Digital forensics
Offering more possibilities to convict criminals

By Annalise Kempen
Information provided by Brig Piet Pieterse and Capt Reinette Coetzee, DPCI

The global agency called We are social has revealed, in its Digital in 2016 report, that there were 3.79 billion unique cellphone users; 3.419 billion Internet users; 2.307 billion active social media users and 1.968 billion active mobile social media users in the world by January 2016. According to the report, 82% of Africa’s population, or 986 million people, have mobile connections. The report states that South Africa had 85.53 million connections; 28.84 million active Internet users; 13 million active social media users; and ten million active mobile social media users by January 2016 (Kemp, 2016).

Irrespective of the type of evidence seized, whether it’s a knife or a cellphone or surveillance footage, the provisions of section 19 to 36 of the Criminal Procedure Act which relate to search warrants, entering of premises, seizure, forfeiture and disposal of property connected with offences, must always be taken into consideration.

Digital evidence
Apart from having knowledge of which items are regarded as digital devices, such devices should also be specified whenever the investigating officer applies for a search warrant (see below*). The term “digital device” refers to an electronic device that can receive, store, process or send digital information. This definition includes, but is not limited to, the following categories of devices:

- **Computers**
  - This category includes personal computers (PCs), laptops, notebooks, hard drives (internal and external), CDs, DVDs, stiflies, memory sticks, servers etc.

- **Mobile devices**
  - This category includes cellphones (smart phones/feature phones), tablets, phablets (a smartphone having a screen which is intermediate in size between that of a typical smartphone and a tablet computer (https://en.oxforddictionaries.com/definition/phablet)), SIM cards, SD cards, memory sticks, USB devices, GPS devices, cameras, video cameras, etc.

- **Skimming**
  - This category includes handheld card readers, point of sale devices, hi-tech skimming devices and other devices that can be used to skim a bank card.

- **CCTV**
  - This category includes DVR devices (including all the cables), as well as recordings from a DVR or CCTV system.

* Imagine a life without a cellphone or computer... not having the ability to speak to your loved ones or send them a message via SMS or WhatsApp ... imagine the impact on your professional life. Imagine that you have to do everything by hand, from writing letters to drafting documents and reports and typing these with a typewriter.
Police members should never play around on digital devices to determine what type of data is stored on the suspect's cellphone or computer. Apart from confirming a passcode, the digital device should be handled in the manner described in the article. "Playing around" on the device will change that data and therefore compromise the integrity of the evidence. It's similar to tampering with evidence such as moving a firearm at a murder scene.

Seizing evidence*

Brig Piet Pieterson, the section head of the Electronic Crime Unit, reminds us that all types of evidence should always be seized according to the provisions of the Criminal Procedure Act 51 of 1977, while also taking into account the legal provisions of other statutes. During an interview with Brig Pieterson and Capt Reinette Coetzee, the acting commander of Digital Forensic Investigations, they reiterated that all activities, procedures and processes must be done within the ambit of the law to ensure the success of the court process. When it comes to the handling of evidence, the chain of custody can seem initially more important than the evidence itself, and they reminded us that if this is flawed, the evidence can be dismissed and be rendered inadmissible in a court of law.

Capt Coetzee made it clear that investigating officers should ensure that search warrants contain detailed descriptions of the specific evidence that should be seized (see supra for a discussion of the different types of digital evidence*). All search warrants dealing with digital evidence should also include/mention all relevant data contained on these devices. If "data" is not included on the original search warrant, a separate search warrant would have to be applied for.

It is important that the person executing the seizure of the exhibits knows why s/he is seizing the exhibit and what s/he wants to obtain as evidence from such a device. It is unlawful to seize anything outside the scope of the search warrant and/or the reason for the search - in other words, if there are no reasonable grounds for the seizure of exhibits, members should refrain from doing so.

Steps to follow on the crime scene

Capt Coetzee says that although it is very important for investigating officers to seize digital equipment according to the search warrant, it is equally important to know the correct procedure when handling evidence to maintain its integrity and ensure that data is not lost in the process. She gave us the following tips:

What to do when seizing a cellphone?

- Ask the suspect for the passcode to unlock his/her cellphone and SIM card and write such passcode down on a piece of paper.
Test the code immediately to confirm whether the correct passcode has been supplied.
Switch the cellphone to "airplane mode" before switching off the phone.
Remove the SIM card from the phone (a handy tip is to always carry a small paperclip, which can be used to open the slot to remove the SIM/SD card).
Place the SIM card as well as the piece of paper with the passcode on it in a forensic evidence bag, together with the cellphone.
Handle every piece of digital equipment as a separate piece of evidence: each cellphone should be placed in its own forensic bag, along with its SIM card and the piece of paper on which the passcode/s is written.

