WHAT'S INSIDE?

Ferlio

Group of Investigators

0860 337 546 / 0860 (F-E-R-L-I-O)

NEWSLETTER

Volume 12 – November 2021

In this newsletter, you will find an article the SA ex—policewoman who killed for insurance money, an insightful article regarding insurance fraud and an article about a notification scam. We also include an article provided by Jason Jordaan from DFIRLABS regarding the Cybercrimes Act.

SOUTH AFRICAN EX-POLICEWOMAN KILLED RELATIVES AND BOYFRIEND FOR INSURANCE CASH

BY BBC NEWS

South African ex-policewoman Nomia Rosemary Ndlovu has been found guilty of killing five relatives and her boyfriend at the end of a trial that has gripped the country.

The six were murdered between 2012 and 2018, most with the help of a hitman, so she could profit from life-insurance payouts.

The 46 year old was finally caught after someone she hired to kill her sister went to the police. She is due to be sentenced next month.

Ndlovu was also found guilty of the attempted murder of her mother, Maria Mushwana, as well as insurance fraud after having pocketed an estimated 1.4m rand ($95,000; £69,000).

Over the course of the three-month trial, the prosecution revealed how she had systematically arranged life and funeral insurance for her relatives and then had them killed.

The first person to be murdered was her cousin, Witness Madala Homu, in March 2012. Then her sister, boyfriend, niece and two nephews were all killed. Her last victim, Brilliant Mashego, died in January 2018.

In most cases she hired hitmen to carry out the murders, but in 2013 she poisoned and strangled her sister Audrey Somisa Ndlovu herself.

The series of murders ended after she approached someone to kill another sister and the sister's five children in March 2018. The man she hired informed the police who then arranged a sting operation to record her talking about the plans, the Times Live news site reports. Ndlovu was heard speaking about how she wanted the six to be burnt alive at home saying that she needed the money, Times Live says.

Throughout the trial, Ndlovu maintained her innocence, accusing many of the 50 state witnesses of lying. But the prosecution produced evidence to show how she had been with most of her victims before their deaths and how she had benefited afterwards.

"The accused was either the last person to see them alive or the first to notice that they were missing," state advocate Riana Williams was quoted by the AFP news agency as saying.

"She nominated herself as the beneficiary so as to cash in on life and funeral covers."

WHAT YOU NEED TO KNOW ABOUT INSURANCE FRAUD

BY IOL

The recent court case against former policewoman Rosemary Ndlovu has put insurance fraud under the spotlight. Ndlovu is accused of plotting the murder of relatives so that she could claim on several insurance policies. BrightRock's head of legal, Glenn Hickling, answers questions on insurance fraud and how it applies to consumers.

What is insurance fraud and what are some of the most common methods?

GH: Insurance fraud is a deliberate act of deceit – such as withholding material information or providing false information – to benefit unlawfully from an insurance policy. Insurance fraud can be committed against an insurance company or an agent of the insurance company. The perpetrators of fraud may include people applying for cover, policyholders, third-party claimants and beneficiaries, and service providers, as well as intermediaries or employees. Some of the most common forms of fraud are padding or inflating insurance claims, providing false information on an insurance application, or submitting false claims. Extreme cases of fraud may involve staging an accident, faking an injury or death, or syndicate schemes where professional fraudsters coordinate and execute complicated fraud strategies.

How prevalent is insurance fraud in SA?

GH: Unfortunately, fraud is quite prevalent and is on the rise. According to statistics released in August 2021 by the Association for Savings and Investment South Africa (Asisa), there was a 12% increase in fraudulent life insurance claims from 2019 to 2020. Last year 3 186 such claims, totalling R587.3 million, were recorded, compared with 2 837 claims (R537.1 million) in 2019. The highest incidence of long-term insurance fraud last year (2 282 claims) was in funeral policies. The Insurance Crime Bureau estimates that in 2019 up to 20% of the R35 billion paid out on short-term insurance claims could have been fraudulent. This means that in 2019 alone the South African short-term insurance industry lost almost R7 billion to fraud. South African life insurance companies are seeing a surge in fraudulent claims.

