The Search and Seizure of Digital Evidence by Forensic Investigators in South Africa

JGJ Nortjé* and DC Myburgh**

P·E·R

Pioneer in peer-reviewed, open access online law publications

Authors

Jacobus GJ Nortjé

Daniel C Myburgh

Affiliation

North-West University
South Africa

Email

Koos.Nortjie@nwu.ac.za
dc@cyanre.co.za

Date Submission

6 April 2018

Date Revised

2 April 2019

Date Accepted

5 April 2019

Date published

25 April 2019

Editor Prof C Rautenbach

How to cite this article

Nortjé JGJ and Myburgh DC "The Search and Seizure of Digital Evidence by Forensic Investigators in South Africa" *PER / PELJ* 2019(22) - DOI http://dx.doi.org/10.17159/1727-3781/2019/v22i0a4886

DOI
http://dx.doi.org/10.17159/1727-3781/2019/v22i0a4886

Abstract

The discipline of digital forensics requires a combination of skills, qualifications and knowledge in the area of forensic investigation, legal aspects and information technology. The uniqueness of digital evidence makes the adoption of traditional legal approaches problematic.

Information technology terminology is currently used interchangeably without any regard to being unambiguous and consistent in relation to legal texts. Many of the information technology terms or concepts have not yet achieved legal recognition.

The recognition and standardisation of terminology within a legal context are of the utmost importance to ensure that miscommunication does not occur.

To provide clarity or guidance on some of the terms and concepts applicable to digital forensics and for the search and seizure of digital evidence, some of the concepts and terms are reviewed and discussed, using the Criminal Procedure Act 51 of 1977 as a point of departure.

Digital evidence is often collected incorrectly and analysed ineffectively or simply overlooked due to the complexities that digital evidence poses to forensic investigators. As with any forensic science, specific regulations, guidelines, principles or procedures should be followed to meet the objectives of investigations and to ensure the accuracy and acceptance of findings. These regulations, guidelines, principles or procedures are discussed within the context of digital forensics: what processes should be followed and how these processes ensure the acceptability of digital evidence. These processes include international principles and standards such as those of the Association of Chiefs of Police Officers and the International Organisation of Standardisation. A summary is also provided of the most influential or best-recognised international (IOS) standards on digital forensics.

It is concluded that the originality, reliability, integrity and admissibility of digital evidence should be maintained as follows:

- Data should not be changed or altered.
- Original evidence should not be directly examined.
- Forensically sound duplicates should be created.
- Digital forensic analyses should be performed by competent persons.
- Digital forensic analyses should adhere to relevant local legal requirements.
- Audit trails should exist consisting of all required documents and actions.
- The chain of custody should be protected.
- Processes and procedures should be proper, while recognised and accepted by the industry.

If the ACPO (1997) principles and ISO/IEC 27043 and 27037 Standards are followed as a forensic framework, then digital forensic investigators should follow these standards as a legal framework.

Keywords

Digital forensics; digital devices; digital search and seizure; digital evidence; forensic investigation; international standards.

.....

1 Introduction

The discipline of digital forensics requires a combination of skills, qualifications and knowledge in the area of forensic investigation, legal aspects and information technology.[1] In many academic papers and court cases information technology terminology is used interchangeably without any regard to its being unambiguous and conducive to consistent interpretation of terminology in a legal context, which is why information technology terminology is largely unknown in the legal system.[2] Many information technology terms or concepts have not yet achieved legal recognition. This notion is supported by the South African Law Reform Commission (hereafter SALRC),[3] which has expressed the opinion that the earlier opinion that computers are "just like" filing cabinets does not hold true in the light of new technological capabilities. This was also the opinion of the Supreme Court in the Canadian case *R v Vu*.[4]

Accurate legal definitions are vital to the operation of legal instruments, where words signify concepts in law, and the vocabulary consists of technical or legal terms and non-technical terms found in everyday language.[5] Many of the words used in legal discourse are derived from ordinary language, but the true development of legal terminology − to a great extent − is derived from legal discourse in courts and depends less on the parameters set for communication with regard to generally recognised legal science principles.[6] The recognition of terminology within a legal context is of the utmost importance to ensure that miscommunication does not occur. One should bear in mind that an initial understanding of texts may not be the only plausible interpretation.[7] This can especially be true in a digital environment where technical aspects can have an influence on the normal interpretation or understanding of terms. Although one acceptable

* Jacobus Gerhardus Johannes Nortjé. BCom Hons Business Administration MBA MCom Forensic Accounting (NWU) (FP)SA CFE. Associated Professor of Forensic Accounting and Forensic Investigation Management, North-West University, South Africa. Email: Koos.Nortje@nwu.ac.za.

** Daniel Christoffel Myburgh. BCom Hons Information Systems MCom Forensic Accounting (NWU). MCom Forensic Accounting Student North-West University, South Africa. Email: dc@cyanre.co.za.

1 Kessler *Judges' Awareness* 1.

2 Kessler *Judges' Awareness* 2.

3 SALRC *Issue Paper 27* 8.

4 *R v Vu* 2013 3 SCR 657 (SCC).

5 Jopek-Bosiacka 2011 *Research in Language* 9.

6 Jopek-Bosiacka 2011 *Research in Language* 10, 14.

7 Clark and Connolly 2006 https://www.law.georgetown.edu/academics/academic-programs/legal-writing-scholarship/writing-center/upload/statutoryinterpretation.pdf 2.

meaning is the ideal, the interpretation of legal texts causes frequent problems, as the meaning denoted in texts may not be the same for all addressees.[8] In 1958 Hart[9] encapsulated this issue perfectly by stating that in the most elementary form of law, the terms used should exist in some standard instance in which no doubt exists about their interpretation. Hart[10] is of the opinion that there should be a "core of settled meaning".

In an attempt to provide clarity or guidance on some of the terms and concepts applicable to digital forensics and for the search and seizure of digital evidence, some of the concepts and terms are reviewed and discussed below.

In the early 1900s Dr Edmond Locard developed one of the cornerstones of modern-day forensic science, the Locard's exchange principle.[11] While studying medicine Locard developed an interest in the application of science to legal matters.[12] Locard theorised that every time a person or an object comes into contact with another, this results in an exchange of physical materials. Locard believed that during this contact all sorts of evidence, including human deoxyribonucleic acid (DNA), fingerprints, footprints, hair, skin cells, blood, bodily fluids, pieces of clothing, fibres and more are exchanged.[13] As early as in 1997 Silvernail[14] stated that when persons start to use a computer, evidence of activities is created. It is therefore recognised that the Locard principle also applies to computers[15] due to the evidential traces or artefacts exchanged between the network of victims and the computers of perpetrators. This is confirmed by Wang,[16] who emphasises the fact that digital evidence can prove crucial links between victims and perpetrators.

If it is recognised that computers have become an attractive medium for criminals[17] and that their activities on computers result in evidence that can

8 Jopek-Bosiacka 2011 *Research in Language* 14.
9 Hart 1958 *Harv L Rev* 607.
10 Hart 1958 *Harv L Rev* 607.
11 Forensics Library 2014 http://aboutforensics.co.uk/edmond-locard/.
12 Forensic Handbook 2012 http://www.forensichandbook.com/locards-exchange-principle/.
13 Forensic Handbook 2012 http://www.forensichandbook.com/locards-exchange-principle/.
14 Silvernail 1997 *Ala Law* 176-177.
15 Chisum and Turvey 2000 http://www.profiling.org/journal/vol1_no1/jbp_ed_january 2000_1-1.html 11.
16 Wang 2007 *CSI* 217.
17 SALRC *Issue Paper 27* 7.

be linked to the crimes of suspects,[18] it is essential to recognise the need for a discipline in the field of digital forensics.

Digital evidence is often collected incorrectly and analysed ineffectively or simply overlooked due to the complexities that digital evidence poses to forensic investigators.[19] This "new" type of evidence has prompted the beginning of a "new" type of forensic science − digital forensics.[20] As with any forensic science, specific regulations, guidelines, principles or procedures should be followed to meet the objectives of investigations, namely the accuracy and acceptance of findings.[21] These regulations, guidelines, principles or procedures are discussed in the context of digital forensics: what processes should be followed and how these processes ensure the acceptability of digital evidence.

A summary is also provided of the most influential or best-recognised international standards on digital forensics.

2 Terminology

2.1 Sections 20 and 21 of the Criminal Procedure Act 51 of 1977

Section 21 of the *Criminal Procedure Act* 51 of 1977 relates to the power of authorised officials to issue search and seizure warrants.

The section furthermore authorises the police official to search and seize section 20 articles:

- which are concerned;
- which may afford evidence;
- which are intended to be used in the commission of a crime.

From this section, four concepts require further scrutiny on how these definitions relate to the digital environment, namely:

- *search*;

18 Casey *Handbook of Computer Crime* 1, 6.
19 Casey *Handbook of Computer Crime* 8; Craiger and Shenoi *Advances in Digital Forensics* 49.
20 Kerr 2005 *Miss LJ* 86.
21 Vacca *Computer Forensics* 6.

- *seize*;
- *articles*;
- *premises*.

The intrusive nature of search and seizure warrants and the obligation of the judicial system to guard against the misuse of this authority are well-documented in the case of *Powell v Van der Merwe*.[22] During this case, it was said that South African law has a long history of scrutinising search and seizure warrants with rigour and exactitude and that the common law rights are now enshrined in section 14 of the *Constitution of the Republic of South Africa*, 1996. Because of the danger of misuse during the application of authority with regard to search and seizure warrants, the judiciary scrutinises the validity of warrants with jealous regard for the liberty of suspects and their rights. The scope of the terms is even more relevant in cases involving digital evidence due to the wide scope of personal and confidential information kept on the digital devices of persons.[23]

The Explanatory Report to the Convention on Cybercrime of the Council of Europe suggests that additional procedural provisions are necessary in order to ensure that data can be secured in a manner as effective as in the case of the search and seizure of tangible objects.[24] This is firstly because the data are intangible – they are in an electromagnetic medium. Secondly, while data can be read by making use of computer equipment, data cannot be taken away in the same sense as paper records.[25] Kerr[26] captures some of the complexities of digital evidence as follows: "How can the old rules fit the new facts? For example, what does it mean to 'search' computer data, or when is computer data 'seized'?" The Explanatory Report to the Convention on Cybercrime further suggests that data can be "seized" in only a specific number of ways, namely data can be printed and seized; the tangible medium upon which data is stored can be seized; or a forensic duplicate can be made of the data and the tangible form upon which the copy is saved can be seized. It is suggested that domestic law should provide for the power to create such duplicates.[27]

22 *Powell v Van der Merwe* 2005 1 All SA 149 (SCA).
23 Guzzi 2012 *Am Crim L Rev* 302.
24 Council of Europe 2001 http://www.oas.org/juridico/english/cyb_pry_coe.pdf 32.
25 Council of Europe 2001 http://www.oas.org/juridico/english/cyb_pry_coe.pdf 32.
26 Kerr 2005 *Harv L Rev* 533.
27 Council of Europe 2001 http://www.oas.org/juridico/english/cyb_pry_coe.pdf 32.

