AN EXPLORATION OF THE INVESTIGATIVE VALUE OF CELL PHONE RECORD ANALYSIS IN THE INVESTIGATION OF SERIOUS AND VIOLENT CRIMES IN THE WINELANDS DISTRICT, WESTERN CAPE PROVINCE

by

DONAVIN ADAM VAN ROOYEN

Student Number: 4290-375-0

Submitted in partial fulfilment of the requirements for the degree of

MASTER OF ARTS IN CRIMINAL JUSTICE

in the subject

FORENSIC INVESTIGATION

at the

UNIVERSITY OF SOUTH AFRICA

SUPERVISOR: PROF J.S. HORNE
CO-SUPERVISOR: DR P. MACHETHE

DATE: JULY 2022

DECLARATION

I, Donavin Adam Van Rooyen, with student number: 42903750, hereby declare that this dissertation titled "An exploration of the investigative value of cell phone record analysis in the investigation of serious and violent crimes in the Winelands District, Western Cape Province" is submitted in accordance with the requirements for the degree of Master of Arts in Criminal Justice in the subject, Forensic Investigation at the University of South Africa (UNISA).

I declare that the above dissertation is my own work and that all the sources that I have used or quoted have been indicated and acknowledged by means of complete references.

I further declare that I submitted the dissertation to originality checking software and that it falls within the accepted requirements for originality.

I further declare that I have not previously submitted this work, or part of it, for examination at Unisa for another qualification or at any other higher education institution.

07 JULY 2022

SIGNATURE DATE

DEDICATION

This research is dedicated to my wife Jacky and the boys, Jordan and Caleb. They have been my support structure throughout the course of this dissertation. Caleb mentioned that his teacher asked a fellow student what his father's profession is. In turn, my wife asked what his response would be if asked about his father, to which he replied: "My father is doing assignments". Jacky and the boys have always understood the importance of this dissertation to me, and that every weekend "daddy is doing assignments". Also to my loving mother Johanna, who has been my 'number one fan' from day one. Without their support and love, this journey would have been difficult, and my race would have been tremendously tiring. They made everything easier for me.

ACKNOWLEDGEMENTS

First and foremost, I give honour and praise to the Almighty Heavenly Father who has blessed me since 2013 with the wisdom, courage, strength and peace of mind to finally complete this research study. The journey had its challenges, but I knew was always going to be worthwhile in the end.

This research would have been impossible without the support of a number of people, including those mentioned below. I sincerely express my appreciation of their respective roles, and acknowledge their continued support and inspiration.

- Special thanks and gratitude to my supervisor Professor Juanida Horne for her role as guardian angel and mother throughout my studies. Thank you for your patience and always being a phone call away. Your invaluable advice, support, guidance and lengthy conversations have finally yielded the most appreciated outcome.
- Dr Petrus Machete my co-supervisor, thank you for your invaluable support and guidance. I was blessed with a great supervising team. God bless you both.
- My wife Jacky, thank you for always taking care of the family responsibilities whenever I needed to focus on my studies. I will continue to cherish your never-ending and tremendous love and support forever.
- Endless thanks to my wonderful children, Jordan and Caleb for the many hours of their precious family time they sacrificed in order to grant me the opportunity to focus on this research project. Jordan, thank you for always taking care of the "coffee duties".
- Thank you to my friend and colleague, Sergeant Marlon Juan Appollis who encouraged me to pursue the topic under investigation. Thank you for the advice, lengthy conversations, and debates that sharpened my mind.
- Thank you to my friends, Xavier Jephthah and Rushanda Erentzen for the encouragement and many productive talks we always had.
- Thank you to the University of South Africa (UNISA) for the funding which enabled me to defray the costs associated with this research study. The assistance is unconditionally appreciated.

- Special thanks to the wonderful SAPS family, the NPA Prosecutors, and all other participants for granting me interviews willingly and without any hesitation. Your respective contributions and inputs are invaluable and highly appreciated.
- My editor Dr Themba J. Mkhonto, thank you for your invaluable editorial contribution to the draft and final research documents.
- Thank you to my wife and Wesley Arendse for assisting with the transcription of the interviews.

ABSTRACT

In modern times, cell phones have influenced people's everyday lives and changed the ways they interact with each other and one another. The continuous development and advancement of cell phone technology has also sophisticated the way in which cell phones are used. For many people, cell phones have replaced many functions previously performed on laptops and computers, such as storing important information, conversations, keeping of schedules; as well as saving and transferring files, and internet surfing. Accordingly, the usage of cell phones has become an important part of people's everyday life, and has changed people's ways of interacting with one another. However, the popularity of mobile devices has been overshadowed by their frequent usage in digital crimes, which also necessitated the application of digital forensics in crime investigation. It could then be postulated that cell phones have played a significant part in the commission of many crimes and the subsequent investigation thereof. In that regard, cell phone investigation could be viewed as the future of criminal investigations and analysis. This research, therefore, explores the investigative value of cell phone record analysis in the investigation of serious and violent crimes in the Winelands District, Western Cape Province.

KEY TERMS

Cell data, cell phone records, crime mapping, criminal investigation, digital evidence, expert evidence, geographic information systems, International Mobile Equipment Identity, serious and violent crime, Subscriber Identity Module.

TABLE OF CONTENTS

LIST OF FIGURES

LIST OF TABLES

ABBREVIATIONS/ACRONYMS

ADN	Abbreviated Dialling Number
AGU	Anti-Gang Unit
AI	Artificial Intelligence
AMA	Automatic Message Accounting
BST	Base Transceiver Stations
CHV1 and CHV2	Card Holder Verification
CCA	Cybercrimes Act 19 of 2020
CDR	Call Detail Records
C1	Cell Phone One
C2	Cell Phone Two
CONSTITUTION	Constitution of the Republic of South Africa Act 108 of 1996
CPA	Criminal Procedure Act 51 of 1977
CSI	Crime Scene Investigation
CSV	Comma-Separated Values
CLAW	College of Law
DPCI	Directorate for Priority Crime Investigation
DPP	Director of Public Prosecutions
ECTA	Electronic Communications and Transmissions Act 25 of 2002
4IR	Fourth Industrial Revolution
FDN	Fixed Dialled Number
FSL	Forensic Science Laboratory
GIS	Geographic Information System
GPS	Global Positioning System
GPRS	General Packet Radio System
HLR	Home Location Register
ICCID	International Circuit Card Identifier
ICC	Integrated Circuit Card
ICT	Information and Communication Technologies
IMEI	International Mobile Equipment Identity
IMSI	International Mobile Subscriber Identity
LA	Movement from the Current Location
LAI	Local Area Identity or Location Area Information

LCRC	Local Criminal Record Centre
LDN	Last Dialled Number
LP	Language Preference
MEC	Member of Executive Council
MCC	Mobile Country Code
MLA	Mutual Legal Assistance
MMS	Multimedia Messaging Service
MNC	Mobile Network code
MSC	Mobile Switching Centre
MS	Mobile stations
MSIN	Mobile Subscriber Identification Number
MSISDN	Mobile Station International Subscriber Directory Number
NDPP	National Director of Public Prosecutions
NCIS	Naval Crime Scene Investigation
NPA	National Prosecuting Authority
OB	Occurrence Book
OL	Operation Lockdown
PDA	Personal Digital Assistant
PDF	Portable Document Format
PIN	Personal Identification Number
PUK	Personal Unblocking Code
RAI	Routing Area Identifier
RICA	Regulation of Interception of Communications and Provision of Communication-related Information Act 25 2002
RSA	Republic of South Africa
SANDF	South African National Defence Force
SAPS	South African Police Service
SIM	Subscriber Identification Module
SMS	Short Message Services
SOP	Standard Operating Procedures
SVC	Serious and Violent Crime
TMSI	Temporary Mobile Subscriber Identity
TSU	Technical Support Unit
UICC	Universal Integrated Circuit Card

UNODC	United Nations Office on Drugs and Crime
UNISA	University of South Africa
UREC	University of South Africa's Research Ethics Committee
VLR	Visitor Location Register
War Room	Operational Command Centre
WCP	Western Cape Province

CHAPTER 1: GENERAL ORIENTATION

1.1 INTRODUCTION

In terms of the Constitution of the Republic of South Africa (Act No. 108 of 1996), the South African Police Service (SAPS) is mandated to prevent and combat crime, maintain public order, protect citizens and secure their property; and to enforce and uphold the law (South Africa, 1996:1). The Constitution of the Republic of South Africa (Act No. 108 of 1996), is (hereinafter referred as Constitution (Act No. 108 of 1996). Accruing from this mandate, the SAPS is then obliged to develop new and scientifically proven strategies, techniques, and practices to fulfil its constitutional mandate. Such an obligation is non-negotiable, considering that criminality renders communities to live in perpetual fear (Roelofse & Gumbi, 2018:322). Western Cape communities live in fear, especially the vulnerable groups such as women and children despite that there are five (5) Police stations among the 10 Police stations with the highest incidence of crime in the country. Moreover, the Western Cape Province (WCP) contributes immensely to the crime statistics nationally, especially serious and violent crime (Detective Service News Bulletin, 2020:8).

The Western Cape Province (hereinafter referred as WCP) is the highest contributor of murder cases in South Africa, which necessitates major intervention strategies to thwart these growing murder trends. Accordingly, General Bheki Cele, current Minister of Police was compelled by the prevailing situation to put concomitant measures in place in order to curb the high number of murder cases and the rise of other serious and violent crimes in the WCP. These measures included General Bheki Cele' introduction of "Operation Thunder" and the Anti-Gang Unit (AGU) to address the disconcerting scourge of murders and other related serious offences in this province. Imbued with the patriotic duty to prevent criminals from threatening the authority of the State, the Minister also initiated "Operation Lockdown", a combined intervention between the SAPS and the South African National Defence Force (SANDF). The fundamental purpose of this operation was to restore the rule of law and order and also enforcing the Covid-19 risk-adjusted restrictions applicable to the country as a whole from time to time (Ministry of Police, 2019:3).

