Ensuring the Legality of the Digital Forensics Process in South Africa

Jason Jordaan
Security and Networks Research Group
Rhodes University
Grahamstown, South Africa

ABSTRACT
In most legal systems, it is crucial that evidence that is obtained for use in any judicial proceedings, especially criminal prosecutions, is obtained lawfully. In other words, no crimes should be committed in the obtaining and examining of any evidence, which will be later, be relied upon in court.

Section 86 of the Electronic Communications and Transactions Act 25 of 2002 in South Africa creates a criminal offence of unauthorized access to data, which has a significant potential impact on the acquisition, examination, and analysis of digital evidence; in that traditional digital forensic processes, unless legally authorized, may potentially be in contravention of this law.

The legal ramifications for both digital forensics practitioners and the cases that they are engaged on are identified, and appropriate legal solutions are provided to ensure that digital forensic practitioners do not contravene the existing legislation.

Keywords
Digital forensics, digital evidence, legal liability, authorization to access data, admissibility of evidence.

1. INTRODUCTION
Digital evidence is now a fundamental part of many investigations. Digital evidence is defined as information of a legal probative value that is either stored, or transmitted in a digital form [1]. The proliferation of digital devices and the Internet has meant that digital evidence can be present in virtually any case, and is not limited simply to computer crimes, but is relevant to the investigation of almost any crime [2]. Over half of the cases investigated by the Federal Bureau of Investigation use some type of digital evidence [3]. In the United States of America, digital evidence has become common in courts, and cases are frequently decided on digital evidence [3]. While no similar definitive evidence exists in the South African environment, observations made by the researcher support the assertion that more and more crimes in South Africa are dependent on digital evidence of one form or another.

Key factors in ensuring the admissibility of digital evidence involve processes based on the practices of criminalistics and forensic science. In relation to digital evidence, digital forensics is a critical component in bringing this evidence to court, as the use of digital forensics follows certain standard processes and procedures which tend to persuade the court to admit digital evidence and give due and proper evidential weigh to it [4]. As digital forensics is a specialised field, the courts in South Africa have tended to treat evidence presented as a result of a digital forensic process as expert witness evidence, similar to that presented by a scientist. As persons who are considered by the courts as experts, they must be held to the standard of an expert, especially within a legal context.

Ignorantia juris non excusat (ignorance of the law does not excuse) or ignorantia legis neninem excusat (ignorance of the law excuses no one) are legal principles which simply state that a person who is unaware of any particular law may not escape liability for a contravention of that law simply because he or she was unaware of it. As experts in the field of digital forensics, digital forensic practitioners are expected to have a good understanding of applicable laws applicable to themselves and their field.

In the field of digital forensics, the Electronic Communications and Transactions Act is a crucial piece of legislation that digital forensic practitioners need to know and understand, as failure to understand the offences contained in it could impact negatively on the practices of digital forensics practitioners.

2. UNLAWFUL ACCESS TO DATA
The Electronic Communications and Transactions Act 25 of 2002 created a number of statutory criminal offences aimed at addressing cyber crime in South Africa. These statutory offences are detailed in Section 86, 87, and 88 of the Act [5].

Section 86(1) of the Electronic Communications and Transactions Act 25 of 2002 creates the criminal offence of unlawful access to data. Section 86(1) states that subject to the Interception and Monitoring Prohibition Act, a person who intentionally accesses of intercepts any data without authority or permission to do so is guilty of an offence [5].

This offence has three essential elements:

- Access
- Data
- Without Authority or Permission

2.1 Access
The definitions section in Section 1 of the Electronic Communications and Transactions Act 25 of 2002 does not provide a specific definition of the term "access", however, Section 85 defines access to include, unless the context indicates otherwise, the actions of a person who after taking note of any data becomes aware that they are not authorized to access that data, and continues to access it [5]. In other words, if a person is viewing or otherwise interacting with any data and they realize that they do not have the necessary authority or permission to view of interact with that data, and they continue to do so, then they are accessing the data in terms of this definition.

According to the Concise Oxford English Dictionary, the term access in relation to computing means to "obtain, examine, or retrieve data" [6].

In terms of the offense created by Section 86(1) of the Electronic Communications and Transactions Act 25 of 2002, due to the fact that access as a term is not specifically defined,

the common usage of the term as found in the Concise Oxford English Dictionary is considered to be an accurate general definition of what is meant by access to data, namely:

- To obtain data
- To examine data
- To retrieve data

Should a person do any of these actions in relation to data, then they will have accessed the data.