2.1.1 Defining the search for digital evidence

Kerr[28] suggests that forensic investigators should first search for and locate physical devices ("search one"). Then, forensic investigators should access and search these physical devices for relevant information or data ("search two"). For the purpose of this article, references to "search" are extended from Kerr's two-step process to include three phases, namely:

- The traditional process in which forensic investigators search for or locate physical computers on a scene.
- The forensic investigators search for or segregate relevant and non-relevant information/data on these computers.
- The analysis or interpretation of relevant information within the context of a larger investigation.

This discussion of the definition of "search" relates to the later steps followed when data is searched, since it is acknowledged that the search for physical articles on premises is well-defined and understood in the law.

The phenomenon of seizing's taking place before a search has taken place is discussed by Brenner and Fredericksen,[29] who state that a search and seizure of digital evidence turns a normal search and seizure on its head in the sense that computers are normally first seized and then searched. In the case of the *Minister of Safety and Security v Bennett*,[30] it was recognised that in instances where large collections of physical documents are located on a scene, and when it is impractical to separate or effectively search these documents on the scene, a broad seizure of the collection of physical documents is permitted, pending a later search to segregate relevant and non-relevant information.

The Explanatory Report to the Convention on Cybercrime proposes that traditional words such as "search" and "seize" should be replaced with more technological-orientated computer terms, such as "access" and "copy".[31] This proposal is supported by Nieman,[32] who is of the opinion that "search and seize" can more accurately described when computer terminology is used that is more neutral in meaning and can include actions, such as the

28 Kerr 2005 *Miss LJ* 85.
29 Brenner and Fredericksen 2002 *Mich Telecomm & Tech L Rev* 82.
30 *Minister of Safety and Security v Bennett 2008* 2 All SA 26 (SCA).
31 Council of Europe 2001 http://www.oas.org/juridico/english/cyb_pry_coe.pdf 33.
32 Nieman 2009 *JILT* 15.

creation of forensic duplicates of data. Currently, in the consultation draft of the proposed South African *Cybercrimes and Cybersecurity Bill* dated 19 June 2016 the term "access" is included and is defined as follows: "to make use of, to gain entry to, to view, display, instruct, or communicate with, to store data in or retrieve data from, to copy, move, add, change, or remove data or otherwise to make use of, configure or reconfigure any resources of a computer device".[33]

In the *Minister of Safety and Security v Xaba* case[34] it was stated that the concept of "search" should be given its ordinary meaning. The National Instruction 2/2002 of the South African Police Service (SAPS)[35] states that "search" entails any action whereby a person, premise or container is visually or physically examined with the aim of establishing whether an item or article is in, on or upon such a person, premises or container. However, Basdeo[36] is of the opinion that this approach is questionable since "visually" is not defined and can include merely looking at something. Furthermore, the question of what constitutes a search is left to common sense − accessed on a case-by-case basis. Basdeo continues and argues that an element of physical intrusion is required to constitute a search of persons, premises or properties.

Merely observing a room does not constitute a fully-fledged search.[37] Kerr[38] proposes that an "exposure-based approach" should be adopted and that data should be considered to have been "searched" only when the data were exposed to human observation.

Basdeo[39] states that the *Council of Europe Convention on Cybercrime* (2001) in Budapest (hereafter *Budapest Convention*) constitutes the current international agreed-upon benchmark for procedural powers in terms of digital evidence collection. The *Budapest Convention* proposes that "search" should include "to seek, read, inspect or review data", which includes the searching or examining of data.[40]

The interpretation of "search" as an "exposure-based approach" is supported and based on any action in which forensic investigators access

33 *Draft Cybercrimes and Cybersecurity Bill*, 2016 6.
34 *Minister of Safety and Security v Xaba* 2003 1 All SA 596 (D).
35 SAPS *National Instruction 2/2002* 1.
36 Basdeo *Constitutional Perspective of Police Powers* 21.
37 Kerr 2005 *Harv L Rev* 536, 540.
38 Kerr 2005 *Harv L Rev* 547.
39 Basdeo 2012 *SACJ* 199.
40 Council of Europe 2001 http://www.oas.org/juridico/english/cyb_pry_coe.pdf 33.

data by whatever means and take notice of information or observe information in a humanly readable format. It is recognised that the term "search" is extraordinarily broad, and a differentiation is made between the different contexts of search, as an action to firstly locate or look for devices on a scene; secondly, to locate and separate relevant and non-relevant data; and lastly, to analyse or interpret the data within the context of a larger investigation.

2.1.2 Defining the seizure of digital evidence

In the *Rudolph v Commissioner for Inland Revenue* case[41] the court held that the term "seize" should be given its natural meaning. This ruling was supported in the case of *Ntoyakhe v Minister of Safety and Security,*[42] when the court held that "seize" means not only to take possession of articles but also to retain them and, according to Steytler,[43] to deprive persons of subsequent control over the articles. Nieman[44] adds that a seizure takes place when persons are deprived of their control over articles, and without the subsequent right of retention of the articles section 21 of the *Criminal Procedure Act* would be worthless. In the *Ntoyakhe v Minister of Safety and Security* case, it was cautioned that the right of retention is not unlimited and does not authorise the State to deprive persons of their lawful possession of articles indefinitely.[45] This is a very important issue raised by the court. Although sections 31 to 36 of the *Criminal Procedure Act* govern the disposal of articles under various conditions, no explicit reference is made to the duration in days for which articles may be retained after the point of seizure, or when forensic duplicates are made when the original articles are to be returned following the creation of the duplicates. The situation with computers differs from that of other classes of articles because computers and other digital devices such as cellular phones play such a large role in our everyday lives. The retention period under discussion does not refer to the retention of forensic duplicates of computers during an analysis phase, but to the period between the seizure of computers on a scene, the creation of off-site forensic duplicates, and the subsequent return of the original computers to the owners. In many countries, legislation stipulates a time period in a number of days for this retention period. In an unstructured interview,[46] it was established that the practice in South Africa − due to there

41 *Rudolph v Commissioner for Inland Revenue* 1996 7 BCLR 11 (CC).
42 *Ntoyakhe v Minister of Safety and Security* 2000 1 SA 257 (E).
43 Steytler *Constitutional Criminal Procedure* 84.
44 Nieman 2009 *JILT* 16.
45 *Ntoyakhe v Minister of Safety and Security* 2000 1 SA 257 (E).
46 Anon *Current Policy and Procedure*.

being limited resources − is that police officials in the most cases seize computers on scenes and then transfer articles to central digital forensic laboratories. During this interview, it was stated that some of the digital forensic laboratories are months − even more than a year − behind in their workload.[47] The interviewee[48] estimated that on average persons are deprived of their computers (or cellular phones) for between five days to two years.

In the light of the unique way in which digital evidence is normally collected or "seized", Kerr[49] poses a number of questions with regard to the interpretation of when digital evidence is considered seized, namely:

- Does the creation of forensic duplicates constitute a seizure?
- Does the creation of forensic duplicates constitute a seizure of original evidence?
- If forensic duplicates are searched, does this constitute a seizure?

Kerr[50] states that these aspects are surprisingly difficult to interpret and at first sight it seems sensible to say that the creation of forensic duplicates constitutes a seizure of evidence. In the United States case of *Arizona v Hicks*[51] an investigator copied the serial number on a stereo system to establish later whether or not it was stolen goods. The court held that the copying of this information did not constitute a seizure. The court also held that the recording, copying or taking of a photograph of information on a scene does not constitute a seizure. This finding highlights the question whether forensic duplicates of computers constitute a seizure. Kerr[52] further reviewed these complexities by arguing that if the creation of forensic duplicates is not recognised as constituting a search and seizure − since the data were not exposed, read or observed by humans, but only forensically duplicated – this could drastically expand the powers of the forensic investigators. In addition, Kerr maintains that should the making of forensic duplicates not be viewed as a search and seizure, the forensic investigators would not need search and seizure warrants, and Kerr refers to such a situation as "troublesome" and downright "creepy".

47 Anon *Current Policy and Procedure.*
48 Anon *Current Policy and Procedure*.
49 Kerr 2005 *Harv L Rev* 541.
50 Kerr 2005 *Harv L Rev* 557.
51 *Arizona v Hicks* 480 US 321, 325 (1987).
52 Kerr 2005 *Harv L Rev* 560.

The Explanatory Report to the Convention on Cybercrime[53] proposes that "seize" should also include "to take away the physical medium which stores the data" or to make and retain forensic duplicates of data. This proposal is supported by Basdeo,[54] who is of the opinion that the seizure of data includes not only the confiscation of data but also the "gathering" of data.

The concept of seizure is important, and it is therefore necessary to consider the way in which and the reason why forensic duplicates are created. Nieman[55] explains that forensic duplicates do exactly what the name suggests − bit-by-bit exact duplicates of every sector of a hard drive are created. The requirement of section 14 of the *Electronic Communications and Transactions Act* 25 of 2002 relating to the originality of evidence stipulates that where the law requires information to be presented or retained in its original form, that requirement is met if the integrity of the digital evidence from the time it was first generated to its final form has passed assessment. Vacca[56] states that a new concept of representational accuracy has emerged in terms of digital evidence − it is not necessary anymore to present the original. If forensic duplicates are created that depict the source data exactly, these duplicates can be considered originals. However, after forensic duplicates of computers are created and the originals are handed back to suspects, as soon as a person switches on the computer the content of that computer changes on a continual basis.[57]

The proposed *Cybercrimes and Cybersecurity Bill* provides a more inclusive definition for "seize" by including the rendering of data inaccessible, the removal of physical devices, to make or retain forensic duplicates, or to make a printout of data.[58] For the purposes of this article, the interpretation of "seizure" includes the creation of forensically-sound duplicate originals, and the seizure or retention of these duplicates is viewed by the State as originals.