The researcher conducted this investigative study in the Winelands District of the WCP, and has a population of 950 578 with 236 006 households (Western Cape Government, 2019:1). The province itself has an estimated population of 6 844 272. The WCP comprises of six (6) municipalities: the City of Cape Town, the Cape Winelands, Overberg, Central Karoo, the Garden Route, and West Coast. These are shown in the map in Figure 1.1 below.

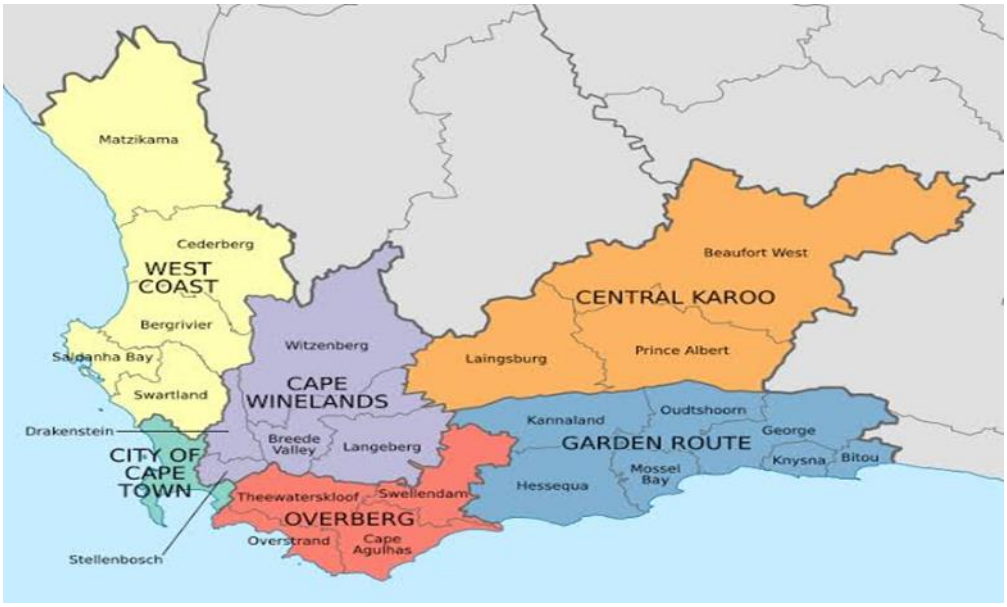

Figure 1.1: Provincial demarcation
(Source: WeatherSA Portal, 2020)

According to Ferraro (2015:1), the field of criminal investigation consists of an extensive variety of expertise whose fundamental intention is to determine the sequence of events leading to the occurrence of a crime. Furthermore, criminal investigation entails a coherent and intellectual collection of information for establishing facts relevant to solving an incident. In addition, criminal investigation is concerned with determining the methods used in the commission of a crime; as well as the establishment of an evidence-based, fact-finding approach to prove the innocence or guilt of the alleged perpetrator or suspect in a criminal event (Gehl & Plecas, 2016:4). According to Higginson, Eggins and Mazerolle (2017b:2), criminal investigation is an extensive element of Police work aimed at addressing serious violent crimes. However, these authors lament that the Police generally lack the required skills and techniques attendant to serious and violent crime investigation trends similar to the production levels observed in other policing fields in addressing

general crime. From the researcher's viewpoint, in many reported cases in which the assailant was specified as unknown, turned out that the assailant's activities were in fact, known. However, the need for personal identification still exists, despite that it is sometimes difficult to prove the link between, and among perpetrators and the crime or incident. Some of the perpetrators manage to evade detection due to insufficient evidence on the crime scene. The role of the Police's investigative methods is vital in investigations of serious violent crime, identifying and arresting the offender, and processing of a confession (Higginson et al., 2017b:1). These methods could have an effect on suspects' acquittal or conviction. The Police may use different investigative tools to accomplish this goal, including crime mapping, which is the systematic utilisation of geographical information systems (GIS) to analyse spatial crime data and other crime related incidents (Santos, 2017:8).

In recent years, cell phone usage has proliferated the Police's methods of investigating crimes, which also reflects most people's conventional form of communication around the world by texting messages and making calls (Alshammari & Alghathbar, 2017:1). Continuous cell phone technology developments have changed and sophisticated the way the cell phone is used. For example, people tend to keep schedules, conversations, and important information on their cell phones. In this regard, cell phone technology has replaced many functions normally performed on laptops and personal computers, such as saving and transferring files and internet surfing. Accordingly, cell phone usage has become an important part of everyday life, and has changed people's ways of interacting with one another. Regrettably, the popularity of mobile devices has been overshadowed by their frequent usage in digital crimes, which also necessitated the digital forensics aspect in crime investigation (Sai, Prasad & Dekka, 2015:4847).

Digital forensics and digital data gathering are a relatively new science (Alshammari & Alghathbar, 2017:1). This novelty has exposed the dire need in digital forensic skills, artificial intelligence and extensive knowledge of computer file systems and their associated file formats to enable the investigators' understanding of digital crime content. Given such scenarios, it is then incumbent on investigators to improve and empower themselves with appropriate training in order to enhance effective investigation.

The outcome of any criminal case is only as effective as the investigation methods used, especially that the investigation of crime has evolved from being a local policing tool implemented to manage serious and violent crime, to a method focusing on achieving justice (Gardner, 2012:7; Van Rooyen, 2012:3). Cell phone record and data analysis provides an opportunity for forensic examiners to comprehend a range of relevant crime information patterns including the members' positions, ranks, and roles within a criminal organisation; as well as the inter-organisational links with fraternal criminal organisations and syndicates (Alshammari & Alghathbar, 2017:2; Clark, 2007:1413).

Criminals rarely operate and work alone. Instead, they operate within a group as part of a criminal network or enterprise that thrives on constantly formulating mechanisms to conceal their criminal activities to evade any scrutiny or exposure (Wall, 2017:4). Generally, there is a hierarchy within crime organisations. Operational orders are issued according to a command system designed to make such orders difficult to trace, because criminals go the extra mile to evade the law at all costs (Clark, 2007:1419; Van Niekerk, 2015:49).

Digital forensics has become instrumental in the investigation of crime, especially that the public has become more reliant on the allure of information and communication technologies (ICT) (Sai et al., 2015:4847). In this regard, cellular device forensics has become a specific component of digital forensic investigations whose primary goal is to recover or collect information and evidence from cell phones and other similar devices. Sai et al. (2015:4847), mention further that digital forensics is advantageous for enhancing investigators' capacity to resolve pertinent questions relating to the link between the commission of varying crimes and mobile device-based communication. The use of cell phone analysis has broadened law enforcement horizons with the introduction of digital forensics as a priceless and valuable investigative tool. However, the lack of knowledge regarding cell phone data analysis amongst investigators could trigger challenges with criminal investigation (Alhassan, Oguntoye, Misra, Adewumi, Maskeliūnas & Damaševičius, 2018:105). Therefore, it is imperative for investigators to gain knowledge regarding cell phone analysis as an investigative tool to solve serious and violent crime. The preponderant growth and usage of cell phone technology has accelerated the

frequency of cellular device usage as an instrument to commit crime (Alhassan et al., 2018:105). Therefore, unresolved or unsuccessful investigation of serious violent crime involving cell phone communication could have immense multiple effects on several levels for victims, the general public, the Police and the criminal justice system (Higginson et al., 2017a:4).

1.2 RATIONALE OF RESEARCH (PROBLEM STATEMENT)

Research is basically premised on a problem that the researcher has identified and desires to resolve (Kumar, 2019b:29). In this regard, the research problem is then defined as a general topic of interest that is characterised by problematic aspects, which can be resolved by means of gathering all the pertinent and essential data and evidence (Kumar, 2019b:29). Furthermore, Kumar (2019b:29) mentions that the most difficult part in research is often to define the research problem. Meanwhile, Henning, Gravett and Van Rensburg (2013:20) aver that a research problem could be viewed as an academic riddle that is addressed through research, or a roadmap which outlines the entire research project and provides guidance on how to locate the problems for research. As such, the researcher distinguishes the rationale of the problem from statement of the problem itself.

According to Henning et al. (2013:21) and Thiel (2014:15), the rationale of the study is mainly the justification or motivation allocated by the researcher to the reasons for undertaking the study. As such, the rationale of this study emanates largely from the researcher's own experience-based observations during his professional career as a qualified Forensic Analyst employed at the Forensic Science Laboratory (FSL) in the Western Cape, a specialised structure within the SAPS. It is in the context of his afore-cited designation that the researcher was prompted to undertake the present study on account of his poignant concerns with the core issue of deficient skills and knowledge in digital forensics by crime investigators. Evidently, such concerns are justifiable, given the rapid advances and levels of sophistication in the commission of digital crimes in which the cell phone has been identified as the foremost instrument of the crime. As for the concerns themselves, they are aptly captured in Sub-section 1.2.1 hereafter.

1.2.1 Research problem

As opposed to the rationale of research (and its justification of the study's undertaking), the research problem itself disentangles the reasons (i.e. concerns) advanced by the researcher and presents them as organised statements of enquiry that articulate the difficulty identified by the researcher in respect of a particular field of study (e.g. digital forensics); a specific situation (e.g. rampant crime in the WCP); or a phenomenon (e.g. investigative value of cell phone record analysis) (Badenhorst, 2014:19; Henning et al., 2013:20; Kumar, Hanumanthappa & Suresh Kumar, 2016:38). In the context of the present study, the research problem resides entirely within the escalation of WCP crime statistics; deficient record retrieval skills; as well as challenges attendant to investigating officers' understanding of the correct procedure to obtain data from the service provider. The escalation of WCP Crime Statistics is discussed hereafter.