2.2 Data

Section 1 of the Electronic Communications and Transactions Act 25 of 2002 defines data as the electronic representation of information in any form [5]. In other words, so long as information is in an electronic form, in is considered to be data as defined in this Act. Neither information nor electronic form is specifically defined in this Act.

According to the Concise Oxford English Dictionary, the term information means "what is conveyed or represented by a particular sequence of symbols" [6]. At the most fundamental level, the data contained on a digital device or storage media exists in a binary numerical form, consisting of "1"and "0" in a sequence of such numbers, which are then represented at a byte level by hexadecimal numbers, and then later through various applications, as human readable information. This means that all binary data contained on an electronic device of storage media is considered information. In other words it can be stated that so long as information is in a binary digital format at its most basic representation level, then it satisfies the legal definition of data.

2.3 Authority or Permission

The Electronic Communications and Transactions Act 25 of 2002 does not defined authority (at least in terms of access to data), nor does it define permission [5].

According to the Concise Oxford English Dictionary, the term authority means "a person or organization exerting control" [6]. According the Oxford Dictionary of Law, it means "power delegated to a person or body to act in a particular way" [7]. To authorize is the process of giving authority, and in the Concise Oxford English Dictionary, it means "give permission for or approval to" [6]. According to the Concise Oxford English Dictionary, the term permission means "authorization" [6], which is a derivative word of "authorize".

In other words, authorization or permission can be defined as when a person or organization that has power over something gives the authority to another to have power over that thing.

3. THE DIGITAL FORENSICS PROCESS

Digital forensics involves the preservation, identification, extraction, and documentation of digital evidence stored as data or magnetically encoded information [8]. In essence, digital forensics is about evidence from computer, digital media, or digital devices which can stand up to scrutiny in court and be convincing [8]. The objective of digital forensics is in essence quite simple, and that is to recover, analyze, and present digital evidence in such a way that it is usable as evidence in a court of law [8].

One definition of digital forensics is that it is the science of acquiring, preserving, retrieving, and presenting data that has been processed electronically and stored on computer media [2]. Digital forensics has also been defined as computer investigation and analysis techniques that involve the identification, preservation, extraction, documentation, and interpretation of computer data to determine potential legal evidence [9]. Another definition of digital forensics is the application of science and engineering to the legal problems associated with digital evidence, in other words, it is a synthesis of science and law [10]. In another definition, digital forensics is the use of scientifically derived and proven methods towards the preservation, collection, validation, identification, analysis, interpretation, documentation, and presentation of digital evidence derived from digital sources for the purpose of facilitating or furthering the reconstruction of events, or helping to anticipate unauthorised actions [11].

3.1 Digital Evidence

Evidence can be defined as anything that tends to logically prove or disprove a fact at issue in a judicial case [2].

Digital evidence is defined as information of a legal probative value that is either stored, or transmitted in a digital form [1]. Another definition of digital evidence is that it is any data stored or transmitted using a computer that supports or refutes a theory of how an offence occurred, or addresses a critical element thereof such as intention or an alibi [1].

Digital evidence is fundamentally no more than data as defined in Section 1 of the Electronic Communications and Transactions Act 25 of 2002.

3.2 Digital Forensic Models

Digital forensics is process, with defined stages, and it is crucial that digital forensics be understood within that context as well. A number of models describe the various stages within this process.

The basic digital forensics methodology is [12]:

- Acquiring the evidence without altering or damaging the source.
- Authenticating that the evidence that you have collected is exactly the same as the source from which it was made.
- Analyze the evidence without altering it.

Another model of the digital forensic process includes the following stages [1]:

- Authorisation and Preparation.
- Identification.
- Documentation, Collection, and Preservation.
- Examination and Analysis.
- Reconstruction.
- Reporting Results.

Based on the various models, the common digital forensic process includes acquiring the digital evidence, examining the digital evidence, and analyzing the digital evidence.

3.3 Accessing Data as Part of the Digital Forensic Process

To conduct a digital forensic examination, a digital forensic practitioner needs to first gain access to the electronic device or digital storage media that contains the evidential data that they seek. This requires access to the physical object containing the data. Without this level of access, the digital forensic examination cannot proceed.

Once the physical object containing the data has been secured, the digital forensic examiner generally makes a forensic image of this data, which requires the digital forensic examiner to access the data contained on the device to make

the forensic image. In essence at this stage a digital forensic examiner is obtaining or retrieving data, and thus would constitute access to data.