Defining premises and containers

Section 1 of the *Criminal Procedure Act* defines "premises" as "including land, any building or structure, or any vehicle, conveyance, ship, boat or aircraft". It is questioned whether this definition permits the inclusion of a computer as a premises and does this definition permit the search of

53 Council of Europe 2001 http://www.oas.org/juridico/english/cyb_pry_coe.pdf 33.
54 Basdeo 2012 *SACJ* 199.
55 Nieman 2009 *JILT* 22.
56 Vacca *Computer Forensics* 237.
57 Vacca *Computer Forensics* 19.
58 *Draft Cybercrimes and Cybersecurity Bill*, 2016 9.

computers prior to seizure? In their Discussion Paper on Computer-related Crime[59] the SALRC is of view that the provisions of the *Criminal Procedure Act* were developed prior to the notion that non-physical premises or non-tangible articles exist, and the commission is of the opinion that chapter two of the *Criminal Procedure Act* most probably does not apply to the search of computers and the seizure of data located on computers. They recommend that the *Criminal Procedure Act* be amended to specifically include the search of computers and the seizure of data. Section 82(4) of the *Electronic Communications and Transactions Act* stipulates, "For the purposes of this Act, any reference in the Criminal Procedure Act, 1977, to 'premises' and 'article' includes an information system as well as a data message". Unfortunately, the new *Cybercrimes and Cybersecurity Bill* is silent in this regard and does not provide a wider, more inclusive definition, but recognises the searching of containers.[60] This definition is also supported by the National Instruction 2/2002 of the SAPS, where it states that a search entails any action whereby persons, premises or containers are visually or physically examined with the aim of establishing whether items or articles are in, on or upon such persons, premises or containers.[61]

In 2012, the Seventh Circuit Court in the case of the *United States v Flores-Lopez*[62] defined containers as any objects containing anything else − including data. The court held that smartphones or tablets comply with this definition and can therefore be searched.

The court held in the *Thint (Pty) Ltd v National Director of Public Prosecutions, Zuma v National Director of Public Prosecutions* case[63] that it is a requirement in a South African environment that "premises" should be clearly defined. The question is then raised that if off-site searches of computers are permitted, what premises should be specified in warrants? Traditionally, premises are where suspects are located, but the presence of computers turns the search and seizure process around: the seizure of computers takes place on a scene but the search of data takes place at the premises of forensic investigators. Should the premises of suspects be listed, or the premises of forensic investigators or should computers be listed as premises? The answer was provided by the court during the

59 SALRC *Discussion Paper 9* 14.
60 *Draft Cybercrimes and Cybersecurity Bill*, 2016 27.
61 SAPS *National Instruction 2/2002* 1.
62 *United States v Flores-Lopez* No 10-3803 (7th Cir 2012).
63 *Thint (Pty) Ltd v National Director of Public Prosecutions, Zuma v National Director of Public Prosecutions* 2009 1 SA 1 (CC).

Minister of Safety and Security v Bennett case,[64] where the seizing of physical documents − prior to the search of these documents off-site − was permitted without a description of the secondary premises of the forensic investigators. In the unreported judgement of *Bennett v Minister of Safety and Security*,[65] the court also expressed the opinion that it is irrelevant where forensic duplicates are created after the seizure and removal from the scene.

Another issue is raised in this regard − if forensic investigators are planning to seize data on another network or at an online location, do the search and seizure warrants need to state the physical location from which the forensic investigators are accessing the data or the physical location of where the data are kept?[66] At the time when Kerr studied these aspects in 2005, cloud hosting was not as prevalent as it is today. If forensic investigators need to seize the files of persons kept in a virtual environment − hosted in a cloud − what premises need to be described? Search and seizure is further complicated by the structure of cloud hosting, where one document can be broken up into a number of segments and each segment can be stored on a different server in a different country. The implications of this issue on search and seizure are recognised by the *Australian Crimes Act*[67] and the New Zealand *Search and Surveillance Act,*[68] both of which permit law enforcement to search remote locations, such as online data storage facilities with no physical addresses or specific singular location, such as cloud services, or where the physical locations are unknown.

For the purpose of this article, the interpretation of "premises" is limited to the traditional description of premises or locations and not extended to describing devices as separate premises or the premises of digital forensic investigators.

Defining articles or items

Bouwer[69] observes that the *Criminal Procedure Act* is lacking in that it does not specifically include data as articles, and stated that the legislature has recognised this omission by referencing the definition of articles and premises in the *Electronic Communications and Transactions Act*, which

64 *Minister of Safety and Security v Bennett* 2008 2 All SA 26 (SCA).
65 *Bennett v Minister of Safety and Security* (TPD) (unreported) case number 10828/2005 of 13 May 2005 11.
66 Kerr 2005 *Miss LJ* 104.
67 Section 3LB of the *Australian Crimes Act* 12 of 1914.
68 Section 111 of the *Search and Surveillance Act* 24 of 2012.
69 Bouwer 2014 *SACJ* 171.

states that data messages are classified as articles if these messages relate to a section 20 article as defined by the *Criminal Procedure Act*. Basdeo[70] states that “data” refers to information that has been transformed into digital form and in terms of the provisions made in section 20 of the *Criminal Procedure Act*, which stipulates that anything can be seized and that anything should be susceptible to a wide enough interpretation to include data. Notwithstanding, Basdeo further advises that the provisions made in the *Criminal Procedure Act* should be restructured to alleviate the restrictive interpretation that “articles” are only physical items. Basdeo further expresses the opinion that law enforcement is currently interpreting “articles” very widely, and applies this definition to the seizure of digital evidence − a practice that has not yet been contested in court. This aspect is addressed in the *Cybercrimes and Cybersecurity Bill,* which defines an "article" as any data, computer devices, computer networks, databases, critical databases, electronic communication networks or national critical information infrastructures or any part thereof or any other information, instruments, devices or equipment.[71]

For the purpose of this paper, the interpretation of "articles" or "items" as per the proposed *Cybercrimes and Cybersecurity Bill* is supported to include data, data storage devices and data processing devices.

2.3 Defining data and data messages

Article 1(b) of the *Budapest Convention* defines computer data as any representation of facts, information or concepts in a form suitable for being processed on computers. The SALRC states that the definition provided by the *Electronic Communications and Transactions Act* of "data" and "data messages" is based on Article 2 of the United Nations Commission on International Trade Law's (UNCITRAL) *Model Law on Electronic Commerce with Guide to Enactment,*[72] which uses "data" and "data message" instead of the terms "electronic evidence" or "digital evidence".[73] This approach is also recommended by the Practical Guide of the SAPS,[74] which uses the term "data" instead of "digital evidence". The accurate use of terminology in search and seizure warrants in line with enabling legislation is supported in the case of *Heaney v S,*[75] where the ruling was that the description of a

70 Basdeo 2012 *SACJ* 198, 205.
71 *Draft Cybercrimes and Cybersecurity Bill*, 2016 6.
72 UN *UNCITRAL Model Law*.
73 SALRC *Issue Paper 27* 32.
74 SAPS *Practical Guide to Apply for Search Warrants* 7.
75 *Heaney v S* 2016 ZAGPPHC 257 (19 April 2016).

suspected crime should be accurately described in line with the enabling legislation, and colloquially used terms should not be applied. The *Electronic Communications and Transactions Act* describes "data" as the electronic representation of information in any form, and "data messages" as data generated, sent, received or stored by electronic means. The SALRC further explains that in Part 2 of the UNCITRAL *Model Law on Electronic Commerce* (1996) it is stated that the concept of data messages is not intended to be limited to communication, but should include computer records and all types of messages that are generated, stored or communicated in a paperless form.[76]

For the purpose of this article, the definition of "data" is adapted from section 1 of the *Electronic Communications and Transactions Act* as is “the digital representation of information in any form”, and not the "electronic representation of data in any form".

2.4 Digital, computer, electronic or cyber evidence

The SALRC observes that Article 2 of the UNCITRAL *Model Law on Electronic Commerce* refers to "data" and "data messages" rather than to "electronic evidence" or "digital evidence".[77] The reason for this is obvious, since the *Model Law on Electronic Commerce*, which forms the basis of the South African *Electronic Communications and Transactions Act*, is aimed at regulating e-commerce, and only a small portion of it relates to defining criminal activities. The *Model Law on Electronic Commerce* stipulates that the law applies to all commercial activities.[78] It is therefore logical rather to use descriptions such as "data" or "data messages". Data or data messages become relevant during investigations into criminal activities, when "electronic evidence" or "digital evidence" should be used. Bouwer[79] recommends that a single definition for "electronic evidence" should be adopted in the South African law as "information of probative value stored or transmitted in digital format".

References to "computer" evidence or "computer" crime seem to be out-dated.[80] The *Model Law on Electronic Commerce* and the *Electronic Communications and Transactions Act* make reference to data, data messages and information systems instead of "computer". The word

76 SALRC *Issue Paper 27* 32.
77 SALRC *Issue Paper 27* 32.
78 UN *UNCITRAL Model Law* 3.
79 Bouwer 2014 *SACJ* 170.
80 Bouwer 2014 *SACJ* 161.