1.2.1.1 Escalation of WCP Crime Statistics

Alan Winde (Western Cape Premier) and Albert Fritz (Member of the Executive Council (MEC) for Safety and Security in the WCP), poignantly lamented that the SAPS has lost the war on crime, despite the promises made by Minister Bheki Cele to restore the rule of law in this province (Chambers, 2019:1). The number of serious and violent crimes remains unchanged in the WCP, as demonstrated by the 6.6% murder rate increases for the 2018/19 financial year (Department of community safety Western Cape Government, 2019:10). Figure 1.2 below indicates the crime statistics in the WCP for the period 2016 to 2019.

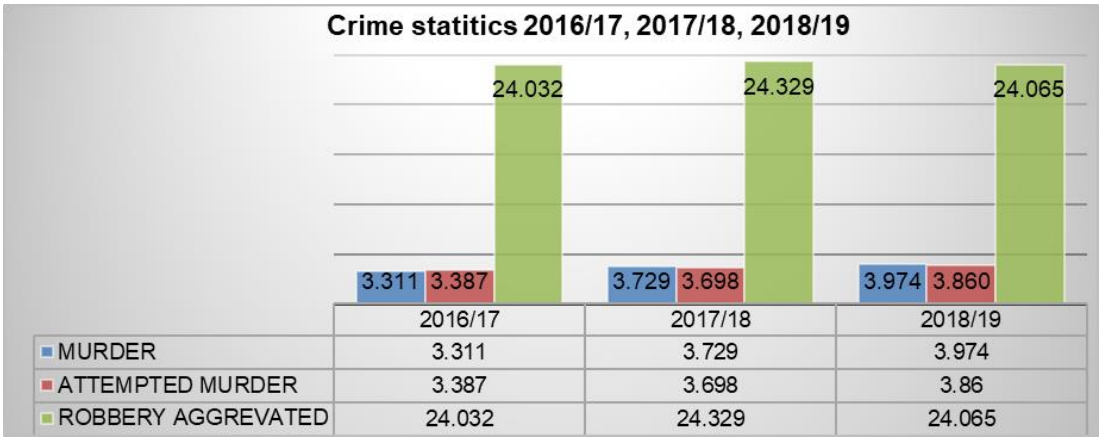

Figure 1.2: Crime statistics

(Source: Researcher's adaptation from Department of community safety Western Cape Government, 2019:10)

All the crime statistics in Figure 1.2 above accrue principally from a collation of SAPS (2019) and Western Cape Government (2019) sources.
Extrapolated from Figure 1.2 above, is that the financial year 2017/18 showed an increase in murders, compared to the 2016/17 financial year by a total of 418 cases (12.6%). Meanwhile, the 2018/19 financial year shows an increase of 245 cases (6.6%), compared to the previous 2017/18 financial year. On the other hand, attempted murder cases increased by 311 (9.2%) for the 2017/18 financial year compared to the previous 2016/17 financial year.

Furthermore, an increase of 162 (4.4%) attempted murder cases were recorded during 2018/19, compared to the preceding 2017/18 financial. At the same time, aggravated robbery shows an increase of 297 cases (1.2%) during 2017/18. However, the crime trends showed a decrease of 264 cases, (1.1%) during the 2018/19 financial year (SAPS, 2019:1; Department of community safety Western Cape Government, 2019:10). As testimony to the problem of escalating crime statistics in the WCP, Minister Cele stated ominously during the official 2017/2018 annual crime statistics presentation: "*We [SAPS] dropped the ball*" (SAPS, 2019:2). Incontrovertibly, the words by a Minister of Police sums the difficulty faced by the SAPS in curbing the rise of crime in the Western Cape particularly and South Africa generally.

1.2.1.2 Deficient record retrieval skills and knowledge

In addition to the escalating WCP crime trends, the researcher has also critically identified the lack of adequate professional training as a disconcerting issue manifested in both the deficient record keeping skills and procedures for obtaining the actual records themselves (discussed in the ensuing section). In terms of Section 205 of the Criminal Procedure Act (Act No. 51 of 1977) the retrieval of any records and data from a seized cell phone is deemed unlawful. The Criminal Procedure Act (Act No. 51 of 1977) is (hereinafter referred as CPA (Act No. 51 of 1977). The Section 205 application must be properly completed to gain access to the records and data stored on the cell phone. Investigating officers need to apply for the "seizure of the cell phone and data" and "SIM card with data", which legalises the downloading and retrieval of the cell phone records and data.

In *S v De Vries and Others* 2009 (1) (SACR 613 (C)) the Court ruled on the admissibility of the Section 205 application. Also, in *S v Motloutsi* 1996 (1) (SACR 584 (C)) and *S v Mayekiso* 1996 (2) (SACR 298 (C)), "the exclusionary rule" clarifies to all State officials the futility of unlawful gathering of evidence because such evidence will be considered as inadmissible by the Courts (South Africa, 1977:1). According to Section 35 (5) of the Constitution (Act No. 108 of 1996), any unlawfully obtained evidence that further violates any of the rights in the Bill of Rights ought to be excluded if its admission would imperil the trial's fairness, or alternatively be inimical to the administration of justice. This Section obligates the Courts to exclude such evidence. When the correct procedure is not followed, it will result in the evidence being ruled inadmissible, and will be excluded as evidence in a trial. Evidence ought to be collected and obtained such that it will not violate the perpetrator's rights (South Africa, 1996:1). Therefore, deficient record retrieval skills and knowledge largely premises on the investigating officers' incorrect interpretation of the applicable legal prescripts.

According to Section 205 of the CPA (Act No. 51 of 1977), subsection (4) and Section 15 of the Regulation of Interception of Communications and Provision of Communication- related Information Act (Act No. 70 of 2002), only a High Court Judge, a Regional Magistrate, or a Magistrate issues a subpoena for any person who may furnish the Court with relevant information of an alleged offence that was committed to justify the "seizure" of a mobile device for its records and data. The Regulation of Interception of Communications and Provision of Communication-related Information Act (Act No. 70 of 2002) is (hereinafter referred as RICA (Act No. 70 of 2002).

In discussions with the researcher, investigating officers informed him (the researcher) about the challenges such as the lack of clear guidance on how to complete the Section 205 application correctly and how to interpret and analyse cell phone records and data. The researcher further established that the investigating officers request the "seizure of the cell phone" which only allows for the cell phone to be seized. The wording "seizure of the cell phone" on the Section 205 application indicates only the seizure of the cell phone, and not retrieval of any of the information and data stored in it.

The correct procedure is that the investigator submits a Section 205 application accompanied by a signed affidavit providing grounds for the issuance of such a subpoena. This will include reasons why the person is suspected of involvement in the particular crime, the specific time of the crime, the location of the cell phone; and the communication for the specific cell phone will be cited in the request. The application for a Section 205 subpoena will be handed to the Prosecutor or Director of Public Prosecutions (DPP) for authorisation to obtain the required cell phone records. The Prosecutor or DPP will then duly recommend that the cell phone records may be obtained, and will present the signed affidavit and application to the High Court Judge, a Regional Magistrate or a Magistrate for review.

1.2.1.3 Procedure to obtain data from the service provider

Once the High Court Judge, Regional Magistrate or Magistrate confirm that there are reasonable and sufficient grounds to issue such a subpoena. The authority will be given to obtain cell phone records from cellular network service providers such as Vodacom, CELL C, and MTN. It is the investigating officer's responsibility to hand over the authorised Section 205 subpoena to the Technical Support Unit (TSU) of the SAPS. TSU is responsible to subpoena the respective cell phone networks for the purpose of obtaining the requested cell phone records, citing the specific periods requested by the investigating officer. Upon receiving the requested cell phone records, the TSU will then hand them over to the investigating officer.

Based on the consultation between the researcher and about 20 investigating officers, it was discovered that once the requested data is received, the investigating officers had difficulty in interpreting, understanding and analysing the cell phone records and data. Sai et al. (2015:4847) and Clark (2007:1500), posit that the world of cell phone (mobile) forensics is complex and deals with various cell phones and different mobile device manufacturers globally. Each of these cell phone and mobile device manufacturers has developed their own proprietary technology and formats different from others, since there is no standard format for every cell phone manufacturer (Van Niekerk, 2015:50). According to Sai et al. (2015:4847) and Clark (2007:1500), the current methods of crime investigation are becoming anachronistic, and the pace is delayed when one considers the fast-growing technology of new mobile devices such as cell phones and personal digital

assistants (PDAs) being released daily. Therefore, forensic investigators are obliged to update their knowledge and advance their technology skills in tandem with the Fourth Industrial Revolution (4IR) and its fast-growing artificial intelligence (AI) (Alhassan et al., 2018:105; Srivastava & Vatsal, 2016:5). The ever-changing and sophistication of the criminals' modus operandi makes it impossible for law enforcement agencies to conform to only conventional ways of investigating crime. Therefore, new methods of the use of technology should be implemented to stay abreast of criminals. The lack of knowledge and advanced skills of technology in cell phone record analysis has a negative impact on the quality of the serious and violent crime investigations, the process of litigation, as well as the successful prosecution of suspects (Alhassan et al., 2018:105; Sai et al., 2015:4852; Srivastava & Vatsal, 2016:5).

Considering the significance of data associated with crimes, the examination of the data is an indispensable component in detecting and preventing crime. Accordingly, criminal investigators have an opportunity to develop cell phone investigating policies and strategies based on data collected for the effective prevention and detection of crime (Alshammari & Alghathbar, 2017:4). Cell phone (mobile) forensics and analysis is imperative in investigation of serious and violent crime, especially when the knowledge and skills are continuously updated (Alhassan et al., 2018:105; Sai et al., 2015:4852). The analyses could be an innovative source of great investigative value to help prove a case beyond any refutable scope. Evidence proves itself either testimonially or physically (Gardner, 2012:7).