What makes people vulnerable to insurance fraud?

GH: Most insurance clients would never consider submitting a fraudulent insurance claim. However, industry statistics suggest that people are more likely to commit insurance fraud in times of economic hardship. As seen from the ASISA statistics above, over the past year, insurers have experienced a dramatic rise in fraudulent behaviour, indicating that the tough economic conditions have led more people to commit some form of insurance fraud. A recent example we've come across is the submission of fraudulent funeral policy claims where the death certificates have been falsified. We've also seen an increase in cases of non-disclosure, where we find that clients have misrepresented or held back information about their health or financial risks when applying for cover. In the case of funeral insurance, it is somewhat easier for fraudsters to try their luck, as these policies don't require any medical reports or blood tests to pay out and pay out far more quickly than a life insurance policy.

What measure can consumers take to prevent a fraudster from taking out insurance policies in their name?

GH: Identity theft is a common problem in South Africa, and internationally, cybercrime is on the rise, exacerbating the problem. It's therefore vital for people to protect their personal and financial information. This includes not sharing your ID number and other personal information with an unauthorised person, not clicking on suspicious links, and keeping your financial documents and information secure. If you suspect that you may have been the victim of identity theft, notify the authorities immediately. Should you discover that any insurance or other financial product has been taken out in your name without your consent, immediately notify the company in question. It's also a good idea to regularly check your bank statements and payslips. If you spot any debit orders or deductions, you're unfamiliar with, notify your bank or your company's HR department immediately and the financial service provider in question.

What measures have insurance companies put in place to prevent insurance fraud?

GH: Insurance companies have a wide range of fraud prevention and detection strategies in place and many of the large insurers have advanced forensics teams in-house to identify and investigate fraud. In recent years, digital technology has enabled insurers to become even more sophisticated in their fraud prevention strategies, using artificial intelligence and Big Data to pick up any inconsistencies, incomplete or inaccurate information or suspicious behaviour. Digital technologies can also be used to verify information, and insurers can cross-check details against industry databases, and social media. Many fraudsters believe that insurance fraud is a victimless crime, but the truth is that fraud is detrimental to all parties, including other policyholders, who may face increased premiums due to the impact of such financial crimes. Insurers will therefore act swiftly to decline a fraudulent claim, claim back any money paid out because of fraud or dishonesty and, institute criminal charges where this is justified, resulting in substantial fines and even a prison sentence.

Can a person commit insurance fraud without knowing they are doing it?

GH: Yes, a person can commit insurance fraud unwittingly. Many people believe that it's harmless to exaggerate their income to receive a higher insurance payout, leave out information about previous claims or their health status when applying for cover, or to add extra items on their long-term insurance theft claim. In the life insurance space, we often find that people leave out important information about their medical history or lie about their smoker status. While this may seem like a harmless white lie, it has a very real impact on the person's risk profile, the cover they can get and the premium they pay. The truth, therefore, is that this kind of dishonesty is fraud.

If a person commits insurance fraud, what are the consequences? Will they be blacklisted or possibly face jail time?

GH: If an insurer learns that a policyholder has committed fraud, their claims will be repudiated, they will become uninsurable, and they may even be criminally prosecuted.

What actions can consumers take to avoid committing insurance fraud?

GH: As with so many things in life, honesty is the best policy. This means being open and honest in your dealings with your insurance provider, answering their questions accurately and comprehensively when signing up for cover. If anything changes, make sure that you keep your insurance provider up to speed. An insurance contract is founded on mutual trust and disclosure. The insurance provider trusts that you will share all the information they need to be accurately able to assess and insure your risk, while you trust the provider to pay your valid claims if you have held up your end of the bargain. If you're not sure about the information you need to provide, it's best to ask your insurance provider or to speak to a trustworthy professional financial adviser.

Where can consumers report insurance fraud?