"computer" is well understood and is derived from what devices do, namely computing.[81] Computers are defined as "electronic devices which are capable of receiving information (data) in a particular form and of performing a sequence of operations in accordance with a predetermined but variable set of procedural instructions (a programme) to produce a result in the form of information or signals".[82] This definition differs vastly from any description of cellular phones with computing capabilities, which are described by the *Oxford Dictionary* as primarily telephones connected via cellular networks over a wide area.[83]

The term "cyber" is also of importance. In 1984 William Gibson originally coined the term "cyberspace" in his science fiction novel *Neuromancer*.[84] The *Oxford Dictionary* defines "cyber" as "relating to or characteristic of the culture of computers, information technology, and virtual reality."[85]

It is very difficult to differentiate between "electronic" and "digital". The SALRC shed light on this dilemma.[86] The commission states that while these two terms are used interchangeably, an important distinction exists between the two − analogue and digital outputs. Examples of analogue outputs are vinyl records, photographic films and old telephone systems making use of switchboards.[87] Neither the *Electronic Communications and Transactions Act* nor the *Model Law on Electronic Commerce* provides any description or definition of "electronic". Spencer[88] states that the term "electronic" is not particularly technical and has become synonymous with consumer electronics, such as clocks, radios, smartphones and tablets. It is therefore obvious that although "electronic devices" should include "data", the term is not exclusively limited to "data". However, "digital" is based on binary coding and functions as the building blocks of data.[89] The Scientific Working Group on Digital Evidence (hereafter SWGDE) supports this by

81 Woodford 2007 http://www.explainthatstuff.com/howcomputerswork.html.
82 Oxford English Dictionary 2016 http://www.oxforddictionaries.com/definition/english/computer.
83 Oxford English Dictionary 2016 https://en.oxforddictionaries.com/definition/cellular_phone.
84 Gibson *Neuromancer*.
85 Oxford English Dictionary 2016 https://en.oxforddictionaries.com/definition/cyber.
86 SALRC *Issue Paper 27* 31.
87 Christensson 2005 http://pc.net/helpcenter/answers/difference_between_analog_and_digital.
88 Spencer 2014 https://www.quora.com/Whats-the-difference-between-electronic-and-digital.
89 Lowe Date Unknown http://www.dummies.com/how-to/content/digital-electronics-binary-basics.html.

defining "digital evidence" as evidence stored or transmitted in a binary form.[90]

For the purpose of this article, the term "digital" is used as opposed to the terms "electronic", "cyber" or "computer".

2.5 Forensic duplicating processes in relation to originality

Digital forensic investigations often involve creating and examining forensic duplicates of the data under analysis.[91] Forensic investigators use forensic duplication techniques to collect or acquire data from hard drives, as opposed to the normal copying of files. This is because forensic duplicates contain all of the data from the source drive − even deleted files.[92] A normal copying process retrieves only the active or currently accessible files, not deleted files as well.[93] A number of references were found to the concept of creating forensic duplicates of digital evidence, including copies, clones, bit-stream copies, images, forensic copies, bit-by-bit copies, mirror images and acquisitions. Vandeven[94] provides the following definitions for some of these concepts:

- *Bit-by-bit* or *bit-stream copies* − exact copies of all the bits of a logical volume or a physical drive. If the copies are made to files, it is referred to as forensic image files. If copies are made to another disk, it is referred to as clones or mirror images. The original and clones are identical and interchangeable, but if clones are not write-protected, subsequent actions of an analysis can alter the data.

- *Disk image files* − files containing exact copies of logical volumes or physical disks.

- *Forensic images* − exact copies of all the bits of logical volumes or physical drives that have been copied bit-by-bit and include all data and metadata. Forensic images include information, such as when these images were copied, by whom, with which forensic tools and the cryptographic hash used for verification of these images.

---

90 SWGDE 2012 https://www.swgit.org/pdf/SWGDE%20and%20SWGIT%20Digital%20and%20Multimedia%20Evidence%20Glossary?docID=60 6.

91 ACPO 1997 http://www.digital-detective.net/digital-forensics-documents/ACPO_Good_Practice_Guide_for_Digital_Evidence_v5.pdf 4.

92 Nieman *Search and Seizure* 44.

93 Kerr 2005 *Harv L Rev* 540.

94 Vandeven 2014 https://www.sans.org/reading-room/whitepapers/forensics/forensic-images-viewing-pleasure-35447 32-35.

- *Raw images* − exact bit-by-bit copies of disks into a single file. Raw images do not contain information regarding the creation of these images.

According to Gerber,[95] forensic duplicates were previously also referred to as "mirror" images, but because the term confused courts, the use of "mirror" images is not recommended. Normally, mirror images are reverse images of originals.

All of these different terms can be confusing, but nowhere was it found in research that any of the terms used − except for "mirror copies" – has been rejected by courts.

In the light of the above, a single expression could prove to be technically incorrect in all situations. Whatever terminology is used, Lidbury and Boland[96] state that what makes "collections" forensically sound should be the main aim − whether data were collected is an exact duplicate of the original source, including metadata. This implies that the collection method and subsequent analysis steps should not alter data and should include mechanisms to ensure the integrity of the data, such as the extraction of hash values. The judicial measures within a South African environment are the requirements specified by section 14 of the *Electronic Communications and Transactions Act* − the originality of data messages is measured against the integrity of digital evidence from the time the data were first generated. Integrity is assessed by considering whether the evidence has remained complete and unaltered except for the adding of endorsements or changes which are caused in the normal course of communication. Vacca[97] states that an important feature of digital forensics is the fact that it changes the legal concept of best evidence. Vacca states that a new concept of representational accuracy has emerged in terms of digital evidence. It is not necessary anymore to present original copies. If forensic duplicates are created and the source data are depicted exactly, duplicates are considered original.[98]

In the Canadian case of *R v Munshi*,[99] it was stated that with the modernisation of technology, forensic duplication processes have developed to such an extent that duplicate originals can exist. Although this

95 Cited in Kessler *Judges' Awareness* 37.
96 Lidbury and Boland 2012 http://www.insidecounsel.com/2012/05/11/technology-forensically-sound-collection-of-esi 1.
97 Vacca *Computer Forensics* 795.
98 Vacca *Computer Forensics* 237.
99 *R v Munshi* 2002 CanLII 39110 (ON SC).

ruling related to documents, the court stated that where exact replication processes are used, it is generally not necessary to compare original documents with the duplicate originals.

Van Deusen Phillips[100] maintains that the test of establishing whether or not digital documents can stand as evidence is to determine or prove that the content of the documents is indeed the original, unchanged content. Van Deusen Phillips further states that this is normally accomplished by presenting the original documents or the duplicate originals. In the American case of *Lorraine v Markel American Ins Co*,[101] the court held that an original is the writing itself or a counterpart intended to have the same effect, and that if data are stored on computers or on similar devices, any printouts or other outputs readable by sight reflect the data accurately, the data can be accepted as original. In the case of *Muller v BOE Bank Ltd*,[102] it was acknowledged that South African courts have accepted and are accustomed to the creation or existence of "copies" recognised as duplicate originals since the inception of carbon copies.

For the purpose of this article, the most elucidating description, which should make room for interpretation, is the creation of "forensically-sound duplicate original records" (hereafter forensic duplicates).

3 Digital forensics and international standards

3.1 Digital forensics

Many definitions of digital forensics exist. Palmer[103] captures the main aspects as the use of scientifically-derived and proven methods in locating, collecting, preserving, analysing, interpreting, documenting and presenting digital evidence relating to incidents, often with the aim of presenting evidence during hearings. The goal of the process is to preserve evidence in its most original form while performing a structured analysis by collecting, identifying and validating digital information for the purpose of reconstructing past events.

---

100 Van Deusen Phillips 2010 https://crlgrn.wordpress.com/2010/07/27/legal-considerations-for-electronic-evidence-part-5-original-vs-duplicate-documents-unfair-prejudice/.

101 *Lorraine v Markel American Ins Co* (2007) 241 FRD 534, 544 (D Md 2007).

102 *Muller v BOE Bank Ltd* 2011 1 SA 252 (WCC).

103 Palmer 2001 https://isis.poly.edu/kulesh/forensics/docs/DFRWS_RM_Final.pdf 16.

As a scientific-based discipline, digital forensics is premised on following set standards or methodologies in the processes defined above, which are susceptible to inspection by judiciaries.[104]

3.2 International standards

Nieman[105] states that it is ironic that digital forensics first and foremost concerns forensic procedure, rules of evidence, legal concepts, precedents and processes and, second to this, computers. It is exactly because of this that standards in this field play such an important role.

Most of the "standards" are presented as guidelines as opposed to set standards.[106]

In the light of the importance of standards or the important role that standards should play in digital forensics as a science, it is surprising that there are no set standards, rules or a protocol for the handling of digital evidence, and that technical processes applied to digital evidence "do not have to pass any formal test" for digital evidence to be placed before courts.[107] It is therefore understandable that the digital forensic industry has largely been self-regulated within a framework of internationally advised practices, case law, guidelines and industry groups.

3.2.1 Principles of the Association of Chief of Police Officers

The Good Practice Guide for Computer-Based Electronic Evidence[108] of the ACPO was drafted in 1997. According to Mohay *et al.*,[109] these principles were reviewed during an International Hi-Tech Crime and Forensic Conference in October 1999 and were further formalised and accepted in 2001 at the 13th International Criminal Organisation's (Interpol) Forensic Science Symposium.

Digital evidence should be accurate, authentic and admissible, like any other evidence, and should conform to common law and legislative principles.[110] If investigators, for example, open files and make copies, move, save or print these files, these actions are not viewed as neutral, and

104 Casey *Digital Evidence* 10.
105 Nieman 2009 *JILT* 22.
106 IOS 2014 https://www.iso.org/standard/44407.html vi.
107 Scholtz *Towards an Automated Digital Data Forensic Model* 60.
108 ACPO 1997 http://www.digital-detective.net/digital-forensics-documents/ACPO_Good_Practice_Guide_for_Digital_Evidence_v5.pdf.
109 Mohay *et al Computer and Intrusion Forensics* 123.
110 Nieman 2009 *JILT* 19.

may influence or modify evidence.[111] The Explanatory Report to the Cybercrime Convention indicates that digital evidence should be retained in the state it was found from the start to the point of prosecution.[112] Kessler[113] highlights the fact that each stage should be performed in such a way that the integrity of the evidence is preserved.

The ACPO principles have long been a guideline for digital forensic investigators in formulating digital forensic procedures to ensure that the requirements as listed above are met when evidence is collected, handled and managed. The guide contains the following four principles concerning the collection and management of digital evidence:[114]

- *Principle 1*: No actions taken by investigators should change the data that may subsequently be relied upon in court.
- *Principle 2*: Only in exceptional situations should investigators work with or access the original data and only if they are competent to do so and in a position to provide evidence explaining the relevance and the implications of their actions.
- *Principle 3*: All processes applied to the digital evidence by investigators should be fully recorded to enable independent third party experts to follow these processes and reach the same results.
- *Principle 4*: Investigators should ensure that all legal principles are adhered to during the analysis of digital evidence.