The chain of custody, proper documentation and preservation of the cell phone records and data become crucial when presenting evidence in Court. Given the researcher's articulation of the research problem and its multi-factorial manifestation, it is clear that the identified problems were likely to persist. Therefore, protracted investment of Police resources is imperative in the investigation of serious and violent crimes (Higginson et al., 2017b:1). It is the researcher's contention that the end results of such investment will yield the desired methodologically precise experimental research on both established and new investigative procedures accessible to law enforcement and administration of justice.

1.3 DEMARCATION OF THE STUDY

Kumar (2019b:47) agrees that the study's demarcation premises on the boundaries set by the researcher to restrict the reach of the study. This involves setting limits and boundaries to indicate what is beyond the control of the researcher. Kumar (2019b:47) adds further that the purpose of delimitation in research as follows:

- It guides and assists the researcher in applying the study in a systematic manner;
- It indicates the research path and process to the researcher;
- It helps to project expenditure items and costs linked to the successful accomplishment of the research project; and
- It assists the researcher to focus on the work by outlining the specific boundaries.

The researcher acknowledges that the research poses certain limitations which are important to list for realistic and practicality purposes in the quest to increase the trustworthiness of the study (Ary, Cheser Jacobs, Sorensen Irvine & Walker, 2019:442; Daniel, 2019:102). For example, it would be impossible for the researcher to interview all digital forensic investigators/analysts who conduct cell phone record analysis as well as investigators from various stations and units within the SAPS. This will not be achievable due to practicalities such as restricted time frames, geographical distribution of experts in the area of cell phone record analysis; as well as the financial wherewithal for such an undertaking.

As such, the researcher was unable to travel long distances to conduct interviews with experts in the field of study. Therefore, only selected Police stations within the Winelands District could be involved in the study. For this study's purpose, the participants from the SAPS (Sample A, C, D & E) was grouped together and participants from the NPA (Sample B), when presenting the responses of the participants. However, these limitations have no bearing on the outcomes of the study.

1.4 AIM OF THE RESEARCH

Habib, Pathik and Maryam (2014:1) describe research as a systematic and methodical academic, scientific and philosophically inspired enterprise in terms of which evidence or relevant data is collected in a particular field of study to support or contribute to existing or new knowledge in that field of study. Bak (2013:15) and Thiel (2014:15) describe research as a journey which leads the researcher to many destinations where he/she wants to arrive and accomplish several aims and purposes. However, Bak (2013:16) and Habib et al. (2014:3), caution that a researcher should avoid many research aims as this might give the impression that the researcher is not certain of what is being investigated. Accordingly, the aim of this research is: *To explore the investigative value of cell phone record analysis in the investigation of serious and violent crimes in the Winelands District, Western Cape Province*.

1.5 RESEARCH OBJECTIVES

Niven and Lamorte (2016:8) describe an objective as a concise statement which outlines the goals set out by the researcher. Kumar (2019b:39) augments that a research objective relates to an individual task which must be carried out to meet the research aims. Therefore, the below-cited objectives were formulated with the view to achieving the aim of the research:

- To explore, describe and analyse the nature of crime investigation in South Africa;
- To explore and describe the meaning of cell phone records analysis;
- To determine how cell phone records are analysed;
- To explore and describe how analysed cell phone records can add value in the investigation of crime;
- To explore and describe the valuable information that cell phones or SIM cards hold in the investigation of crime; and
- To develop practical guidelines, procedures and recommendations for the SAPS to successfully use analysed cell phone records in the investigation of serious and violent crimes.

1.6 RESEARCH QUESTIONS

Kumar (2019b:33) mention that the terms, ‘research question’ and ‘problem statement’ are occasionally used interchangeably. However, they serve different purposes. A research question is not a “re-statement” of the research problem, but unfolds the research problem (Badenhorst, 2014:25). Research questions shape the principal components of what will be investigated and guide the research process. The formulation of a good research question is an essential step in the research process (Lamont & Boduszyński, 2020:52). Following are the research questions formulated for this study:

- What is the nature of crime investigation in South Africa?
- What is the meaning of cell phone records analysis?
- How are cell phone records analysed?
- What is the value of analysed cell phone records in the investigation of crime?
- What is the valuable information that cell phones and SIM card hold in the investigation of crime?
- What practical guidelines, procedures and recommendations can be offered to the SAPS to successfully use in analysing cell phone records in the investigation of serious and violent crimes?

1.7 PURPOSE OF THE RESEARCH

Babbie (2014:94), Leavy (2017:5) and Maxfield and Babbie (2017:12) posit that there are various purposes entailed in social research. Meanwhile, Kumar (2019b:8) alludes that the main purpose of any research should be to answer the research questions by means of scientific procedures in order to establish credible findings. Habib et al. (2014:11), are of the view that the significant purpose in research is to produce new ideas, broaden knowledge, revision and/ or repositioning of current theories, as well as testing concepts. According to Patten and Newhart (2018:4), many careers challenge individuals to establish means to collect, interpret, analyse and understand information and data. As such, opportunities are created to undertake systematic enquiry on what is known, and what still needs to be researched or known. Moreover, gathering of information during research is a combined effort, where each well-designed research study affords proof that may sustain, adjust, disprove, or intensify the understanding of existing information.

Ultimately, the results obtained from a research project may empower the reader to view and understand facts better (Alderson & Morrow, 2020:6; Badenhorst, 2014:25). It is in this regard that the primary research purposes applicable to this study relate to exploration, description and explanation, and empowerment of those who are being investigated or researched.

1.7.1 Exploration

According to Babbie (2014:94) and Habib et al. (2014:7), much research in the social sciences is conducted for exploration of a specific topic for researchers to familiarise themselves with the topic under investigation. Babbie (2014:94) and Leavy (2017:5) intimate further that researchers conduct exploratory studies in the fields which are relatively new or under-researched in order to create opportunities to fill gaps in knowledge, or to generate new and emerging scholarly insights. In addition, exploratory studies are normally conducted with three purposes in mind: to satisfy the curiosity of the researcher and the aspiration for better insight; to investigate the possibility of undertaking a more protracted study; or to develop procedures for utilisation in any successive study Babbie (2014:94) and Patten and Newhart (2018:4).

Based on the assertions by Babbie (2014:94) and Leavy (2017:5), the researcher believes that an exploratory research is appropriate for this research; more so, the topic under investigation is a relatively new topic. The researcher intends to explore the interpretation and analysis of cell phone records, as well as the utilisation of those records for evidential purposes in investigation of serious and violent crimes. The intention of the researcher is to apply the new knowledge to develop good practices that will provide new guidelines and procedures that can be used by investigating officers in serious and violent crimes. This will be done through consultation of national and international sources, conducting interviews with selected participants for the singular purpose of obtaining new information to explore the investigative value of cell phone record analysis in the investigation of serious and violent crimes.

1.7.2 Description

Habib et al. (2014:8), aver that descriptive research can be utilised to provide more details or information about a unit of analysis. Descriptive research transcends mere investigating of the problem in an exploratory and explanatory research. Maxfield and Babbie (2017:13) argue that descriptive research is often concerned with documenting or counting participant observations. Corbin and Strauss (2015:59) mention that individuals would literally not be able to communicate without the ability to describe situations or a phenomenon. Corbin and Strauss (2015:59) and Leavy (2017:5) add further that individuals often describe objects, events, actions, emotions, scenes or people in their everyday conversations with one another. In the case of this study, the researcher applied semi-structured interviews to obtain descriptive data from the selected participants.

1.7.3 Explanation

According to Tardi (2019:28), explanatory research entails intensive and detailed research for developing a comprehensive and complete understanding of the topic. Meanwhile, Maxfield and Babbie (2017:13) are of the view that the explanatory research is conducted to explain situations and phenomena, and when a change in policy is considered. Therefore, the purpose of explanatory research is to develop and improve understanding in respect of the topic under investigation. Tardi (2019:29) further argues that explanatory research necessitates the collection of reliable data from trustworthy and primary sources. In the current research study, the researcher extends the exploration and description of the interview-based information by explaining (analysing and interpreting) the participants' views in relation to the topic being researched, the researched problem; as well as the objectives and questions. Ferraro (2015:3) augments that such explanation should also enhance the establishment of measurable results and findings. Accordingly, the researcher has continuously provided explanations of the participants' perspectives in the respective chapters throughout the study.

1.7.4 Empowerment of those being researched

Research is conducted in a methodical and organised manner in order to discover underlying issues and matters that sustain professional development and dignity; as well as presenting an opportunity to develop knowledge based on sound

scientific findings (Habib et al., 2014:11). It is in such a context that Edwards and Holland (2013:5) contend that the participants who partake in research do so in a ***representative*** capacity. Therefore, the findings on these participants are intended to be generalised for the empowerment of even those in the same (professional) category, but did not participate in the research study. For example, Bleck (2015:101) and Vallabhaneni (2019:303) state that the main purpose for empowerment is to place the power and capacity to improve to the relevant people within the organisation, where the real work is being done.

The findings of the research can be used to empower the researcher, fellow investigators within the SAPS, Crime Intelligence, SAPS Operational Command Centre (also known as the 'War Room') and or the Directorate for Priority Crime (DPCI/Hawks); and other law enforcement agencies to better understand cell phone record analysis. In addition, the research and its results could be of value to the SAPS for integration into the detective training manuals and other lecturing materials. Investigators could gain knowledge and experience from this study, which will empower them in the execution of their daily criminal investigation tasks.

The researcher made recommendations for the development of good practices, which will empower the investigating officers to understand the investigative value of cell phone record analysis as a source of evidence in investigating serious and violent crimes. Academically, the University of South Africa and the broader academic community might use the study for future reference to students who pursue their studies in digital criminal investigation. The research will also be submitted to an accredited journal for possible publication to make the findings of this study available for academic research to empower students and be available for future reference.