Once the data has been secured by the forensic practitioner, it is crucial to examine and analyze it to identify data of evidential value, and to interpret that evidence. In essence at this stage a digital forensic examiner is examining data and thus would constitute access to data.

In instances where a digital forensic practitioner has to examine live data on an electronic device as part of a digital triage process, then that process would also constitute access to data.

At the most fundamental level, the core digital forensic processes require the digital forensic examiner to access data.

4. DIGITAL FORENSICS AND THE CONTRAVENTION OF SECTION 86(1) OF THE ELECTRONIC COMMUNICATIONS AND TRANSACTIONS ACT 25 OF 2002

The fundamental offense defined by Section 86(1) of the Electronic Communications and Transactions Act 25 of 2002, is when anyone accesses any data without authorization or permission.

Considering that the essential digital forensic processes require a digital forensic practitioner to access data, and that this access as a fundamental part of the digital forensics process is always intentional; if this access occurs without the appropriate permission or authorization, then they commit a criminal offence.

In other words, if any digital forensics process is performed in relation to any data (including forensic acquisition and imaging, examination, and analysis), and that they did not have permission or authority from an appropriate person or authority to do so; then they have contravened Section 86(1) of the Electronic Communications and Transactions Act 25 of 2002, and could potentially be prosecuted and convicted.

5. THE NECESSITY FOR LEGAL AUTHORITY TO CONDUCT DIGITAL FORENSICS

For evidence to be useable in any court proceedings, it must be admissible. If it is not admissible, then in may not be considered in the case before court, as it may unfairly prejudice or give an unfair advantage to one of the parties of the court case. In addition to the legal requirements and rules which governed the use of digital evidence in court, traditional concepts in the law of evidence nevertheless still apply.

5.1 The Admissibility of Digital Evidence Obtained in Contravention of Section 86(1) of the Electronic Communications and Transactions Act 25 of 2002

Evidence is either admissible or inadmissible [9]. Admissible evidence is evidence that meets all regulatory and statutory requirements, and has been correctly obtained and handled [9]. The quickest methods to ensure that evidence will not be admissible in court would be to collect it in an illegal manner [9], or to obtain it without the correct authorisation [1].

Section 35(5) of the South African Constitution places a duty of the courts to rule evidence as inadmissible if it was obtained in violation of any right contained in the Bill of Rights, and if its admission would result in an unfair trial or be detrimental to the administration of justice [14]. Section 35(3) must be read with Section 35(3) of the Constitution which guarantees the right to a fair trial [14].

In general in South Africa, evidence that has been obtained unlawfully, that is in contravention of the law, then it would probably be ruled inadmissible in a criminal prosecution, and may potentially be ruled inadmissible in civil proceedings as well [9]. The key issue is whether or not allowing evidence that had been obtained unlawfully would render the trial unfair or be detrimental to the administration of justice [9].

Essentially this means that if the digital evidence has been obtained in contravention of Section 86(1) of the Electronic Communications and Transactions Act 25 of 2002, then there is a real probability that it could be ruled inadmissible in a court of law.

To insure that digital evidence is not at risk of being ruled inadmissible, it must be obtained legally, and as such digital forensic practitioners should ensure that they do not contravene Section 86(1) of the Electronic Communications and Transactions Act 25 of 2002, and thus there is a necessity to have the appropriate legal authority to conduct digital forensics.

5.2 Avoiding Criminal and Civil Liability

Beside the necessity for legal authority when conducting digital forensics to ensure that the digital evidence will be admissible and thus usable in a court of law, the other necessity for ensuring legal authority is to prevent criminal and civil liability by the digital forensic practitioner.

If a digital forensic examiner does not have the appropriate authority or permission to access the data necessary for the digital forensic process, and they do so, then they face the risk of being criminally prosecuted in terms of Section 86(1) of the Electronic Communications and Transactions Act 25 of 2002. Not only is there a risk of criminal prosecution, which carries the possibility of a fine or imprisonment not exceeding 12 months [5], but the digital forensic practitioner could potentially be subject to civil litigation for delict.

6. OBTAINING LEGAL AUTHORITY

To be able to conduct digital forensics, a digital forensics practitioner requires access to the data that they will conduct digital forensics processes on. This generally requires access to the physical electronic device or storage media containing the data, and the authority or permission to access these and thus the data contained thereon.