The principles provide guidelines so that the actions of investigators do not change the digital evidence under investigation, and if original evidence is accessed, this should be done by competent persons. A complete audit trail should be maintained so that the actions of investigators can be reviewed, assessed and evaluated against local legal requirements. These international principles were drafted with the aim of ensuring that the handling of digital evidence conforms to the requirements of evidence in terms of the law and especially to ensure that the integrity of evidence is maintained by ensuring that data have remained unaltered.[115] The

111 Vacca *Computer Forensics* 19.
112 Council of Europe 2001 http://www.oas.org/juridico/english/cyb_pry_coe.pdf 38.
113 Kessler *Judges' Awareness* 6.
114 ACPO 1997 http://www.digital-detective.net/digital-forensics-documents/ACPO_Good_Practice_Guide_for_Digital_Evidence_v5.pdf 4.
115 ACPO 1997 http://www.digital-detective.net/digital-forensics-documents/ACPO_Good_Practice_Guide_for_Digital_Evidence_v5.pdf 6-7.

SALRC[116] affirmed the importance of these principles when the commission stated that by accessing files, the actions of forensic investigators are not neutral and it is not easy to prove the integrity of digital evidence given the volatile nature of digital evidence. It has also been stated that the incorrect following of crime scene protocols and proper procedures can render digital evidence unusable or vulnerable to claims of prejudicial distortion by the defence.

3.2.2 Standards and guidelines of the International Organisation of Standardisation

3.2.2.1 ISO 27037 − Security Techniques − Guidelines for identification, collection, acquisition and preservation of digital evidence

In October 2012 the ISO 27037 Standard on Information Technology − Security Techniques − guidelines for the identification, collection, acquisition and preservation of digital evidence was approved and published. The ISO standards are very well known, but even the ISO standards seem to shy away from setting rigid standards in a digital forensic environment. In the opening line of the scope of the ISO/IEC DIS 27037 Standard,[117] it is stated that it merely provides "guidelines for specific activities in handling potential digital evidence; these processes are: identification, collection, acquisition and preservation of potential digital evidence".

The processes specified in the standard set guidelines to ensure that digital forensic investigators maintain the integrity of digital evidence during the collection phases of investigations by following analysis methodologies aimed at advancing the admissibility of evidence during legal processes. The importance of the integrity of evidence is supported by Kanellis,[118] who emphasises that evidence should be managed correctly so that it cannot lose value and as a result, be inadmissible in courts. The ISO/IEC DIS 27037 Standard sets out four fundamental principles for procedures to be followed in collecting digital evidence.[119] Digital forensic investigators should:

- Minimise the handling of original evidence.

116 SALRC *Issue Paper 27* 7.
117 IOS 2012 https://www.iso.org/standard/44381.html 1.
118 Kanellis *Digital Crime* 58.
119 IOS 2012 https://www.iso.org/standard/44381.html 8.

- Document all actions taken and account for any alterations in the data to allow experts to express an opinion regarding the reliability of the data.

- Adhere to local rules of evidence.

- Not take any actions beyond their competence.

The ISO/IEC DIS 27037 Standard specifies that, in most jurisdictions, digital evidence is governed by three primary principles:[120]

- Relevance

  A standard requirement is that only relevant data should be collected. In other words, the data collected should assist in examining incidents or aspects of incidents at hand and there should be a need and a reason to collect the data. This requirement is supported by sections 28, 31 and 210 of the *Criminal Procedure Act*, which regulate wrongful searches and seizures, the inadmissibility of irrelevant evidence and the return of articles not required for criminal proceedings. Digital forensic investigators should be in a position to explain the procedures followed and validate the reasons and grounds why specific data were collected. Francoeur[121] explains that any evidence should have an adequate level of relevance to the matter investigated.

- Reliability

  All processes followed in handling digital evidence should be auditable and repeatable. The result of applying these processes should be reproducible by independent parties when they follow the same process. Hofman[122] highlights that digital evidence should satisfy ordinary requirements related to the admissibility of documents. Documents should be authentic, reliable and original.

- Sufficiency

  Digital forensic investigators should ensure that all relevant information is collected to ensure that the matter at hand can be sufficiently analysed and considered. Digital forensic investigators

120 IOS 2012 https://www.iso.org/standard/44381.html 6.
121 Francoeur J 2003 http://www.scribd.com/doc/276157/The-Principles-of-Electronic-Agreement-Legal-Admissibility-WP-8-07.
122 Hofman 2006 http://hofman@law.uct.ac.za 7.

should be able to provide an indication of how much data was considered and should be able to justify the decision about what data and how much data to acquire.

The ISO/IEC DIS 27037 Standard specifies that all processes in relation to digital forensic investigations should be:[123]

- Auditable

  All processes, procedures and results should be auditable by independent forensic investigators to evaluate the activities performed by digital forensic investigators. Audits can be facilitated if the processes and actions followed by digital forensic investigators are sufficiently documented. Digital forensic investigators should be able to explain the basis upon which decisions were taken and the choice of methodology followed during analyses.

- Repeatability

  Repeatability is established when the same results are obtained in the following situations:

  - when the same procedures and methods are used;
  - when the same equipment under the same conditions is used.

  It should be noted that repeatability is not possible in all situations - for example, where live data was analysed, or volatile memory. In this case, digital forensic investigators should ensure that acquisition processes are reliable.

- Reproducibility

  Reproducibility is established when the same test results are produced under the following conditions:

  - when the same method is used;
  - when different equipment is used under different conditions;
  - when the same results can be reproduced at any time after the original test.

123 IOS 2012 https://www.iso.org/standard/44381.html 7.

- Justifiability

  Digital forensic investigators should be able to validate all actions and methods used in identifying, collecting, analysing and managing potential digital evidence. Justification can be achieved by demonstrating that their decisions were best practice in a specific case in obtaining all of the potential digital evidence in existing circumstances.

In terms of handling digital evidence, the ISO/IEC DIS 27037 Standard advises that "devices that may contain potential digital evidence [should be] removed from their original location to a laboratory or another controlled environment for later acquisition and analysis" and that forensic duplicates should be made for analyses to take place.[124]

The standard sets out a number of phases during digital forensic investigations,[125] which directly relate to searches and seizures, namely:

- *Identification* – which includes the search for data storage devices, the recognition thereof and the documentation of processes followed. It also entails the prioritisation of the sequence of methods used to secure digital evidence, which can be volatile.

- *Collection* – which relates to the collection and removal of evidence or the acquisition of evidence on a scene.

- *Acquisition* – which entails the creation of forensically sound duplicates of evidence in the least restrictive manner possible.

- *Preserving evidence* − from the point of collection throughout all of the digital forensic processes followed.

These phases are described during the process of digital seizures and divided into two distinctly different stages, namely the search of physical devices on a scene and later searches for relevant data.[126] To ensure that evidence is not compromised, forensic duplicates are created of originals,

124 IOS 2012 https://www.iso.org/standard/44381.html 9.
125 IOS 2012 https://www.iso.org/standard/44381.html 8.
126 Kerr 2005 *Miss LJ* 87.

and it is the forensic duplicates that are analysed.[127] The process followed in creating forensic duplicates should ultimately stand up to legal scrutiny.[128]

The collection of digital evidence is a forensic and procedural process which should always be performed with care.[129] Data should be collected in such a way that the information is retained in the exact state in which it was found.[130]

Cross[131] explains that "acquisition" refers to the process of collecting digital evidence from specific devices, normally the computers of suspects or victims.

The process of creating forensic duplicates usually commences by removing the hard drive from the computer of the victim or suspect and by connecting the hard drive to a write-protector device.[132] This procedure is in line with the principles set out by the ACPO[133] and the IOS[134] − the actions of investigators should not change data and, where possible, forensic duplicates should be made of the relevant data and these forensic duplicates should be analysed.

A write-protector device places a computer in a read-only form.[135] This device prevents actions taken by investigators, such as opening and closing files or searching through files from influencing or changing metadata. This device allows digital forensic investigators to conduct preliminary searches on computers to establish whether these computers contain relevant information or not.

At this stage, evidence can be browsed to determine whether it contains relevant evidence or whether imaging can be started without browsing the evidence. Once it is determined that devices contain relevant evidence, forensic duplicates of the evidence should be made. This is done by means of a number of forensic software programs which allow digital forensic investigators to create forensic duplicates of devices. Nieman[136] explains

127 Kessler *Judges' Awareness* 37.
128 Nieman 2009 *JILT* 22.
129 Kanellis *Digital Crime* 273.
130 Council of Europe 2001 http://www.oas.org/juridico/english/cyb_pry_coe.pdf 33.
131 Cross *Scene of the Cybercrime* 210.
132 Nieman 2009 *JILT* 22.
133 ACPO 1997 http://www.digital-detective.net/digital-forensics-documents/ACPO_Good_Practice_Guide_for_Digital_Evidence_v5.pdf 4.
134 IOS 2012 https://www.iso.org/standard/44381.html 6-8.
135 National Institute of Justice *Forensic Examination of Digital Evidence* 41.
136 Nieman 2009 *JILT* 22.

that bit-by-bit copies do exactly what the name suggests – copies are created bit-by-bit. A bit is the smallest size that data can be broken up into, an exact replica of every sector of a hard drive. Bit-by-bit copies are exact reproductions of digital records that contain all of the data, even hidden or deleted data.[137] Forensic duplicates and original pieces of evidence are exact copies of one another based and proven on scientific principles, and they can therefore be considered as duplicate originals.[138] With the current technology available, digital forensic investigators are able to collect a single file from a computer or a whole folder or the whole hard drive, including empty or unallocated space.[139] To create forensic duplicates can be a lengthy process. According to the Digital Intelligence,[140] an average transfer rate to create forensic duplicates is approximately 6GB per minute. If a hard drive is 500GB in size, it therefore takes 83 minutes to create one forensic duplicate and another 83 minutes to verify the integrity of a forensic duplicate. Creating forensic duplicates of a server can easily take more than 12 to 24 hours.

