

ASSESSMENT OF EVIDENCE IN THE DIGITAL ERA¹

Petrus T Damaseb²

Introduction

My host has asked me to speak on *Assessment of evidence in the Digital era*.

It is a subject on which as a Judge I am no stranger - but certainly not an expert. But as judges always do - we deal with whatever is brought before us!

I have assumed that what is intended by the assignment is to give my perspective on how a trier of fact should go about making findings of fact when faced with digital evidence.

But what is the nature of the beast? What is digital evidence?

Digital evidence comes from three main sources: The Internet, computers and portable devices. In other words, information

¹ Zimbabwe JSC's Bar- Bench Colloquium held 24-27 November 2022 at Caribbea Bay Resort, Kariba, Zimbabwe.

² Deputy Chief Justice of the Republic of Namibia.

gathered in online conversations, emails, message boards, chat rooms and file sharing networks.

Now, you will readily recognize the potential treasure-trove *that* represents for criminal investigators and any party bearing the onus.

It is a truism that because of the prevalence of digital devices, ‘evidence is now present or potentially present in almost every crime’.³

But just as it presents opportunities in the investigation, detection and prosecution of crime (or proof of a claim in a civil case) digital evidence poses challenges of collection, analysis and interpretation - to meet the requisite standard of proof. I will return to this theme presently.

Basic rule of the common law

As Adrian Keane⁴ observes: ‘the broad governing principle underlying the English law of evidence can be stated in no more than nine words: all relevant evidence is admissible subject to the exceptions’. He goes on to state:

‘In an ideal world, where parties to litigation disputes [or assert] the existence of certain facts, all available evidence which is relevant, in the

³ Association of Chief Police Officers (UK) Good Practice Guide for Digital Evidence at para 3.2.

⁴ The Modern Law of Evidence (1985) Professional Publishers, Oxon, p 1.

sense that it is logically probative or disapprobative of the existence of those facts, should be taken into account by the court.⁵

What the above means is that the most important criteria for the reception of any evidence are its admissibility, relevance and reliability.

It is trite that admissibility is a matter of law: in other words, the law (either statutory or common law) dictates which evidence is inadmissible or admissible as the case may be. Therefore, if it is not barred by either statute or the common law⁶, all evidence with a probative value will be admitted by the court. Digital evidence is no exception.

Most jurisdictions have a civil, criminal or computer evidence statute⁷. Ordinarily, those will be the first points of call to ascertain whether any item of digital evidence passes muster.

⁵ Ibid, footnote 4.

⁶ For example, hearsay evidence.

⁷ For example, in Zimbabwe see s 258 of the Evidence Act [Cap 9:07] and s 281 (3) of the Criminal Procedure Act. In Namibia and South Africa, see s 210 of the Criminal Procedure Act 51 of 1977 and s 34(1) of the Civil Proceedings Evidence Act 25 of 1965.

Challenges

One, if not the most important, challenge about digital evidence is its reliability and authenticity which are the function of three things: integrity of collection; integrity of preservation and skill in its presentation to court.

Digital forensics therefore assumes a critical role when it comes to the reception and assessment of digital evidence. People need to be properly skilled in the value chain of digital evidence collection, prosecution and presentation. It is expecting too much of judicial officers to make favorable findings of fact in favour of the presenter of digital evidence that has been incompetently handled.

A very useful guide to action are the set of guidelines regularly published by the *Association of Chief Police Officers of England Wales & Northern Ireland: 'The Guide for Digital Evidence'*.⁸

This Guide states, correctly in my view, that 'digital evidence is subject to the same rules and laws that apply to documentary evidence'. My view of the matter is that - depending on the form it takes - digital evidence would fall under either documentary or real evidence as understood under the common law.

⁸ <https://athenaforensics.co.uk/acpo>.

In *Ndlovu v Minister of Correctional Services and another* [2006] 4 All SA 165 (W) (at page 172) Gautschi AJ held that the admissibility of an electronic communication will depend on whether it is treated as real evidence or as a document.

Adrian Kean has suggested that documentary evidence would *'include not only documents in writing but also maps, plans, graphs, drawings, photographs, discs, tapes, video-tapes, films ... [and that such evidence] may be produced to show their contents, their existence or their physical appearance'*.⁹

The same author suggests that the *'contents of a document may be received as evidence of their truth, by way of exception to the hearsay rule, or for some other purpose, for example to identify the document or to show what its author thought or believed.'*¹⁰

Real evidence on the other hand *'usually takes the form of some material object produced for inspection in order that the court may draw an inference from its own observation as to the existence, condition or value of the object in question'*.¹¹

⁹ Ibid, p 10.

¹⁰ Ibid p 10-11.

¹¹ Ibid p 11.

Real evidence and documentary evidence, while they are important sources of evidence and will invariably be decisive proof of facts in dispute, will be worthless *‘in the absence of some accompanying testimony identifying the object in question and explaining its connection with or significance in relation to the facts in issue or relevant to the issue’*.¹²

I return to the theme of authenticity and reliability. In assessing the probative value of digital evidence, a court should, I propose, take a common-sense approach.

Yardsticks for testing reliability of digital evidence

As the ACPO Guide recognises, reliability of digital evidence will depend on:

- Whether the investigator is able to demonstrate an audit trail or other record of all processes applied in obtaining the digital evidence;
- Whether the presenter of the digital evidence can demonstrate how the evidence was recovered and show each process through which it was obtained; that it was preserved in a manner that an independent third party is able to repeat the same process and arrive at the same result as that presented to the trier of fact;

¹² Ibid, p 11.

- Whether an independent third party will be able to examine those processes and achieve the same result;
- Whether there is not the possibility that any action was taken by the collector of the evidence which could have tainted the incriminating digital data;
- Whether the evidence was collected by a person who is competent to do so and is able to explain its relevance to the issues before court;
- Whether the collector of the evidence ensured that all relevant laws were complied with.

A court faced with the task of assessing digital evidence must at all times bear in mind who bears the burden of proof. The duty lies on the party that bears the burden to satisfy the trier of fact that the evidence collected from the digital source is reliable and authentic. This note of caution is based on the reality that digital evidence can be easily altered. As the ACPO Guide recognises (at para 2.2.3):

‘Operating systems and other programs frequently alter, add and delete the contents of electronic storage. This may happen automatically without the user necessarily being aware that the data has been changed.’

At all events, the court should bear in mind that it is there to ensure fairness and compliance with the law. It will therefore be concerned about breaches of the law that infringe upon the subject’s

constitutional rights against invasion of privacy and unauthorized search and seizure.

Lessons

The court receiving the evidence must be satisfied of the objectivity of the presenter and his or her competence in extracting it.

Law enforcement agencies must offer training to investigators and prosecutors in digital forensics and ensure that they are familiar with the process of giving evidence in court.

In my view, the ACPO Guide represents sound practice. Based as it is on good practices and standards developed and refined from time to time by law enforcement practitioners in a jurisdiction with some of the most sophisticated criminal investigation techniques, if applied with necessary modifications, the Guide can assist investigators, legal practitioners and the court.

If properly followed by investigators it can reinforce the integrity of the information received. On the other hand, it can be used by the opposing side – subject to the proper foundation being laid – to challenge the credibility of digital evidence being presented to court.

In conclusion, I accept that there is room for legislation in the area of digital evidence, especially to create a basic floor of rights in favour of the citizen against unfairness and arbitrariness. But I take the view that it is an area that should not be over-regulated but should be left to the wisdom and experience of the judges to develop the common law on a case by case basis.

I thank you