GH: If you become aware of fraud related to your insurance cover, there are several ways to report it. Many insurers have a forensic unit dedicated to investigating fraud, and you can report anything suspicious to them confidentially. If you prefer to report fraud anonymously, many insurers have independently operated whistle-blower hotlines, where you can safely report your suspicions. You can also report insurance fraud to the police, or to the Insurance Crime Bureau, a non-profit, voluntary organisation dedicated to fighting organised criminal activity and fraud in the insurance industry.

https://www.iol.co.za/personal-finance/insurance/what-you-need-to-know-about-insurance-fraud-977abf26-82bf-4fa7-90f8-365b550a0cc4

A COINBASE USER LOST R175 MILLION IN BITCOIN IN UNDER 10 MINUTES, IN A NOTIFICATION SCAM

BY KEVIN SHALVEY , BUSINESS INSIDER US

https://www.businessinsider.co.za/huobi-global-warrant-seeks-102-bitcoin-coinbase-theft-doj-2021-10

A US federal judge this month approved a warrant to claw back more than R10 million in bitcoin from a Huobi Global wallet, after federal investigators said it was part of a R175 million haul stolen from a Coinbase account.

In April, after a Coinbase user bought 200 bitcoin, a notification popped up, alerting them that their account had been locked, according to a complaint filed by the US Attorneys Office in Los Angeles. Although the notification appeared to be from Coinbase, it wasn't. Instead, the fake notification was the first step in an alleged fraud. In the moments that followed, almost $11.6 million in crypto, about 206 bitcoin, was removed from the user's account, US investigators said.

It is unclear how the alleged fraudster knew about the Coinbase transaction, and whether the online notification noted in the warrant appeared on a phone or computer. Coinbase declined to comment.

The Coinbase user, who was identified in court documents only as G.R., called a phone number on the notification, thinking it would connect to a Coinbase customer service rep, according to a federal complaint filed by investigators last month.

An "unidentified individual 1," or "UI-1," answered the call and asked G.R. to make a series of changes to the account, according to the complaint. Those changes included allowing remote access to the account, the complaint said.

"Once granted access to the Victim Account, UI-1 increased the daily transaction limit and also attempted to deactivate certain notifications and alert settings on the Victim Account," Dan G. Boyle, assistant US attorney, wrote in a document filed in US District Court in the Central District of California in September. Within moments, millions in bitcoin and XLM were removed from G.R.'s Coinbase account, investigators said.

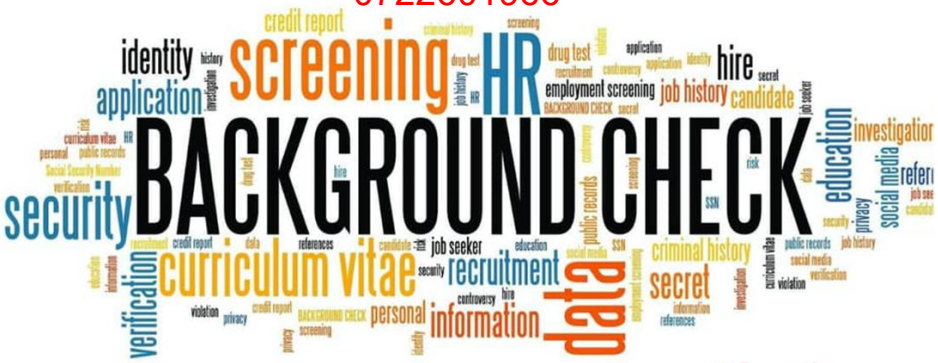
"The total value of virtual currency transferred out of the Victim Account between 2:02:40 PST and 2:12:41 PST on or about April 20, 2021, without G.R.'s authorization was approximately $11,570,138," they wrote in their complaint. The money was then moved by an unknown person through a series of transactions between several accounts. About 10.2 bitcoin ended up in an account with Huobi Global, one of the world's largest exchanges, according to investigators.

The investigators filed a forfeiture notification, seeking to reclaim those bitcoin. Huobi Global didn't respond to a request for additional information.