During collection processes, forensic programmes use a cryptographic hashing algorithm to ascertain the hash value of data. This is referred to as the MD5 hash algorithm or SHA1 hash algorithm. Nieman[141] correctly states that this hash value is often referred to as the electronic fingerprint of a piece of data.

The MD5 hash algorithm is a 128 bit hash value, while the SHA1 algorithm is a 160 bit hash value and the SHA1 hash is considered to be a more complex and more secure algorithm.[142] Schneier[143] explains that the MD5 hash value has a key size of 128 bits with 3.4 × 1038 possible combinations. The chance of randomly finding two files that produce the same hash value should be computationally unfeasible. Digital forensic investigators can therefore mathematically − beyond a reasonable doubt − show in court that digital evidence has not changed by even one character.

137 Angermeier 2010 *J Crim L & Criminology* 1615.
138 Van Deusen Phillips 2010 https://crlgrn.wordpress.com/2010/07/27/legal-considerations-for-electronic-evidence-part-5-original-vs-duplicate-documents-unfair-prejudice/.
139 Vandeven 2014 https://www.sans.org/reading-room/whitepapers/forensics/forensic-images-viewing-pleasure-35447 1.
140 Digital Intelligence 2016 https://www.digitalintelligence.com/products/forensic_duplicator/.
141 Nieman 2009 *JILT* 22.
142 Thompson 2005 *Digital Investigation* 39.
143 Schneier *Applied Cryptography* 436-441.

An example of hash values for the word "CAT" is:

MD5 hash value – c01ae1a5f122f25ce5675f86028b536a

SHA1 hash value – cf9b775c2c444520178d30c267440066c6eff6e8

Losey[144] explains that if one single character in a computer is changed, the hash value changes. If the word "CAT" is changed, for example, to "CATS", the hash values change to:

MD5 hash value – ee77f71f2b809c0f6d92320fc9b480f6

SHA1 hash value – c7da99899675795b2f1d94607dbe57b731dd2255

Brown[145] states that an imaging process is a scientific process and subject to the Daubert reliability test,[146] which was formulated in *Daubert v Merrell Dow Pharmaceuticals, Inc*.[147] This scientific requirement is further discussed in the ISO/IEC DIS 27043 Standard below.

3.2.2.2 ISO/IEC 27043 Standard on Information Technology − Security techniques − Incident investigation principles and processes

The American Academy of Forensic Sciences identified digital forensics as a forensic science.[148] As it is a scientific discipline, evidence prepared through digital forensics should meet the same standards as other scientific and technical evidence to be admissible in court.[149] The final draft of the ISO/IEC 27043 Standard on information technology − Security techniques − Incident investigation principles and processes[150] - specify that persons can be considered experts based on their experience, knowledge, skill, training or education. The opinions, theories, processes, procedures and tools used by experts should be evaluated against the Daubert test,[151] which has for long been the *de facto* test in the United States of America and is applied by courts to scientific procedures used to prepare or uncover

144 Losey 2007 https://e-discoveryteam.com/school/computer-hash-5f0266c4c326b9a1ef9e39cb78c352dc/.
145 Brown *Computer Evidence* 28.
146 Kessler *Judges' Awareness* 4.
147 *Daubert v Merrell Dow Pharmaceuticals, Inc* 509 US 579 (1993).
148 AAFS 2008 http://www.aafs.org/students/choosing-a-career/types-of-forensic-scientists-disciplines-of-aafs/.
149 Kessler *Judges' Awareness* 20.
150 IOS 2014 https://www.iso.org/standard/44407.html 4.
151 *Daubert v Merrell Dow Pharmaceuticals, Inc* 509 US 579 (1993).

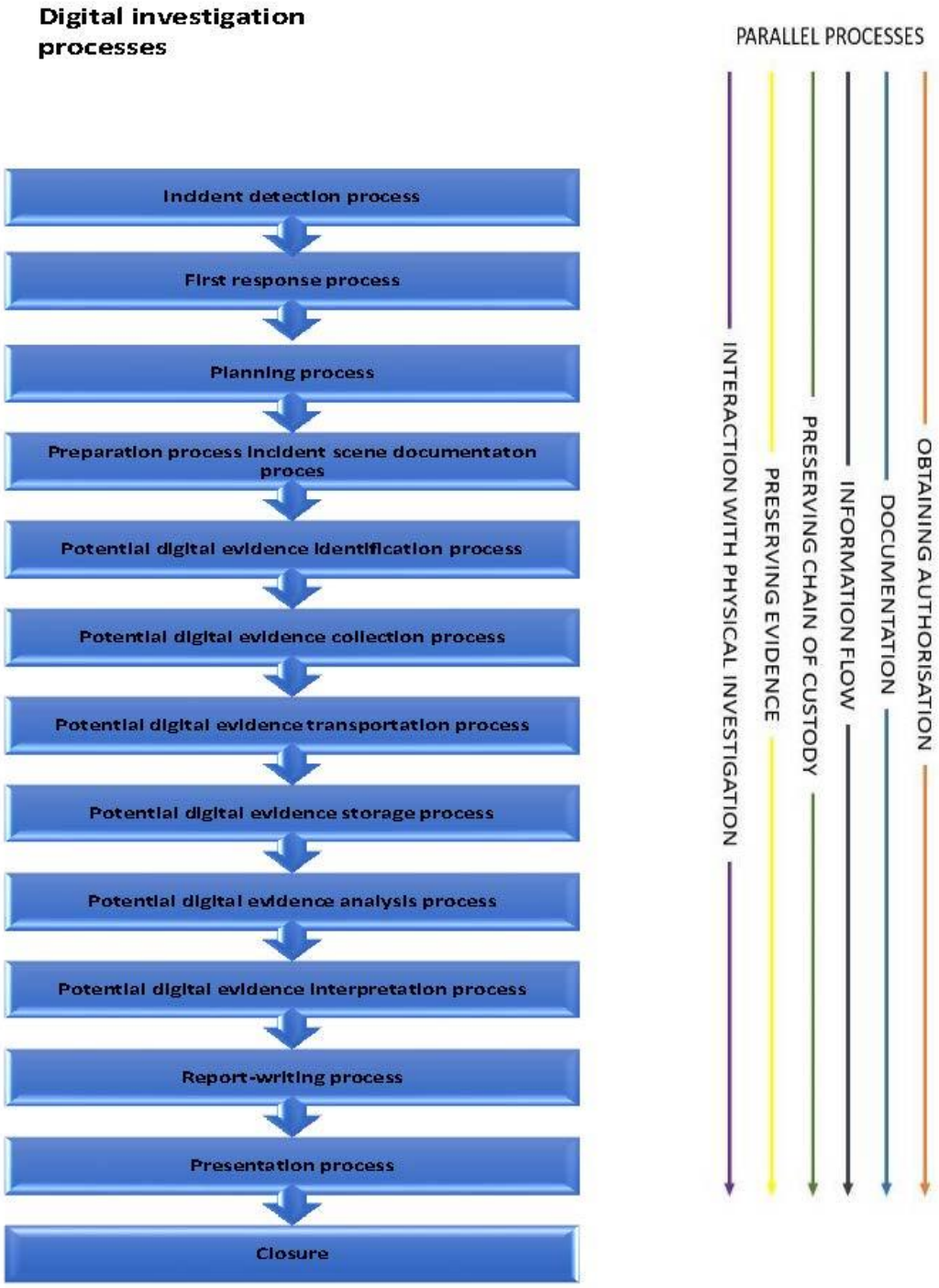
evidence. The Daubert test comprises the following factors that should be taken into account to ensure the integrity of evidence:[152]

- The theories and techniques used by experts should have been tested.
- The theories and techniques should have been subjected to peer review and should appear in publications.
- Any error rates should be known to the experts and have been reported.
- Experts should be governed by standards governing their applications.
- The theories and techniques used by experts should enjoy widespread acceptance.

The ISO/IEC 27043 Standard expanded and sets out the different phases of a digital investigation. It is divided into two main areas, namely digital investigation processes and the concurrent or parallel processes depicted below.[153]

152 *Daubert v Merrell Dow Pharmaceuticals, Inc* 509 US 579 (1993).
153 IOS 2014 https://www.iso.org/standard/44407.html.

Figure 1 – Digital forensic processes[154]



A summary of the different phases of a forensic investigation,[155] as depicted in Figure 1, includes:

154 IOS 2014 https://www.iso.org/standard/44407.html 14.

- *Detection phase* – incidents are detected.
- *First responder phase* − digital forensic investigators attend to incidents.
- *Planning phase* − investigations of incidents are planned.
- *Preparation phase and scene documentation phase* − preparation steps are taken to investigate incidents and document actions are taken on scenes.
- *Evidence identification phase* − potentially relevant evidence is identified.
- *Evidence collection phase* − evidence is collected.
- *Evidence transportation phase* − evidence is transported from scenes to digital forensic laboratories.
- *Evidence storage phase* − digital evidence is securely stored.
- *Evidence analysis phase* − evidence is analysed to determine its relevance.
- *Evidence interpretation phase* − evidence is interpreted in relation to its evidential value.
- *Reporting phase* − evidence is reported on.
- *Presentation phase* − testimonies or overviews are provided regarding the evidence.
- *Closure phase* – cases are archived.

The parallel processes include:

- Obtaining of authorisation to investigate incidents.
- Documentation of all actions during investigations.
- Continual information flow between digital forensic investigators and forensic investigators.

155 IOS 2014 https://www.iso.org/standard/44407.html 14-21.

- Maintaining chain-of-custody.
- Preserving the integrity of evidence.
- Interaction with physical investigations.

Three of the parallel processes set out by the standard are of paramount importance:

Obtaining authorisation

Proper authorisation should be obtained for each process performed during an investigation. Authorisation may be required from government authorities, system owners, system custodians and principals. For the purpose of this article, proper authorisation is achieved through the application for search and seizure warrants in terms of the provisions stipulated in sections 20 and 21 of the *Criminal Procedure Act*.