1.8 DEFINITION OF KEY TERMS

Putman and Albright (2018:30) state that key terms are useful for guiding and performing preliminary searches that enhance the researcher's familiarity with the area of investigation. It is the responsibility of the researcher to identify the key terms and concepts, placing emphasis on what is known and understood; and how this will be used during the course of the research. There should be no room for

uncertainty or misinterpretation about these important key terms and concepts (Niven & Lamorte, 2016:18; Putman & Albright, 2018:30).

1.8.1 Cell data

Cell data is the complete billing records which are created and stored when a subscriber uses the network. This will record and store all cell phone activity of the particular cell phone gadget (Zinn & Dintwe, 2016:328).

1.8.2 Cell phone records

Schmitz (2005) as cited in Van Niekerk (2015:49) describes cell phone records as documented and stored cellular activity recorded by the service providers for billing purposes. Such records can be used for forensic cell phone investigation purposes.

1.8.3 Crime mapping

Kawthalkar, Jadhav, Jain and Nimkar (2020:360) describe crime mapping as a technique of detecting and signifying particular areas in a specific geographical region as crime hotspots.

1.8.4 Criminal investigation

Reilly (2019:1) describes criminal investigation as the continuum of symbiotic processes and activities linked to the maintenance and support for the rule of law, analysing criminal conduct with the objective of establishing what happened, *why* it happened and *who* did it. Eventually, offenders are then prosecuted and convicted.

1.8.5 Digital evidence

Zinn and Dintwe (2016:371) mention that digital evidence is any form of data which is stored or transmitted in some or other electronic dual format to be used for Court procedures, whether criminal prosecution, civil litigation or disciplinary hearing to prove or disprove the facts in question.

1.8.6 Expert evidence

According to Swanepoel, Lötter and Karels (2014:261), expert evidence is defined as evidence provided by an individual considered as an expert within their respective field of specialisation, and who possesses the necessary qualification in the form of knowledge, skills and experience to be regarded as such.

1.8.7 Geographic Information Systems (GIS)

A geographic information system (GIS) is a system for creating, managing, analysing, and mapping all types of data. It is also an investigative tool used to visualise the spatial crime trends and criminal behaviour to identify and plot crime hotspots. The system is also used to track crime locations, and track serial offenders in crimes such as murder, rape and burglary (Zinn & Dintwe, 2016:314).

1.8.8 International Mobile Equipment Identity (IMEI)

Kumar et al. (2016:46-47), describe the International Mobile Equipment Identity as the specific and unique number of a mobile device that remains unchanged despite the user's change of service provider or mobile number.

1.8.9 Serious and violent crime

According to Higginson et al. (2017a:3), there are various definitions of serious violent crime in literature. As such, there is conceptual ambiguity about the ontological nature of violent crime, and the 'serious violent crime' variant. Notwithstanding, Higginson et al. (2017a:3), is of the view that the most effective approach is to offer an offence-based perspective of serious violent crime, which includes: robbery, aggravated, assault, murder, rape or other sexual assault.

1.8.10 Subscriber Identity Module (SIM) Card

Srivastava and Vatsal (2016:2) describe the Subscriber Identity Module (SIM) card or chip as a Universal Integrated Circuit Card (UICC), which is essentially a smart card that assists devices, such as mobile phones and set top boxes to connect to its closest cellular radio network tower for the purpose of communication.

1.9 RESEARCH STRUCTURE

This research is divided into six chapters as indicated below.

Chapter 1: General orientation

This chapter presents the introduction, the research problem, the research aim, the objectives, questions and purpose of this study. The chapter also presents the demarcation of the study, followed by the definition of key terms.

Chapter 2: Methodological framework of the study

This chapter presents the methodological framework in terms of the philosophical worldview offered in this study, as well as the research design and approach of this study. Furthermore, the chapter outlines and discusses the population and sampling methods, data collection, analysis and the interpretation thereof. The evaluation of the study's trustworthiness and ethical considerations are also discussed in the chapter.

Chapter 3: Criminal investigation

The chapter explores, describes and analyses the nature of crime investigation in South Africa, as well as the role of the investigating officer and the Prosecutor. The chapter also discusses the principles, objectives, and evidence in criminal investigation.

Chapter 4: Cell phone record analysis

In this chapter, the exploration of the role of cell phone record analysis in the investigation of serious and violent crime is presented with a detailed evaluation of Section 205 applications as prescribed in the CPA (Act No. 51 of 1977), which deals with obtaining cell phone records. The investigative value of cell phone record analysis is discussed and explored. The chapter also outlines the type of evidence which cell phone record analysis can present in the investigation of serious and violent crime.

Chapter 5: Analysis of SIM cards

In this chapter, the analysis of SIM cards is presented, as well as the investigative value of SIM cards in the investigation of serious and violent crime. The chapter further outlines the use of SIM cards in obtaining valuable data to assist in the investigation of serious and violent crime. Furthermore, the structure and definition of a SIM Card is presented.

Chapter 6: Research findings and recommendations

This chapter presents the analysis and interpretations of the findings, as well as the recommendations accruing from these findings. This chapter concludes with the researcher's own remarks based on the research findings.

CHAPTER 2: METHODOLOGICAL FRAMEWORK OF THE STUDY

2.1 INTRODUCTION

According to Walker and Solvason (2014:62), it is essential for researchers to differentiate between the data collection methods and procedures in order to decide appropriately on a research methodology that strengthens rather than weakens the nature of the research findings. Such differentiation is enhanced through a methodological framework and its constituent building blocks demonstrating the practicality of the study in relation to its outcomes and the means by which those outcomes were reached or accomplished. It is in this regard that Mason (2018:32), Silverman (2020:56) and Taylor, Bogdan and DeVault (2016:3) refer to methodology in research as the strategies, plans, techniques, approaches and methods (research instruments) used for addressing the research problem and its associated research questions. It is on the basis of its methodological framework that the study is able to allocate a degree of structure and synchrony between its data acquisition processes on the one hand, and data analysis procedures on the other (Majid, 2018:1; Mason, 2018:32).

Daniels (2019:104) further accentuate the importance of the philosophical foundations of a study, is providing a coherent narrative for stitching and weaving the various constituent methodological elements into building blocks that ultimately illuminate on the nature of the study's theoretical and eventual experiential construction. Accordingly, this chapter presents the philosophical worldview offered in the study, followed by the research design and approach; data collection; study population and sampling; data interpretation; as well as the trustworthiness and ethical issues.

2.2 PHILOSOPHICAL WORLDVIEW OFFERED IN THIS STUDY

Both Creswell (2015:15) and Yin (2014:128) intimate that a philosophical worldview (paradigm or perspective) is basically a scientifically or intellectually informed orientation that researchers bring to the study. Such an orientation encapsulates some fundamental beliefs, abstract ideas and assumptions that guide, inform or direct the researcher's universal conceptualisation and view of the world, people, knowledge, and truth (Yin, 2014:128).

According to Creswell (2014:6) there are generally four widely discussed worldviews in literature, namely: the post-positivist, transformative, constructivist, and pragmatic worldviews. The constructivist and pragmatic worldviews are discussed briefly in this section insofar as their relevance apply to this research.

2.2.1 Constructivist worldview

In qualitative research, the constructivist worldview often combines social constructivism with interpretivism to reflect on the belief that people seek and construct meaning and knowledge about the world in which they live and work (Hammond & Wellington, 2013:32). On the other hand, the aspect of interpretivism is concerned with the extent to which there is acknowledgment of subjective meanings as critically influential in social action, and aims to disclose interpretations and meanings rather than behavioural relations (Creswell, 2014:8; Walliman, 2016:12). Meanwhile, Leavy (2017:13) corroborates further that the qualitative researcher should value the participant's subjective perceptions, knowledge, understanding and interpretation of their experiences and circumstances. It is axiomatic that all the afore-cited constructivist-interpretivist assertions posit the role and viewpoint of the participant as most pivotal in the construction and development of the study's most sought-after knowledge and evidence.

The constructivist worldview is deemed to be most applicable to this study insofar as it allows and is reliant on a participant-focused construction and interpretation of knowledge about the investigative value of cell phone record analysis when investigating serious and violent crime, from their own subjective understanding (Bryman, Bell, Hirschsohn, Dos Santos, Du Toit, Masenge, Van Aardt & Wagner, 2014:14). The researcher interviewed participants to basically understand their views, thoughts and meanings they attach to the investigative value of cell phone record analysis when serious and violent crime is investigated. Through a more open-ended line of questioning, the researcher listened carefully to the participants as they shared their knowledge and understanding of cell phone record analysis within their own right.

2.2.2 Pragmatic worldview

The pragmatic worldview is premised on the notion of what is practicable and fits the context, or what applies without the constriction of any particular philosophical or methodological orientation or tradition in any particular setting (Creswell, 2015:37; Khaldi, 2017:15). In the pragmatic worldview, individual researchers can freely choose the procedures, techniques, approaches, and methods and procedures of research which best suit their needs (Morgan (2007) as cited in Creswell, 2014:11; Padgett, 2012:26). Furthermore, an essential pragmatism principle is to recognise and consider concepts and their practical meanings and consequences, instead of embracing preconceived ideas and orientations about those particular concepts in their everyday meaning (Hammond & Wellington, 2013:125).

It is the forte of the pragmatic paradigm to produce solutions which fit their abductive rationale, which is neither induction nor deduction, but a constant process of producing and testing theories to generate practical solutions (Hammond & Wellington, 2013:125). Creswell (2015:26) and Hammond and Wellington (2013:125) are of the view that pragmatism accentuates actions and outcomes to present a solution to the problem being studied. As such, the pragmatic worldview welcomes and integrates multiple or mixed-methods research (combining quantitative and qualitative approaches) and more than one data source to resolve both the research problem and attendant research question/s (Creswell, 2015:27).