Remember that the cellphone needs to be switched off, as the data on the phone changes when the phone moves from one cellphone tower to the next.

What to do when seizing a computer?
- If a computer or laptop is switched off, do not switch it on. Pack, seal and transport it to the SAPS 13 store.
- It is preferable to also bring along the cables, especially when seizing Apple Mac products.
- If a computer server is detected at a crime scene, the assigned DFI commander or member on standby must be contacted in order to do the acquisition on site, as servers are normally found at business premises.
- If the computer (or similar device) is switched on, it is vital to remember that no member must work on or touch the computer without first speaking to digital forensic investigators who have been trained and who have received international certification in dealing with such evidence. In such a case, the scene should be sealed-off and the police member must act on the instruction of the members of the DFI.

The integrity of the evidence must be preserved at all times and it is therefore vital that the police member at the scene knows exactly which steps to take when dealing with any form of computer. For example, if the computer is still running, there may be encryption software, eg BitLocker, running in the background. This may result in some information being lost if the correct procedure is not followed before the computer is shut down.

As is the case when dealing with cellphones, the police member should ask the suspect/computer operator to provide the necessary passwords and whether any encryption software is running on the system. Again, such passwords should be written down and handled as evidence.

The investigating officer or his/her authorised member must complete a mobile device seizure form for every device that is being seized, and this form must accompany the exhibits.

All seized evidence must be booked into the SAPS 13 exhibit store of the station in which policing area the search was conducted. After the exhibits have been booked out of the SAPS13 exhibit store, they must be taken to the assigned DFI for backup/extraction of the information.

The process
DPCI investigating officers who act as first responders at crime scenes where digital forensic input is required need to activate the DFI to react. The investigating officer has to initiate a formal request, either written or verbal, and follow it up with a written request to the DFI commander giving a summary of the case at hand and attaching a copy of the search warrant.

The digital forensic investigator must then liaise with the investigating officer to ensure that the required resources and personnel are allocated. Again, it should be emphasised that only those digital devices specified on the search warrant must be seized and that the investigating officer must know why s/he is seizing the exhibit and what s/he wants to obtain as evidence from each device.

Once the seizure is completed, as has been discussed supra, and the digital evidence has been delivered to Digital
Forensic investigations, a request for extraction/acquisition/analysis must be completed and must accompany the digital evidence for every case.

It is vital that the investigating officer provides the assigned digital forensic investigator with detailed descriptions of the type of evidence that is required. For example, it must be specified that all data (text and graphic images) relating to terrorism, e.g. the chemistry needed to manufacture a bomb or the plans of specific buildings, must be extracted from a specific digital device.

To summarise: when an investigator requests the assistance of DFI and has handed over the seized digital evidence; the process requires the investigator to complete a request form explaining what specific data needs to be extracted from a device. The latter step is vital, especially when the digital forensic investigator will later have to give evidence relating to exactly what they had to investigate and stating that this was specified. Such investigator should then provide evidence relating to the scientific processes that were followed and according to which they give evidence in court.

Capt Coetzee told us that the communication between the investigating officer and the digital forensic investigator is vital during the analysis period to ensure that all the related digital evidence is extracted as specified within the ambit of the search warrant. She also confirmed the importance of regular liaison with the State prosecutor during the process.

After the investigation process and analysis have been completed, the DFI supplies the investigating officer with a CPA section 212(4)(a)(iii) statement, together with the media/devices on which the findings of the specific investigation are captured. This will be supplied as two identical files; the first sealed for "court purposes" and the other to be utilised during the investigation process.

**The future**

It is envisaged that a standard operational procedure (SOP) will be finalised in due course within the SAPS through the National Cybersecurity Policy Framework (NCPF), which will ensure a holistic approach in dealing with all digital evidence.

---

Technological advances might make life easier for many of us, by enabling us to communicate instantaneously with whomever we want to. But this same technology can also be an individual’s downfall—especially when it is used to plan or perpetrate a crime.

The variety of digital evidence that exists represents a key component of police investigations and a potential source of evidence that could prove critical in supporting the prosecution of different types of crimes. The key is to ensure that digital evidence is seized in a legally correct manner; that it is not tampered with and that those responsible for the extraction and analysis of data have clear instructions as to what is needed, to strengthen the case.

**Who to contact when dealing with digital evidence?**

Within the DPCI structure, contact the standby officer at your local DPCI (Hawks) Office; alternatively, contact Capt. Reinetje Coetzee, the acting commander of Digital Forensic Investigations in the Hawks, at cell: 079 886 6829 or send an e-mail to: coetzee1r@saps.gov.za. Alternatively, contact Brig. Piet Pieterson, the section head of the Electronic Crime Unit, at cell: 082 463 7227 or send an e-mail to: ecu@saps.gov.za. You can also contact the assigned digital forensic investigators at Detective Services or Crime Intelligence.