Preserving the chain of custody

A traditional requirement for proving the integrity of evidence is the chain of custody. Van der Merwe *et al.*[156] state that the prosecution needs to convince the court that the evidence was not interfered with from the time it was seized to the presentation in court. It is therefore critical that forensic investigators should ensure that digital evidence remains secure throughout the analysis.[157]

The chain of custody requirements were expanded upon in the ISO/IEC DIS 27037 Standard. These requirements relate to the ability of digital forensic investigators to account for all the acquired evidence from the point when it was within their custody.[158] A chain of custody can be viewed as a record that chronologically captures the movements and handling of evidence. A chain of custody should contain:

- a unique identifier;
- a record of who accessed the evidence at what time and place;
- a record of who checked the evidence in or out of storage and for what reason or under whose authority;

156 Van der Merwe *et al Information and Communications Technology Law* 85.
157 Cross *Scene of the Cybercrime* 211.
158 IOS 2012 https://www.iso.org/standard/44381.html 10.

- a record of any unavoidable changes made to the evidence, who made the changes and a justification for introducing the evidence to court.

Schetina, Green and Carlson,[159] together with Lange and Nimsger,[160] state the importance of a chain of custody in relation to the admissibility of digital evidence and say that courts need to be informed concerning the measures that were adhered to. A chain of custody ensures that evidence was not tampered with. Standard digital forensic processes − if followed and executed correctly − support and contribute to the chain of custody requirements.

5 Conclusions

It is evident that the uniqueness of digital evidence poses complications to traditional legal approaches. Digital evidence encompasses both tangible devices and intangible data and requires special methodologies to identify and collect all relevant evidence. The seizure of all data on computers can be viewed as a too extensive action due to the fact that not all of the relevant information is contained in files. It can reside in different locations on computers. The technical nature of cybercrimes and subsequent technical expert testimony adds further dynamics that are faced by digital forensic investigators.

The technical analysis and interpretation of terminology in relation to digital evidence are aspects that will be debated at length in South African courts in years to come. These interpretations can be problematic in terms of data, but a sound understanding can be gained from case law with regard to technical issues. It is argued that the "premises" described in search and seizure warrants should be the premises of suspects, and the interpretation of "search" should include actions in which the content of data becomes exposed. It is proposed that "search actions" such as look, locate, separate the information, interpret and analyse should be recognised. The creation of forensically-sound duplicate original records should constitute the seizure of data as items or articles of digital information in any form and should be recognised as original duplicates.

The originality, reliability, integrity and admissibility of digital evidence should be maintained as follows:

159 Schetina, Green and Carlson *Internet Site Security* 351.
160 Lange and Nimsger *Electronic Evidence* 76.

- Data should not be changed or altered.
- Original evidence should not be directly examined.
- Forensically sound duplicates should be created.
- Digital forensic analyses should be performed by competent persons.
- Digital forensic analyses should adhere to relevant local legal requirements.
- Audit trails should exist consisting of all required documents.
- Chains of custody should be protected.
- Processes and procedures should be proper while recognised and accepted by the industry.

If the ACPO (1997) principles and ISO/IEC 27043 and 27037 Standards are followed as a forensic framework, then the actions of digital forensic investigators should be legally acceptable.

Bibliography

Literature

Angermeier 2010 *J Crim L & Criminology*
Angermeier V "Swinging for the Fences: How Comprehensive Drug Testing, Inc. Missed the Ball on Digital Searches" 2010 *J Crim L & Criminology* 1587-1632

Anon *Current Policy and Procedure*
Anon *Current Policy and Procedure on Digital Search and Seizure by the SAPS* [telephonic interview] (15 September 2016 Pretoria)

Basdeo *Constitutional Perspective of Police Powers*
Basdeo V *Constitutional Perspective of Police Powers of Search and Seizure in the Criminal Justice System* (LLM-thesis UNISA 2009)

Basdeo 2012 *SACJ*
Basdeo V "The Legal Challenges of Search and Seizure of Electronic Evidence in South African Criminal Procedure: A Comparative Analysis" 2012 *SACJ* 198-211

Bouwer 2014 *SACJ*
Bouwer GP "Search and Seizure of Electronic Evidence: Division of the Traditional One-step Process into a New Two-step Process in a South African Context" 2014 *SACJ* 156-171

Brenner and Fredericksen 2002 *Mich Telecomm & Tech L Rev*
Brenner SW and Fredericksen BA "Computer Searches and Seizures: Some Unresolved Issues" 2002 *Mich Telecomm & Tech L Rev* 60-63, 81-82

Brown *Computer Evidence*
Brown CLT *Computer Evidence: Collection and Preservation* 2nd ed (Charles River Media Hingham 2010)

Casey *Handbook of Computer Crime*
Casey E (ed) *Handbook of Computer Crime: Forensic Tools and Technology* (Academic Press London 2000)

Casey *Digital Evidence*
Casey E (ed) *Digital Evidence and Computer Crime: Forensics Science, Computers and the Internet* 3rd ed (Elsevier Amsterdam 2011)

Craiger and Shenoi *Advances in Digital Forensics*
Craiger JP and Shenoi S *Advances in Digital Forensics III* (International Federation for Information Processing New York 2007)

Cross *Scene of the Cybercrime*
Cross M *Scene of the Cybercrime* 2nd ed (Syngress Publishing Arlington 2008)

Gibson *Neuromancer*
Gibson W *Neuromancer* (Phantasia Washington 1984)

Guzzi 2012 *Am Crim L Rev*
Guzzi S "Digital Searches and the Fourth Amendment: The Interplay between the Plain View Doctrine and Search-protocol Warrant Restrictions" 2012 *Am Crim L Rev* 301-329

Hart 1958 *Harv L Rev*
Hart HLA "Positivism and the Separation of Law and Morals" 1958 *Harv L Rev* 593-629

Jopek-Bosiacka 2011 *Research in Language*
Jopek-Bosiacka A "Defining Law Terms: A Cross-cultural Perspective" 2011 *Research in Language* 9-29

Kanellis *Digital Crime*
Kanellis P *Digital Crime and Forensic Science in Cyberspace* (Idea Group London 2006)

Kerr 2005 *Harv L Rev*
Kerr OS "Searches and Seizures in a Digital World" 2005 *Harv L Rev* 531-585

Kerr 2005 *Miss LJ*
Kerr OS "Search Warrants in an Era of Digital Evidence" 2005 *Miss LJ* 85-108

Kessler *Judges' Awareness*
Kessler G *Judges' Awareness, Understanding, and Application of Digital Evidence* (PhD-thesis Nova Southeastern University 2010)

Lange and Nimsger *Electronic Evidence*
Lange MCS and Nimsger KM *Electronic Evidence and Discovery: What Every Lawyer should Know* (ABA Chicago 2004)

Mohay *et al Computer and Intrusion Forensics*
Mohay GM *et al Computer and Intrusion Forensics* (Artech House Boston 2003)

National Institute of Justice *Forensic Examination of Digital Evidence*
National Institute of Justice *Forensic Examination of Digital Evidence: A Guide for Law Enforcement* (US Department of Justice Washington 2004)

Nieman *Search and Seizure*
Nieman A *Search and Seizure, Production and Preservation of Electronic Evidence* (PhD-thesis North West University 2006)

Nieman 2009 *JILT*
Nieman A "Cyberforensics: Bridging the Law / Technology Divide" 2009 *JILT* 1-29

SALRC *Discussion Paper 9*
South African Law Reform Commission *Discussion Paper 99, Project 108. Computer-related Crime: Preliminary Proposals for Reform in respect of Unauthorised Access to Computers, Unauthorised Modification of Computer Data and Software Applications and Related Procedural Aspects* (SALRC Pretoria 2002)

SALRC *Issue Paper 27*
South African Law Reform Commission *Issue Paper 27, Project 126. Review of the Law of Evidence - Electronic Evidence in Criminal and Civil Proceedings: Admissibility and Related Issues* (SALRC Pretoria 2010)

SAPS *National Instruction 2/2002*
South African Police Service *National Instruction 2/2002: Search and Seizure* (SAPS Pretoria 2002)

SAPS *Practical Guide to Apply for Search Warrants*
South African Police Service *Practical Guide to Apply for Search Warrants in terms of Section 21 of the Criminal Procedure Act 51 of 1977* (SAPS Pretoria 2016)

Schetina, Green and Carlson *Internet Site Security*
Schetina ES, Green K and Carlson J *Internet Site Security* (Addison-Wesley Boston 2002)

Schneier *Applied Cryptography*
Schneier B *Applied Cryptography, Second Edition Protocols, Algorithms and Source Code in C* (Wiley New Jersey 1996)

Scholtz *Towards an Automated Digital Data Forensic Model*
Scholtz J *Towards an Automated Digital Data Forensic Model with Specific Reference to Investigation Processes: A Survey of Actual and Desirable Practice* (MCIS-thesis Auckland University of Technology 2009)

Silvernail 1997 *Ala Law*
Silvernail SJ "Electronic Evidence: Discovery in the Computer Age" 1997 *Ala Law* 176-177

Steytler *Constitutional Criminal Procedure*
Steytler N *Constitutional Criminal Procedure: A Commentary on the Constitution of the Republic of South Africa* (LexisNexis Butterworths Durban 2004)

Thompson 2005 *Digital Investigation*
Thompson E "MD5 Collisions and the Impact on Computer Forensics" 2005 *Digital Investigation* 36-40

UN *UNCITRAL Model Law*
United Nations *UNCITRAL Model Law on Electronic Commerce with Guide to Enactment* (United Nations New York 1996)

Vacca *Computer Forensics*
Vacca JR *Computer Forensics: Computer Crime Scene Investigation* 2nd ed (Charles River Media Hingham 2005)

Van der Merwe *et al Information and Communications Technology Law*
Van der Merwe D *et al Information and Communications Technology Law* (LexisNexis Durban 2008)

Wang 2007 *CSI*
Wang SJ "Measures of Retaining Digital Evidence to Prosecute Computer Based Cybercrimes" 2007 *CSI* 216-223

Case law

Canada

R v Munshi 2002 CanLII 39110 (ON SC)

R v Vu 2013 3 SCR 657 (SCC)

South Africa

Bennett v Minister of Safety and Security (TPD) (unreported) case number 10828/2005 of 13 May 2005

Heaney v S 2016 ZAGPPHC 257 (19 April 2016)