In early October, Judge Dolly M. Gee approved the warrant request, and a notice was posted, in case anyone other than G.R. wanted to claim ownership of the 10.2 bitcoin. "Huobi has agreed to maintain a freeze on the funds pending resolution of the forfeiture action," Thom Mrozek, director of media relations for the US Attorneys Office in Los Angeles, told Insider via email. "No one has been arrested or charged, but our investigation is ongoing."

FERLIO NOTIFICATION BOARD

Applying For Sace Or NCR Membership? Or Need Pre-Employment Checks Done For New Employees? Contact Ferlio Today On 0860 Ferlio (337546) Or Whatsapp Us On 0722601966



MOTIVATION FOR THE MONTH:

BIRTHDAYS

We here at Ferlio wish you have a wonderful birthday and a prosperous year ahead.

Lauren Whitfield – 15 November

Lucas Venter – 23 November

Lance Epstein – 24 November

Dominique Stapelberg – 29 November

Jaco Coetzee – 29 November

Diana Coler Barnett – 02 December

Willie Beckmann – 04 December

Ferlio

Group of Investigators

SPECIALIST SERVICES OFFERED:

Investigations, including but not limited to:
- Criminal
- Civil
- Forensic
- Cyber

Profiling
- Profiling / Lifestyle audit of individuals
- Business profiling
- Strategic audits on business
- Fingerprint screening
- Financial Audit Investigations
- Employee Background Screening
  - Identification documents
  - Driver's License & PDP
  - Criminal record
  - Educational background & qualifications
  - Prior employment records
  - Credit status
  - Integrity testing
  - Identification photos
  - Fingerprint verification

Undercover agents
- Standard level agents
- High level agents
  - Strategic level agents

Surveillance
- Physical
- Static
- Electronic
- Counter
- Covert escorting

Close Protection
- Executive protection
- Executive Support
- Asset in transit protection

Handwriting Specialist & Fingerprint Specialist

Polygraphs

Fraud Detection Initiatives

Security Risk Assessments

Transcripts / Translations

Pre-employment Psychometric Assessments

Truck & Driver Inspections

Security Vulnerability Assessment

GET IN TOUCH:

Phone: 0860 337 546 / 0860 (F-E-R-L-I-O)

Email: office@ferlio.co.za

Find us on Facebook: @FerlioGroupOfInvestigators

Ferlio Group of Investigators
@FerlioGroupOfInvestigators · Private Investigator

INVESTIGATOR OF THE MONTH:

Ensuring the Legality of the Digital Forensics Process in South Africa in Terms of the Cybercrimes Act – By Jason Jordaan (DFIRLABS)

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. 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. Over half of the cases investigated by the Federal Bureau of Investigation use some type of digital evidence. In the United States of America, digital evidence has become common in courts, and cases are frequently decided on digital evidence. While no similar definitive evidence exists in the South African environment, observations made by the author 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. 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 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 Cybercrimes 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 A COMPUTER SYSTEM OR COMPUTER DATA STORAGE MEDIUM

The Cybercrimes Act 19 of 2020 created several statutory criminal offences aimed at addressing cybercrime in South Africa.

Section 2(2)(a) creates the criminal offence of unlawful access to a computer system of computer data storage medium.

This offence has three essential elements:

- Access
- Computer system or computer storage medium
- Without authority or permission

3. ACCESS

The Cybercrimes Act 19 of 2020 defines access in Section 2(2)(b) as:

- Using data or a computer program stored on a computer data storage medium
- Stores data or a computer program on a computer data storage medium
- Using data or a computer program held in a computer system
- Stores data or a computer program on a computer data storage medium forming part of the computer system

- Instructs, communicates with, or otherwise uses, the computer system

If a person performs any of these actions, then they have fulfilled the element of access in this offence. In essence if you interact with any data, or program

4. COMPUTER SYSTEM OR COMPUTER STORAGE MEDIUM

Section 1 of the Cybercrimes Act 19 of 2020 defines a computer system as one computer; or two or more inter-connected or related computers, which allow these inter-connected or related computers to exchange data or any other function with each other; or exchange data or any other function with another computer or a computer system. It defines a computer data storage medium as any device from which data or a computer program is capable of being reproduced or on which data or a computer program is capable of being stored, by a computer system, irrespective of whether the device is physically attached to or connected with a computer system.