**List of references**

https://en.oxforddictionaries.com/definition/phablet

**Boiler rooms**

Identity theft is nothing new, yet many people handle their personal information and documentation as if it has no value. This happens despite the fact that it is estimated that 48% of all fraud involves record and account take-over fraud, which has skyrocketed by as much as 300% in only five years (confirming why it has become a priority offence).

Apart from requiring the victim’s personal information, those perpetrating the fraud need computers to perpetrate the crime. Fraudulent documentation, such as fake identity documents and payslips, are created in so-called boiler rooms. Police members who receive tip-offs relating to such boiler rooms need to deal with the digital evidence involved according to the tips provided in this article.
In our technologically mad world, criminals do not hesitate to use digital devices in the execution of their crimes. Criminals use cellphones to speak to their accomplices to plan a crime, while computers are used in many cases to commit fraud, to create and distribute child pornography or to carry out cybercrimes. However, law enforcement officers can use these devices in the investigation of crimes, to ensure that perpetrators are prosecuted for breaking the law. But who is responsible for the forensic analysis of these digital devices? SERVAMUS spoke to some of the digital examiners at the Technological Investigation Support Centre (TISC) at Detective Services Head Office in Pretoria to learn more about the challenges they face while doing their job.

Experts who are able to collect, restore and analyse digital evidence are very important to investigating officers. The SAPS has 12 coordinating offices which are permitted to deal with section 205 applications. These are the nine Provincial Office Communication, Interception and Monitoring Offices (also known as technical support units); Technical Support Services at Crime Intelligence Head Office; the Specialised Priority Crime Investigations at DPCI; and TISC Detective Services Head Office. These 12 offices have digital forensic examiners who are responsible for the analysis of digital devices itself and the data found on cellphones, computers, CCTV footage, tablets, SD cards, X-Boxes and GPS devices.

SERVAMUS spoke to Col Micheal Sales, Head of TISC at Detective Services Head Offices, and Lt-Col Francois Möller about their unit and the work they are doing. TISC at Detective Services Head Office reports directly to Maj-Gen Magson of Commercial Crimes, Detective Services. Col Sales and 13 other SAPS employees are responsible for a variety of functions at this section (see below). Although each of the members specialises in a specific field, for example digital examination or data analysis, their collective field of knowledge in terms of digital expertise is wide. They render a service to detectives and investigating officers from all over the country, except for members attached to Crime Intelligence and the DPCI (the Hawks [see related article from p 22]). A large part of their work is doing digital analysis for the Family Violence, Child Protection and Sexual Offences (FCS) Units.

The job of digital forensic examiners
Digital forensic examiners assist in the investigation of all sorts of crime where digital evidence is available. For example, they can assist in placing a suspect on a crime scene by analysing cellphone records and CCTV footage as well as by downloading and analysing data from computers, such as in child pornography and fraud cases.

CCTV analysis forms part of TISC’s responsibilities. They either attend crime scenes personally in order to download and extract CCTV footage, or they receive CCTV footage from investigating officers on compact discs or memory sticks. CCTV footage is analysed to compile frame break downs, where after a photo album is compiled and printed. In 2016, this office was involved in 282 cases in which such CCTV analysis was done.

Digital forensic investigations are done to extract digital evidence which can be used in court. This evidence is extracted from devices such as computers, hard drives, memory sticks, cellphones and tablets, which are received from
investigating officers in sealed forensic evidence bags. Col. Sales emphasised that maintaining the integrity of the chain of evidence from seizure to analysis is very important, including when dealing with digital evidence. The TISC also assists investigating officers with search and seizure activities at crime scenes, and they consult with investigating officers to ascertain the scope of investigation. Due to the vast number of child pornography cases that are investigated by FCS Units, especially the Serial and Electronic FCS Investigation Unit in Gauteng under the command of Lt-Col Heila Niemand, as well as enormous numbers of digital images on these devices, the TISC prefers that the investigating officers search and mark the data themselves, leaving the digital forensic examiner with only the analysis of that specific data to compile a report for further investigation and court purposes.

During the investigation process, the digital forensic examiner makes a mirror image of the memory device, which is an exact copy of a computer's physical memory. They recover deleted data, index all the data and analyse the relevant data by using various data analysis software packages. Once the necessary evidence has been obtained from the data, a comprehensive report of the required evidence (a section 213 statement) is compiled, and the digital examiner from TISC also attends court to present expert evidence. In 2016, the TISC handled 214 pieces of evidence in 28 cases.

With regard to mobile devices (cellphones), the information saved on the mobile device must be downloaded and this includes the logical and physical extraction of evidence. The data is analysed and interpreted in order to answer to the requested scope of investigation, within the ambit of the search warrant. Again, as in the case of memory devices, a report is compiled and expert evidence is presented in court. During 2016, the TISC handled 317 cases in which 606 devices were analysed.