Minister of Safety and Security v Bennett 2008 2 All SA 26 (SCA)

Minister of Safety and Security v Xaba 2003 1 All SA 596 (D)

Muller v BOE Bank Ltd 2011 1 SA 252 (WCC)

National Director of Public Prosecutions v Zuma 2008 1 All SA 197 (SCA)

Ntoyakhe v Minister of Safety and Security 2000 1 SA 257 (E)

Powell v Van der Merwe 2005 1 All SA 149 (SCA)

Rudolph v Commissioner for Inland Revenue 1996 7 BCLR 11 (CC)

Thint (Pty) Ltd v National Director of Public Prosecutions, Zuma v National Director of Public Prosecutions 2009 1 SA 1 (CC)

United States of America

Arizona v Hicks 480 US 321, 325 (1987)

Daubert v Merrell Dow Pharmaceuticals, Inc 509 US 579 (1993)

Lorraine v Markel American Ins Co (2007) 241 FRD 534, 544 (D Md 2007)

United States v Flores-Lopez No 10-3803 (7th Cir 2012)

Legislation

Australia

Australian Crimes Act 12 of 1914

New Zealand

Search and Surveillance Act 24 of 2012

South Africa

Constitution of the Republic of South Africa, 1996

Criminal Procedure Act 51 of 1977

Draft Cybercrimes and Cybersecurity Bill, 2016

Electronic Communications and Transactions Act 25 of 2002

International instruments

Council of Europe Convention on Cybercrime (2001)

UNCITRAL Model Law on Electronic Commerce (1996)

Internet sources

AAFS 2008 http://www.aafs.org/students/choosing-a-career/types-of-forensic-scientists-disciplines-of-aafs/

American Academy of Forensic Sciences 2008 *AAFS Digital and Multimedia Sciences* http://www.aafs.org/students/choosing-a-career/types-of-forensic-scientists-disciplines-of-aafs/ accessed 5 January 2016

ACPO 1997 http://www.digital-detective.net/digital-forensics-documents/ACPO_Good_Practice_Guide_for_Digital_Evidence_v5.pdf

Association of Chief Police Officers 1997 *Good Practice Guide for Computer-Based Electronic Evidence Version 5* http://www.digital-detective.net/digital-forensics-documents/ACPO_Good_Practice_Guide_for_Digital_Evidence_v5.pdf accessed 27 December 2015

Chisum and Turvey 2000 http://www.profiling.org/journal/vol1_no1/jbp_ed_january2000_1-1.html

Chisum WJ and Turvey BE 2000 *Evidence Dynamics: Locard's Exchange Principle and Crime Reconstruction* http://www.profiling.org/journal/vol1_no1/jbp_ed_january2000_1-1.html accessed 29 January 2018

Christensson 2005 http://pc.net/helpcenter/answers/difference_between_analog_and_digital
Christensson P 2005 *What is the Difference between Analog and Digital Technology?* http://pc.net/helpcenter/answers/difference_between_analog_and_digital accessed 10 December 2015

Clark and Connolly 2006 https://www.law.Georgetown.edu/academics/academic-programs/legal-writing-scholarship/writing-center/upload/statutoryinterpretation.pdf
Clark K and Connolly M 2006 *A Guide to Reading, Interpreting and Applying Statutes* https://www.law.georgetown.edu/academics/academic-programs/legal-writing-scholarship/writing-center/upload/statutoryinterpretation.pdf accessed 15 February 2016

Council of Europe 2001 http://www.oas.org/juridico/english/cyb_pry_coe.pdf
Council of Europe 2001 *The Council of Europe Convention on Cybercrime: Status Quo and Future Challenges* http://www.oas.org/juridico/english/cyb_pry_coe.pdf accessed 29 April 2016

Digital Intelligence 2016 https://www.digitalintelligence.com/products/forensic_duplicator/
Digital Intelligence 2016 *Forensic Duplicator* https://www.digitalintelligence.com/products/forensic_duplicator/ accessed 1 April 2016

Francoeur 2003 http://www.scribd.com/doc/276157/The-Principles-of-Electronic-Agreement-Legal-Admissibility-WP-8-07
Francoeur J 2003 *The Principles of Electronic Agreement Legal Admissibility* http://www.scribd.com/doc/276157/The-Principles-of-Electronic-Agreement-Legal-Admissibility-WP-8-07 accessed 14 June 2016

Forensic Handbook 2012 http://www.forensichandbook.com/locards-exchange-principle/
Forensic Handbook 2012 *Locard's Exchange Principle* http://www.forensichandbook.com/locards-exchange-principle/ accessed 16 July 2016

Forensics Library 2014 http://aboutforensics.co.uk/edmond-locard/
The Forensics Library 2014 *Edmond Locard* http://aboutforensics.co.uk/edmond-locard/ accessed 12 December 2015

Hofman 2006 http://hofman@law.uct.ac.za
Hofman J 2006 *Electronic Evidence in South Africa* http://hofman@law.uct.ac.za accessed 2 November 2014

IOS 2012 https://www.iso.org/standard/44381.html
International Organisation of Standardisation 2012 *ISO/IEC 27037:2012 Information Technology − Security Techniques − Guidelines for Identification, Collection, Acquisition, and Preservation of Digital Evidence* https://www.iso.org/standard/44381.html accessed 22 February 2016

IOS 2014 https://www.iso.org/standard/44407.html
International Organisation of Standardisation 2014 *ISO/IEC 27043:2014 Information Technology − Security Techniques − Incident Investigation Principles and Processes* https://www.iso.org/standard/44407.html accessed 22 February 2016

Lidbury and Boland 2012 http://www.insidecounsel.com/2012/05/11/technology-forensically-sound-collection-of-esi
Lidbury T and Boland M 2012 *Technology: Forensically Sound Collection of ESI* http://www.insidecounsel.com/2012/05/11/technology-forensically-sound-collection-of-esi accessed 13 January 2016

Losey 2007 https://e-discoveryteam.com/school/computer-hash-5f0266c4c326b9a1ef9e39cb78c352dc/
Losey R 2007 *e-Discovery Team Blog: Hash* https://e-discoveryteam.com/school/computer-hash-5f0266c4c326b9a1ef9e39cb78c352dc/ accessed 16 July 2016

Lowe Date Unknown http://www.dummies.com/how-to/content/digital-electronics-binary-basics.html
Lowe D Date Unknown *Digital Electronics: Binary Basics* http://www.dummies.com/how-to/content/digital-electronics-binary-basics.html accessed 2 September 2015

Oxford English Dictionary 2016 https://en.oxforddictionaries.com/definition/cellular_phone
Oxford English Dictionary 2016 *Cellular Phone* https://en.oxforddictionaries.com/definition/cellular_phone accessed 23 October 2016

Oxford English Dictionary 2016 http://www.oxforddictionaries.com/definition/english/computer
Oxford English Dictionary 2016 *Computer* http://www.oxforddictionaries.com/definition/english/computer accessed 23 April 2016

Oxford English Dictionary 2016 https://en.oxford dictionaries.com/definition/cyber
Oxford English Dictionary 2016 *Cyber* https://en.oxforddictionaries.com/definition/cyber accessed 23 October 2016

Palmer 2001 https://isis.poly.edu/kulesh/forensics/docs/DFRWS_RM_ Final.pdf
Palmer G 2001 *A Road Map for Digital Forensic Research* https://isis.poly.edu/kulesh/forensics/docs/DFRWS_RM_Final.pdf accessed 10 November 2015

Spencer 2014 https://www.quora.com/Whats-the-difference-between-electronic-and-digital
Spencer M 2014 *What's the Difference between "Electronic" and "Digital"?* https://www.quora.com/Whats-the-difference-between-electronic-and-digital accessed 23 May 2016

SWGDE 2012 https://www.swgit.org/pdf/SWGDE%20and%20SWGIT%20Digital%20and%20Multimedia%20Evidence%20Glossary?docID=60
Scientific Working Group on Digital Evidence 2012 *SWGDE/SWGIT Digital and Multimedia Evidence Glossary* https://www.swgit.org/pdf/SWGDE%20and%20SWGIT%20Digital%20and%20Multimedia%20Evidence%20Glossary?docID=60 accessed 3 May 2015

Van Deusen Phillips 2010 https://crlgrn.wordpress.com/2010/07/27/legal-considerations-for-electronic-evidence-part-5-original-vs-duplicate-documents-unfair-prejudice/
Van Deusen Phillips S 2010 *The Documentalist - Legal Considerations for Electronic Evidence, Part 5: Original vs Duplicate Documents and Unfair Prejudice* https://crlgrn.wordpress.com/2010/07/27/legal-considerations-for-electronic-evidence-part-5-original-vs-duplicate-documents-unfair-prejudice/ accessed 23 October 2015

Vandeven 2014 https://www.sans.org/reading-room/whitepapers/forensics/forensic-images-viewing-pleasure-35447
Vandeven S 2014 *Forensic Images: For Your Viewing Pleasure* https://www.sans.org/reading-room/whitepapers/forensics/forensic-images-viewing-pleasure-35447 accessed 2 October 2015

Woodford 2007 http://www.explainthatstuff.com/howcomputerswork.html
Woodford C 2007 *Computers* http://www.explainthatstuff.com/howcomputerswork.html accessed 22 February 2016

List of Abbreviations

AAFS	American Academy of Forensic Sciences
ACPO	Association of Chief Police Officers
Ala Law	The Alabama Lawyer
Am Crim L Rev	American Criminal Law Review
CSI	Computer Standards and Interfaces
DNA	Deoxyribonucleic Acid
GB	Gigabyte
Harv L Rev	Harvard Law Review
IOS	International Organisation of Standardisation
J Crim L & Criminology	Journal of Criminal Law and Criminology
JBP	Journal of Behavioral Profiling
JILT	Journal of Information, Law and Technology
Mich Telecomm & Tech L Rev	Michigan Telecommunications and Technology Law Review
Miss LJ	Mississippi Law Journal
NLJ	New Law Journal
SACJ	South African Journal of Criminal Justice
SALRC	South African Law Reform Commission
SAPS	South African Police Service
SWGDE	Scientific Working Group on Digital Evidence
TB	Terabyte
UN	United Nations
UNCITRAL	United Nations Commission on International Trade Law