegedly used in committing the offence could have been proven through a number of methods including using the device's International Mobile Equipment Identity (IMEI) number which according the website https://www.imei.info is the identity of a phone can be established through its International Mobile Equipment Identity (IMEI) number which is a number assigned to a specific device such that when that device is active, it can be tracked with precision using its IMEI since that number is its unique identifying 15-digit code

Nyanzi (cont'd)

- This information actually could have been secured from Facebook itself as can be read from its Data Policy page found at : https://www.facebook.com/policy.php where it is provided that the digital footprint left behind by a device on Facebook computers such as the operating system including the device's settings such as its GPS location, the name of mobile operators or ISP used , the language, the time zone, the mobile phone number, the IP address of the device, the connection speed of the device and in even information about other devices which were nearby could be secured from Facebook by law enforcement agencies upon request or upon court order
- NB **Mind jurisdictional issues**

General evaluation

- Do not base yourself on the isolated evidence of the prosecution...evaluate all the evidence as a whole, including the e-evidence presented
- How does evidence from one source compare with the evidence from another source
- Is it sufficient?
- Contradictions and inconsistencies, and their effect
- Believability; reliability
- Corroboration
- The relevance of the evidence; Don’t lose sight of the essential elements of the offense, and how the e-evidence fits in

THE END

THANK YOU