Digital devices include the following:
- CCTV;
- computers
- cellphones;
- SD cards;
- tablets;
- GPS;
- XBox

Evidence from scene collected in forensic bag

Investigating officer crime scene management

To TISC
- Book in SAPS 13
- Assigned to digital examiner

Crime scene

 Downloads
Still photos
Photo albums

CCTV

Cellular phone

Computers

CD / DVD
Section 213 statement

TISC

IMAGE ANALYSE REPORT

ANALYSIS
section 205

Downloads

Court 1

Functions at TISC

Coordination of section 205 applications; cell-site analysis; imaging of computers; download of CCTV; extraction of data from cellphones analysis (timestamps / communication); social media investigations; and section 213 statement court-related investigations
As part of their investigations, the TISC also reacts to requests from investigating officers to assist with online investigations on social media platforms such as Facebook, Twitter and Instagram. In such cases, they liaise with foreign law enforcement agencies and various international Internet service providers. They also monitor the deep web for indications of possible local criminal activities.

Data analysis is done to provide both investigating officers and the court with a visualised summary of large volumes of data. This is done after a request has been received from an investigating officer. Col Sales stresses that all data used for analysis must have been obtained legally - in other words, within the ambit of the search warrant - in order to be admissible in court. The digital examiner should consult regularly with investigating officers and prosecutors to ensure proper planning, to determine the scope of the investigation and provide feedback. If the need arises, the digital forensic examiner might visit the crime scene, but Col Sales noted that, in the majority of cases, they do not go to the crime scene. Again, after analysing the data, a comprehensive statement and analysis report (a section 213 statement) is compiled, which the digital examiner can present as a subject matter expert in court.

Communication analysis is done to establish links of communication between different cellphone numbers/people by using association analysis. It further establishes sequences of events or time lines.

Cell site analysis establishes the communication and possible movement of a cell number/person by plotting the cellphone towers used during communication, as it also indicates the area in which the phone was operating. The digital forensic examiner maps the information and compiles a comprehensive statement and mapping reports.

Before any cellphone investigation can be done, a section 205 application must be filed. The two section 205 coordinators at TISC Detective Services Head Office are responsible for mobile handset profiling, which aims to establish whether a handset has been used after it was stolen from a crime scene. Col Sales explains that every cellphone has a unique 15 digit IMEI number and that a handset profile can be done on this IMEI number, whereafter a section 205 application can be done on the new number. These coordinators are also responsible for the administration of section 205 applications received from investigating officers, and for capturing these section 205 requests on service provider systems. As mentioned in the related article about cellphone evidence (see p 16), the required data is made available in a short period of time. During 2016, this office handled 3225 section 205 applications as well as 11 865 handset profiles.

Expert witnesses

When physical evidence is used in cases, testimony by subject matter experts relates the facts to the evidence. In a case where a cellphone signal is mapped, it is important that an expert testifies about it. The expert will give testimony about the processing of the data that appears on the cellphone statement and which therefore represents the activities on the cellphone record. Col Sales explained that digital forensic examiners do not compile a section 212 statement since there are a lot of prerequisites attached to such statement. Such a statement is usually provided by an expert with a qualification in a specific field; for example, a pathologist provides a section 212 statement to court. A section 213 statement is provided to a court by experts with other qualifications (certificates, skills, and/or applicable experience), such as a digital forensic examiner.

Technology

Digital examiners use a variety of technological aids to extract data from cellphones, download data from computers and analyse the extracted/downloaded data. According to Col Sales, the TISC has more specialised equipment than the Provincial Office Communication, Interception and Monitoring Offices.

Regular training

Technology and the use of technology are growing at an increasingly rapid rate. In today's high-tech world, industries are either leading the way or playing catch up. This is no less true for law enforcement officers who specialise in digital forensic examination. It is therefore important that they regularly attend local and international training courses and seminars to stay abreast of the latest developments and one step ahead of criminals.

Court assistance

TISC is also involved with court assistance and setting up digital equipment at court; for example, in the Oscar Pistorius case, this was done to enable those who gave evidence to use technology.

* * *

Col Sales is very proud of his team and says that they are willing to walk the extra mile to get information and to help investigating officers from all over the country. He used the example of the Oscar Pistorius case in which the digital examiners went to the USA to get help to access the suspect's phone. Another example was the case in which the American marketing consultant, Gabriela Kabrins Alban, was murdered in Camps Bay during July 2015. Her tablet was destroyed, but the digital forensic examiner involved called in the help of experts in Israel, enabling them to download a large amount of data. This case is still sub judice.

Col Sales described their office as a one-stop service for investigating officers as they do the digital forensic investigation and analysis and then provide the investigating officer with a final product which is ready to present to court.