There are three methods to obtain the necessary legal authority to gain access to the physical electronic devices and storage media which contain data which is necessary for digital forensic processes. These are:

- Consent
- Search Warrant/Anton Pillar
- Subpoena

6.1 Consent

A person or organization in control of the physical electronic device or storage media containing the data, or the owner thereof, can consent to the access. This consent effectively provides authorization.

A key issue with consent is that the person should be informed of exactly what they are consenting to, and that the consent be provided voluntarily without undue influence or duress [15].

Consent could be used in both criminal and civil actions, and ideally should be obtained in writing.

6.2 Search Warrant/Anton Pillar

It certain instances, the State or its agents can gain access to the physical electronic device or storage media containing the data, without the permission of the controller or owner thereof, by using a search warrant issued in terms of applicable legislation. A copy of the applicable executed search warrant would constitute authorization.

In certain instances, the applicable legislation allows for searches and seizures to take place without a warrant in very particular circumstances. In these instances, it is suggested that a sworn affidavit from the person who conducted the search and seizure detailing the reasons why and what happened, would constitute authorization.

While search warrants are available only to the State and its agents, private persons and organizations can make use of civil processes to obtain what is essentially a civil search warrant, an Anton Pillar order. A copy of the executed Anton Pillar order would constitute authorization.

6.3 Subpoena

A court may issue a subpoena compelling a person or organization to produce the physical electronic device or storage media containing the data. This could be used in both criminal and civil matters. A copy of the subpoena would constitute authorization.

7. CONCLUSION

The digital forensic process, unless performed on data that has been obtained with the appropriate legal authorization, satisfies all of the element necessary for a contravention of Section 86(1) of the Electronic Communications and Transactions Act 25 of 2002.

This could result in digital evidence obtained as a result of these digital forensic processes being ruled inadmissible, or even potentially worse, the digital forensic practitioners involved being prosecuted or litigated against.

To ensure the legality of the digital forensic process, a key issue is to ensure that before any digital forensic processes are conducted on any data that the appropriate legal authority is in place.

8. REFERENCES

[1] Casey, E, (2004), *Digital Evidence and Computer Crime*, 2nd ed. London: Academic Press.

[2] Swanson, C R, Chamelin, N C, Territo, L, & Taylor, R W, (2006), *Criminal Investigation*, 9th ed. New York: McGraw-Hill.

[3] Peisert, S, Sishop, M, & Marzullo, K, (2008), "Computer Forensics in Forensics," in *Systematic Approaches to Digital Forensic Engineering*, pp. 102-122.

[4] Van Der Merwe, D, Roos, A, Pistorius, T, & Eiselen, S, (2008), *Information and Communications Technology Law*. Durban: LexisNexis.

[5] Republic of South Africa, (2002), *The Electronic Communications and Transactions Act 25 of 2002*. Pretoria: Government Printer.

[6] Oxford University, (2002), *Concise Oxford English Dictionary*, 10th ed., Judy Pearsall, Ed. Oxford: Oxford University Press.

[7] Oxford University, (2013), *Oxford Dictionary of Law*, 7th ed., Jonathan Law and Elizabeth A Martin, Eds. Oxford: Oxford University Press.

[8] Vacca, J R, (2005), *Computer Forensics: Computer Crime Scene Investigation*, 2nd ed. Boston: Thomson.

[9] Solomon, M G, Barrett, D, & Broom, N, (2005,) *Computer Forensics Jump Start*. Alameda: Sybex.

[10] Jones, A & Valli, C, (2009,) *Building a Digital Forensic Laboratory*. Burlington: Syngress.

[11] McKemmish, R, (2008), "When is Digital Evidence Forensically Sound?," in *Advances in Digital Forensics IV*, Indrajit Ray and Sujeet Shenoi, Eds. Boston: Springer, pp. 3-15.

[12] Sansurooah, K, (2006), "Taxonomy of Computer Forensics Methodologies and Procedures for Digital Evidence Seizure," in *Proceedings of the 4th Australian Digital Forensics Conference*, Perth, pp. 67-77.

[13] Schwikkard, P J & Van Der Merwe, S E, (2002), *Principles of Evidence*. Cape Town: Juta.

[14] Republic of South Africa, (1996), *The Constitution of the Republic of South Africa Act 108 of 1996*. Pretoria: Government Printer, 1996.

[15] Joubert, C, (2001), *Applied Law for Police Officials*, 2nd ed. Lansdowne: Juta.