A computer is defined in Section 1 of the Act as any electronic programmable device used, whether by itself or as part of a computer system or any other device or equipment, or any part thereof, to perform predetermined arithmetic, logical, routing, processing, or storage operations in accordance with set instructions and includes any data, computer program or computer data storage medium that are related to, connected with, or used with such a device. A computer program is defined as data representing instructions or statements that, when executed in a computer system, causes the computer system to perform a function.

Data is defined in Section 1 of the Act as electronic representations of information in any form, but information is not defined. According to the Concise Oxford English Dictionary, the term information means "what is conveyed or represented by a particular sequence of symbols". 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.

These definitions are broad enough to essentially cover any data or any device that has data processing or storage capacity. So, whether it is a mobile phone, a laptop, a server, a drone or even a car's engine management system, if you perform any of the actions, in the previous section in relation to anything that falls within the definitions in this section, then you have satisfied this element of the offence.

5. UNLAWFULLY

The Cybercrimes Act 19 of 2020 does not define unlawfully. The general interpretation of the concept thus needs to apply. In other words, something is unlawful if it goes against the law. Section 14 of the South African Constitution gives everyone the right to privacy which includes the right not to have their property searched or their possessions seized, or the privacy of their communications infringed. In other words, if anyone accesses a person's data or their devices, without the consent of the owner, then their actions would be unlawful, and would thus satisfy this element of the offence.

6. THE DIGITAL FORENSICS PROCESS

Digital forensics involves the preservation, identification, extraction, and documentation of digital evidence stored as data or magnetically encoded information. 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. The objective of digital forensics is in essence quite simple, and that is to recover, analyse, and present digital evidence in such a way that it is usable as evidence in a court of law.

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. 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. 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. 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.

7. DIGITAL EVIDENCE

Evidence can be defined as anything that tends to logically prove or disprove a fact at issue in a judicial case. Digital evidence is defined as information of a legal probative value that is either stored, or transmitted in a digital form. 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.

Digital evidence is fundamentally no more than data as defined in Section 1 of the Act.

8. 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:

- 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.
- Analyse the evidence without altering it.

Another model of the digital forensic process includes the following stages:

- 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.

9. 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 must 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.

10. DIGITAL FORENSICS AND THE CONTRAVENTION OF SECTION 2(2)(A) OF THE CYBERCRIMES ACT

The fundamental offense defined by Section 2(2)(a) of the Cybercrime Act, is when anyone accesses any computer system or computer data storage medium, and any of the data thereon.

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 2(2)(a) and could potentially be prosecuted and convicted.

11. 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.

12. THE ADMISSIBILITY OF DIGITAL EVIDENCE OBTAINED IN CONTRAVENTION OF SECTION 2(2)(A) OF THE CYBERCRIMES ACT

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

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. Section 35(3) must be read with Section 35(3) of the Constitution which guarantees the right to a fair trial.

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. 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.

Essentially this means that if the digital evidence has been obtained in contravention of Section 2(2)(a) of the Cybercrimes Act, 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 2(2)(a) of the Cybercrimes Act, and thus there is a necessity to have the appropriate legal authority to conduct digital forensics.

13. 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 2(2)(a) of the Cybercrimes Act. Not only is there a risk of criminal prosecution, which carries the possibility of a fine or imprisonment, but the digital forensic practitioner could potentially be subject to civil litigation for delict.

14. 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

15. 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.

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

16. 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 an 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.

17. 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.

18. CONCLUSION

The digital forensic process, unless performed on data that has been obtained with the appropriate legal authorization, satisfies all the element necessary for a contravention of Section 2(2)(a) of the Cybercrimes Act.

This could result in digital evidence obtained because 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.