The latter author submits further that individuals who hold an interpretive framework grounded in pragmatism would be more inclined to focus on the research findings, actions, circumstances and consequences of an enquiry, instead of antecedent conditions. The researcher considered the pragmatic worldview as relevant to this study, because it allows for the employment of methods, procedures and techniques best suited in addressing the research problem and multiple responses to the research questions from the vantage point of the participants.

2.3 RESEARCH DESIGN AND APPROACH

Rees (2016:111) and Kay and Wainwright (2018:136) intimate that a research design incorporates the type of approach and structure the researcher intends to

use in the study. The latter author submits further that it also includes the data collection methods that will be employed to answer the research questions linked to the phenomenon under investigation. Bryman et al. (2014:100), elaborate that in addition to providing structure of the study, the research design further enables the articulation of a framework linking the adopted philosophical worldview with the data collection and analysis approaches and procedures respectively. Meanwhile, Bhattacherjee (2012:35) asserts that the research design pertains to a “blueprint” or comprehensive empirical data gathering plan developed by the researcher, and addresses the research problem and its specific research questions, or even testing theory in some instances.

Thomas (2017:138) augments further that the research design concerns itself with outlining the plan and structure of the entire programme of the research, from the purpose to the execution thereof. For Majid (2018:1), the research design includes the use of informed procedures, approaches, processes and guidelines that provide the appropriate research instruments and frameworks. In this study, the qualitative research approach is employed, and its choice was influenced mostly by the type of worldview adopted, including the methods of data collection and analytic procedures (Creswell, 2014:17). The qualitative research approach is discussed in greater detail hereafter.

2.3.1 Qualitative approach

Hennink, Hutter and Bailey (2020:10), Grove, Gray and Burns (2015:67) and Yin (2016:9) define the qualitative research approach as enabling the researcher’s investigation of unquantifiable attributes of the participants, such as their knowledge, experiences and perceptions or understanding in relation to a particular phenomenon. Creswell (2014:4) and Silverman (2020:46) ascribe qualitative research to an approach intended to discover and comprehend the degree of importance allocated to a social or human problem by individuals or groups of people. Creswell (2014:4) and Silverman (2020:46) furthermore argue that the qualitative process involves the collection of data with the use of open-ended questions, the deduction of general themes accruing from the collected, analysed and interpreted data. On the whole, the qualitative research approach essentialises non numerical data through the spoken and written words in their original context

(Cassell, 2015:4; Curtis, Ramsden, Shaban, Fry & Considine, 2019:97). The qualitative research approach is considered appropriately placed for this study, based on its non-quantification of the overall study outcomes (Curtis et al., 2019:97; Hennink et al., 2020:17). In this regard, exploration, description, observation, analysis and interpretation were relied upon as the most viable tools to derive social meanings relevant to achieving the intended research outcomes (Silverman, 2020:6; Tarab, 2019:1). The qualitative approach was preferred for its facilitation of studying human behaviour and its motivations, utilisation of ethnography and phenomenology (interpretive methodology), narratives, small samples, and case study designs (Mavodza, 2020:5; Silverman, 2014:5).

Accordingly, the researcher was able to explore, describe, analyse and interpret the investigative value of cell phone record analysis in the investigation of serious and violent crimes in the Winelands District from the participants (experienced investigators and Prosecutors involved in investigation of serious and violent crimes) in their own words and natural setting; and according to their own understanding, experiences and perceptions (Cassell, 2015:4; Hennink et al., 2020:10; Yin, 2016:11).

2.3.1.1 Case study research design

In the methodological context, “case” relates to units, processes, systems, persons, events or any other (in)tangible object and/ or idea that can be studied singularly or collectively by applying a single method or more (Bell & Waters, 2014:11; Kay & Wainwright, 2018:127; Tight, 2017:9). Case study design, therefore, entails a comprehensive, in-depth and rigorous analysis of a single case or more which the researcher wishes to examine for an extensive period (Bhattacherjee, 2012:40; Bryman et al., 2014:110). According to Bell and Waters (2014:11), a case study design is best suited for researchers who work individually as it affords them the opportunity to investigate a particular aspect of a problem in depth.

In this study, the investigative value of cell phone records (core unit of analysis) presents a complex and bounded case framework in terms of which individuals or groups (i.e. participants), events, systems and activities (i.e. investigations) and the Winelands (i.e. place) interact as different but interlinked constituent parts or

aspects of the research problem and its associated research questions. Therefore, the researcher found the case study design approach to be suitable insofar as it allows for the investigation of various aspects of a “case” from multiple participant perspectives, and with the utilisation of multiple data sources and methods (Bell & Waters, 2014:11; Tardi, 2019:4). From the study’s viewpoint, the participants themselves could further be viewed as non-numeric individual “cases” of multiple subjective experiences and realities concerning the same (single) phenomenon of the investigative value of cell phone record analysis in the investigation of serious and violent crimes.

The case study research design approach is most relevant in this study, since it encourages the utilisation of interviews as a mechanism to gather ‘cases’ of participants’ experiences and knowledge in respect of the research problem and answers to the research questions (Tardi, 2019:4; Yin, 2014:110). In addition, such a design approach is beneficial for its allowance of the researcher’s recommendations emanating from the findings and the various constituent elements or cases of experiences of the participants revealed during the in-depth interviews and other pertinent qualitative data collection methods; such as literature and documentary reviews, observations and personal experience (Astalin, 2013:122; Tight, 2017:12).

2.4 DATA COLLECTION

Data refers to pieces of information that has been converted, translated or transformed into some intelligible form (Bard, 2019:4; Merriam & Tisdell, 2016:105). On the other hand, Habib et al. (2014:1), elaborates further that data relates to raw facts or information necessary in research studies for measuring a particular phenomenon for researchers to make valid and reliable decisions. Accordingly, data collection is then viewed as a methodically conducted process for acquiring information deemed to be useful or relevant for purposes of the study; that is, in terms of resolving the research problem and achieving the specific intentions of the study (Cassell, 2015:3; Haven & Van Grootel, 2019:232). There are basically two data forms or types, primary and secondary. Primary data is immediately obtainable from the participants for the specific purpose of the research through the researcher’s direct involvement in the acquisition process, either by fieldwork or

direct surveys (Habib et al., 2014:4). Meanwhile, secondary data is already available to the researcher and has been collected by others for other purposes (Kumar, 2014:40). Interviews and focus group discussions are examples of primary data, while literature and documentary reviews are examples of secondary data (Bryman et al., 2014:267; Haven & Van Grootel, 2019:232). In the present study, both primary and secondary qualitative data collection techniques were applied in order to address the research problem, aim, objectives, and research questions. The researcher collected primary data from his personal experience and by interviewing the sampled participants, while secondary data was obtained by reviewing literature and the relevant South African legislative and policy documents. These methods are discussed in greater detail hereafter.

2.4.1 Literature review

Once a research topic has been selected, it then becomes imperative to review all possible material relevant to the particular topic (Anderson & Poole, 2014:21). According to Badenhorst (2014:19) and Flick (2020:82), literature review is regarded as a protracted examination of previous research studies for their contextualisation in an existing academic situation or environment; that is, establishing what other scholars have contributed in a particular research field. Badenhorst (2014:19) submits further that the concerns with knowledge breaches is something peculiar to the academic environment; hence, all studious research is based on preceding research. In the latter regard, the review of literature could be seen as a continuing process throughout the entire research process (Anderson & Poole, 2014:21).

It is for this reason that Flick (2020:82) submits that the first step in reviewing literature focuses on identification of relevant secondary data pertinent to the particular topic in order to differentiate between what is already known from what is still unknown (gaps/breaches) about the topic (Kumar, 2014:48). Such differentiation can also improve, broaden and strengthen the researcher's knowledge base in the field of study. An effective search of previous or past and currently available literature in the field of study is enabled by the researcher's detailed understanding and organised analysis of both the research problem and its attendant questions, which presents an opportunity to separate truth from fiction,

gaps and contradictions (Bak, 2013:18; McDowell, 2013:5). Additionally, a literature review presents an opportunity for the researcher to analyse the strengths, weaknesses and shortcomings within the field of study. The current research explores the investigative value of cell phone record analysis when investigating serious and violent crime. The researcher consulted various sources of literature, including articles in newspapers and magazines addressing the above-mentioned subject matter of the study. However, these sources cannot be treated as scientifically proven literature (Flick, 2020:82).

For further scientifically proven literature, the researcher consulted search engines and databases (e.g., Google Scholar and ResearchGate), academic books, research articles in accredited journals, as well as unpublished and published dissertation and theses with related information on cell phone record analysis. The actual literature review process was preceded by a process of breaking up all the key concepts and compiling a list of headings and keywords in order to identify relevant literature that deals with the chosen topic under investigation (Bak, 2013:18; Kumar, 2014:48).

The researcher read both locally and internationally published literature and performed further internet searches on the research topic, including South African legislative and policy documents relevant to the use of cell phone record analysis when serious and violent crime is investigated. Upon identifying such literature, the researcher then processed it in order to determine whether it was relevant or not (Flick, 2020:83; McDowell, 2013:6).

2.4.2 Documentary review

Reviewing of literature and policies are classic examples of documentary research (Tight, 2019:15). As a method of (primary) data collection, the review of relevant documentary sources focused on the relevant legal and official policy frameworks applicable to the research topic. The following laws were deemed to be relevant and appropriately applicable in the study.

2.4.2.1 Constitution of the Republic of South Africa, Act 108 of 1996 (Constitution)

It is the supreme law within the Republic of South Africa (RSA) and prescribes powers of the State, and the rights of every individual citizen within the Republic (South Africa, 1996: 13).

2.4.2.2 Criminal Procedure Act 51 of 1977

The Act guides law enforcement agencies on how to perform their duties and also deals with various aspects of criminal investigation, search and seizures, and arrest with or without a warrant are a few to mention (South Africa, 1977:1).

2.4.2.3 Regulation of Interception of Communications and Provision of Communication related Information Act 70 of 2002 (RICA)

The Act is relevant to this research, since it addresses cell phone registration and communications, as well as with interception of communication and private information of the subscriber.

2.4.2.4 Electronic Communications and Transmissions Act 25 of 2002 (ECTA)

This Act deals with computer generated documents or printouts, such as cell phone evidence that is used in criminal investigations. Moreover, the ECTA regulates the evaluation and admission of data messages in criminal trials. The Electronic Communications and Transmissions Act 25 of 2002 (hereinafter referred as ECTA (Act No. 25 of 2002)).

2.4.2.5 Cybercrimes Act 19 of 2020

This Act came into effect on 1 December 2021 as a factor of the repeal of certain sections of the ECTA (Act No. 25 of 2002). This Act addresses offences which have an effect on cybercrime, and also criminalises the disclosure of potentially deleterious data messages. Moreover, this Act addresses the search and seizure of cyber related matters, including cell phones. The Cybercrimes Act 19 of 2020 (hereinafter referred as CCA (Act No. 19 of 2020)).

2.4.3 Interviews

The interview is one of the foremost methods of qualitative data collection (Aurini, Heath & Howells, 2016:80; Edwards & Holland, 2013:1). In research, the interview depicts a focused conversation or dialogue between a researcher and her/his participants, according to which the researcher elicits specific information from the participants with the aim of resolving the research problem, as well as addressing the aims, objectives and questions of the research (Cassell, 2015:1; Edwards & Holland, 2013:1). In order to derive maximum benefit from the interviews, the interview questions ought to be answered by participants (interviewees) who possess first-hand knowledge, experience and expertise in the field of study (Glenn & Gray, 2016:479; Luton, 2015:26).

Interviews could be in the form of emails, structured (i.e. formal), unstructured (informal), semi-structured (non-formal), individual (face-to-face), in-depth, in groups, telephonic, or virtual. Aurini et al. (2016:83), motivate that face-to-face interviews are the preferred (pre-Covid-19) methods of data collection, and are beneficial because they are conducted in real-time with less delay between asking a question and receiving a response thereof. Aurini et al. (2016:85), submit further that face-to-face interviews have potential benefits for researchers and participants insofar as they enable the sharing of the same physical space which can result in a better trust relationship, thereby, providing the researcher with an opportunity to observe conscious and unconscious non-verbal cues Aurini et al. (2016:85).

2.4.3.1 Piloting the In-depth Interview Research Instrument

Laws, Harper, Jones and Marcus (2013:89) emphasise that planning and drafting of research tools should be given careful consideration in order to reduce the time-consuming effects of conducting research. Accordingly, the researcher decided to pre-test (pilot) the in-depth interview data collection instrument. It should be noted that the terms, ‘piloting’ and ‘pre-testing’ are used differently by different research scholars and professionals. Whereas others view them as separate/different, others view these terms as synonymous and interchangeable (Schneider, Whitehead, LoBiondo-Wood & Haber, 2013:339; Tight, 2017:33). In this study, ‘piloting’ is used since the object of the study is not to test or select the viability of any particular data collection method above others.

Piloting the research instrument (in-depth interviews) is beneficial for testing whether the interview schedule will provide sufficient data to answer the research questions (feasibility and relevance) prior to the main study (Smith, Morrow & Ross, 2015:216). Therefore, pilot testing presents an opportunity to highlight and identify possible issues or misunderstanding in order to change the procedures. Necessarily, the identification of possible issues would involve multiple data collection runs to ensure both the research methods and the outcomes are valid and reliable (Tardi, 2019:8; Tight; 2017:33).

When pilot-testing a research (data collection) instrument, it is most important for researchers to maintain the same research design and procedures as those of the main study; and the selected participants should also be representative of the same population (Smith et al., 2015:220; Thomas, 2017:146). In this study, the researcher piloted the interviews with one (1) investigator, one (1) branch commander, and one (1) Prosecutor; all of whom were not part of the main study (Edwards & Holland, 2013:3). There were no significant issues that warranted any changes to the final interview schedule used in the main study.

2.4.3.2 Use of the in-depth semi-structured interview mode in the study

The researcher opted for the semi-structured interview mode to generate empirical data from the sampled participants following the successful piloting of the (preliminary) interview schedule. The researcher's initial preparation for these interviews involved the consultation and review of various literature sources on the topic under investigation to ensure sufficient understanding of the topic (Gray & Grove, 2021:441). The in-depth nature of the required data necessitated that a small number of these participants be selected in order to enhance data saturation independent of the numerical of individuals involved in this study (Cassell, 2015:4).

As such, the interviewees consisted of a small group of investigators who are representatives of the components involved in the policing and investigation of serious and violent crime in the greater Winelands District, WCP. It is also worth mentioning that the actual implementation of the in-depth interviews as part of the main study only occurred after the official granting of permission to conduct the study by the University of South Africa's Research Ethics Committee (UREC) and

the College of Law (CLAW). In addition to compliance with this ethical requirement for the internal institutional review, the researcher also ensured that informed consent form clearly disclosed or stipulated how the interviews would be conducted; as well as what was expected from the participants (Glenn & Gray, 2016:479-480). The latter issues are addressed further in Section 2.10 of the current chapter (see Annexure A). In worth noting, the researcher adhered to the prescribes of National Instruction Policy 1 of 2006 and obtained approval from the SAPS to conduct interviews with SAPS members stationed in the Winelands District, WCP and DPCI Western Cape (see Annexure B) (SAPS,2006). National Instruction Policy 1 of 2006. In addition, approval was also granted by the NPA to interview Prosecutors of the Winelands District, WCP (see Annexure C).

Both the construction or formulation and implementation of the in-depth interview adhered to the following general propositions and recommendations by authors such as Bryman et al. (2014:228), Laws et al. (2013:91), Martin (2016:40), Roulston (2014:298), UNISA (2016; 2020a; 2020b) and many others:

- The interviews were held face to face, some virtually and audio-recorded with the participants' consent. The Covid-19 protocols were adhered to at all times, thus ensuring the safety of the participant and the researcher;
- The researcher established a directive on the topic to allow a sequence for questions. The list of questions was compiled in relation to the research topic, but allowed each participant to express and provide their own answers according to their own knowledge and experiences;
- The interview schedule was flexible (not confined to sequence) and allowed the researcher some freedom to rearrange the order of questions and follow-up (probing) questions based on participants' answers;
- The researcher asked follow-up questions in instances when he was unsure of the participants' responses and meaning thereof. This allowed for the participant to provide more data;
- The researcher ensured that the formulation and structure of interview questions was not too specific, but clear enough for participant to answer according to their own knowledge and understanding;

- The participants' views and answers were respected, irrespective of the researcher's anticipation of 'correctness' or otherwise;
- The researcher used basic (uncomplicated) language that is understandable and applicable to participants, thereby constructing accurate, applicable and realistic questions;
- The researcher avoided leading questions which may contain the answer, and focused on open-ended questions to prompt further answers by participants;
- The researcher ensured confidentiality by withholding personal information of the participants, with each receiving a code name (e.g., "Interviewee/Participant 1", "Participant/Interviewee 2" and so on). This ensured that the interviewee's personal particulars are not revealed;
- The researcher made use of a place where noise was limited to avoid any distraction like an unoccupied boardroom, meeting room or office from where the participants were virtually interviewed due to the Covid-19 requirements for social distancing and no physical contact with participants (UNISA, 2016; 2020a; 2020b);
- The researcher wrote his field notes to capture the participants' unrecorded non-verbal expressions observed during the interviews; and
- The researcher collated all the audio-recorded verbatim responses of the participants together with his field notes for final review, transcript development and ultimate data analysis as the framework of the findings and required evidence of the study.

Finally, a complete record of the entire research and interview process (audit trail) was kept in order to enable the researcher's retrieval and provision of the necessary information when needed later (Martin, 2016:40). In that regard, the researcher stored all recordings, interview transcripts and schedules in the researcher's safe to ensure safety and access control for 5 (five) years following the research report's submission for final review to the researcher's academic supervisor. If any queries arise from the findings, the researcher is able to substantiate and corroborate these findings based on evidence from both available documentary and digital copies. The researcher has clearly marked and labelled all recordings by indicating the date and time of collection to assist the researcher's expeditious tracing of the recordings.

The researcher discusses his personal experience in the section below in relation to the data collection architecture of the study.

2.4.4 Personal experience

The researcher's own personal experiences and training do impact on several research aspects, such as their choice of approach, significance attached to the study, rationale for the study; as well as the nature of recommendations they were likely to propose (Creswell, 2014:20). The researcher's personal experience in this study is also a reflection of his familiarity with both the topic being studied and research problem whose alternative measures of resolution or intervention are being explored through the current research (Habib et al., 2014:9). The researcher currently holds a B-Tech degree in Forensic Investigation and a Diploma in Policing obtained from University of South Africa (Unisa).

The researcher has 17 years of service within the SAPS. He is also a Warrant Officer who previously spent fourteen years at the Local Criminal Records Centre (LCRC) as a criminalist and fingerprint expert, investigating serious and violent crimes (including murders) on a daily basis. The researcher's current duties include investigating and analysing cases of unidentified deceased persons by assisting the investigating officers to establish their identities. The researcher held several meetings with different investigating officers in the Winelands Police District based on the investigative value of cell phone analysis in the investigation of serious and violent crimes from January 2019 until December 2019 to evaluate the extent of the problem.

These meetings helped in informing the researcher about the investigating officers' challenges, such as the lack of clear guidance on how to complete the Section 205 application correctly and how to interpret and analyse cell phone records and data. Records of cell phones can be obtained in terms of Section 205 of the CPA (Act No. 51 of 1977) (South Africa, 1977:1). The investigating officers with whom meetings were held (between January and December 2019) do not form part of the current study's sampled participants. The researcher further established that the investigating officers only made requests for the "*seizure of the cell phone*", which

only allows for the cell phone to be seized. The wording “seizure of the cell phone” on the Section 205 application indicates only the seizure of the cell phone.

2.5 POPULATION AND SAMPLING

Factors such as time, logistical and cost or budget constraints prevent researchers from travelling to and from their selected interview sites and also involve an entire population in their studies (Bhattacherjee, 2012:65). As such, researchers are obliged to choose a sample that is representative of the population of interest in order to conduct a detailed examination and analysis of the research problem and its attendant research questions (Aurini et al., 2016:85). The population of a study relates to the total number of individuals who possess a homogeneity of qualities, features or attributes in which the researcher are interested in (Manly, 2015:7; Ruel, Wagner & Gillespie, 2016:124). According to Asiamah, Mensah and Oteng-Abayie (2017:1607), sampled participants themselves form part of the population, since they are selected from the very population on the basis of their representative characteristics or traits.

The participants form part of the population, which is the grouping of individuals with one or more features of interest. The ideal population in this study is all investigating officers in the SAPS; all Cell phone analysis experts in the SAPS; all Prosecutors from the NPA; and all forensic investigators from the Western Cape DPCI who is based in Bellville. The forensic investigators from the Western Cape DPCI work in their digital forensic laboratory and possess valuable knowledge of the topic under investigation. In total, the research population consists of 83 members from whom the target population was selected. The implausibility of involving all population members in the study have necessitated the researcher’s narrowing or reduction of the larger population and targeting a manageable group as a sensible strategy (Hennink et al., 2020:16; Rees, 2016:114). Further details of that targeted population are discussed hereafter.

2.5.1 Target population

According to Alvi (2016:10) and Majid (2018:3), a target population is the smaller sampled group that adheres to the specific criteria for a research study and best contributes to advancement of the study aim by sharing their knowledge and

experiences. Furthermore, the distinguishability and prominence of the target population is underlined by identifying and removing any ineligible individuals or prospective participants; that is, those who may not have the capacity to share their experiences, knowledge and perceptions to the level of clarity and depth required in the study (Asiamah et al., 2017:1613; Daniel, 2015:514). The researcher particularly chose the Winelands District, WCP, which is where he resides, and also where the researcher identified the research problem. Conducting this research in the Winelands District, WCP will be cost effective, practical and convenient for the researcher. The target population consist of WCP, Winelands District serious and violent crime investigators who conduct serious and violent crime investigations, Prosecutors who prosecute these type of cases, forensic investigators from the DPCI Western Cape who conduct cell phone related investigations and cell phone analysis expert. The DPCI is based in Bellville, Western Cape and services the entire Western Cape. Therefore, the researcher selected participants from the Western Cape DPCI.

The targeted population in this study consists of the following members:

- Serious and violent crime investigators in the Winelands District (forty-three (43) of which six (06) members was sampled);
- NPA Prosecutors from the regional Courts in the Winelands District (Eleven (11 of which two (2) members was sampled);
- Forensic investigators of the DPCI Western Cape (four (4) of which two (2) members was sampled);
- Detective branch commanders in the Winelands District (twenty-three (23) of which three (3) members was sampled); and
- Cell phone analysis expert in the Winelands District (one (1) member was sampled).

In total, the target population comprised of eighty-three (83) members, fourteen (14) of whom were sampled according to different techniques determined by the researcher as constituting the criteria for their inclusion in the study (Alvi, 2016:11; Denscombe, 2014:32). The next section discusses of the study's overall sampling framework, with the main emphasis placed on the various sampling methods used to select the various above-stated target group members.

2.6 SAMPLING

Ruel et al. (2016:123), define a sample as simply a subdivision of the entire population designed to select elements that will be used to make statements about the whole target population. Meanwhile, Alvi (2016:11), Grove et al. (2015:278), Hennink et al. (2020:17) and Kumar (2019a:290), are convinced that the purpose of sampling is to ensure that the carefully selected group of individuals possesses valuable information to cogently answer the research questions and render the overall findings as a reliable, valid and authentic testimony of the researcher's accurate interpretation of the sampled participants' perspectives.

In this study, two main sampling strategies or techniques were used, namely: simple random and purposive sampling. Both these techniques belong respectively to the probability and non-probability types of sampling (Babbie, 2014:94; Leavy, 2017:5), and are discussed below as they were applied for the various samples in this study. Most importantly, it is worth noting that sampling constitutes a significant instrument selection mechanism in research studies, since the population of interest may typically consist of many individuals for any research study to involve as participants (Majid, 2018:3). Therefore, the choice of a sampling method and its consequent sample size are motivated primarily by the need for relevance, information accuracy and reasonable representativity (Bryman et al., 2014:176; Denscombe, 2014:32; Vallabhaneni, 2015:165). Figure 2.1 below is reflective of the non-probability and probability sampling procedures for the study's various sample categories.

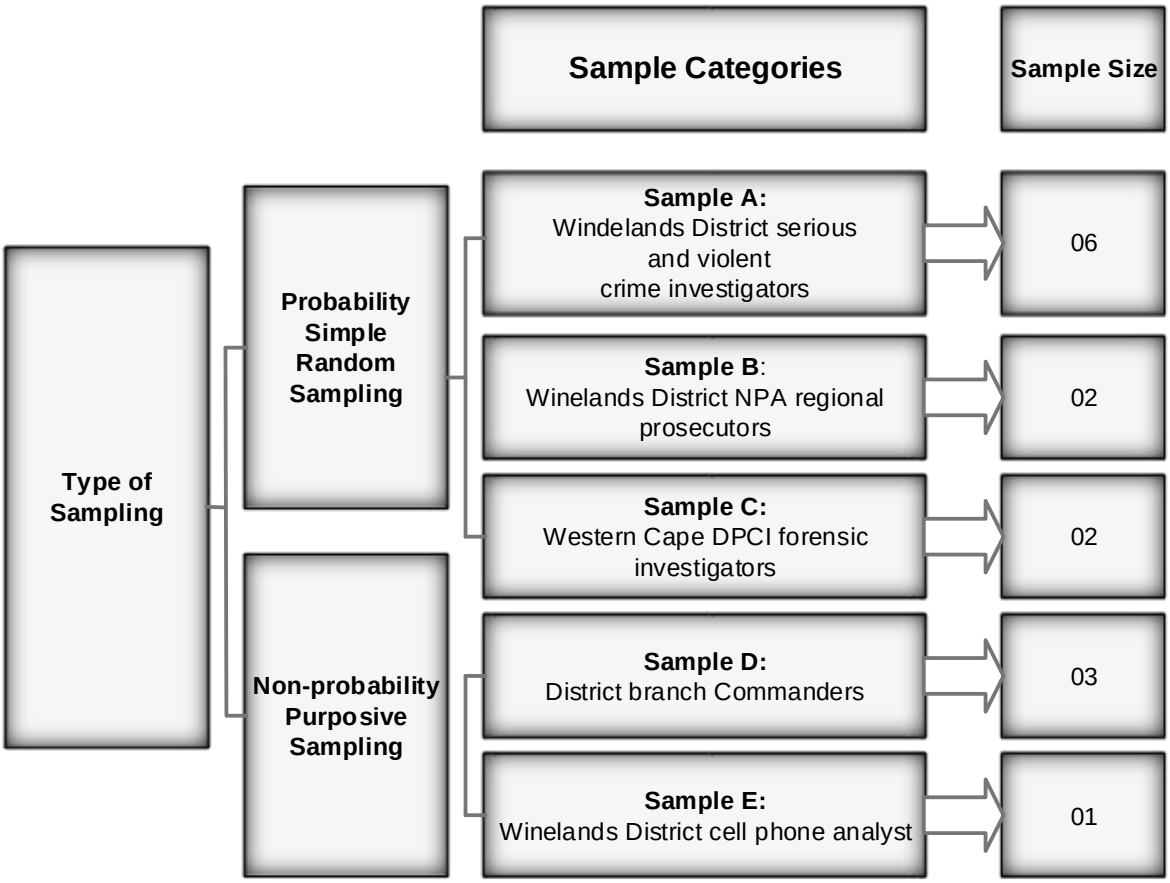

Figure 2.1: Probability and non-probability sampling in the study

(Source: Researcher's own compilation)

2.6.1 Probability sampling

In general, the probability sampling variants mostly derive from the principle of randomisation, which emphasises on the certainty of every individual population member's equal chance or opportunity of being included, which can even be known or predicted prior to such selection or inclusion (Chauvet, 2020:188; Ros & Guillaume, 2020:188; Ruel et al., 2016:123). The probability sampling methods are viewed as enhancing sampling representativity and also maintaining the most minimal sampling error possible (Bryman et al., 2014:170; Clark, Foster & Bryman, 2019:165). All methods of probability sampling methods are commonly characterised by the fact that every population unit has a known non-zero probability for selection, and inclusion of random selection during the process (Bhattacherjee, 2012:67). Probability sampling is viewed as ideal for studies that accentuate generalising as an important aspect of research. However, some other unique circumstances could also justify the implementation of non-probability sampling (Bhattacherjee, 2012:66-67).

For reasons that are commensurate with the aim of the study, the simple random variant of probability sampling was found to be most appropriately suited for this study.

2.6.1.1 Simple random sampling

As stated earlier, simple random sampling constitutes an example of the probability type of sampling (Bishnu & Bhattacherjee, 2018:268; Ruel et al., 2016:123; Vallabhaneni, 2015:165). Other probability (random) sampling methods include stratified random, systematic and multi-usage sampling. Ros and Guillaume (2020:188) and Bruce (2015:107) describe the simple random as the simplest, comprehensible and straightforward sampling technique with the potential for generalisability of the findings, since equal and fair chances of inclusion also enhance the degree of representativity (Bishnu & Bhattacherjee, 2018:268; Manly, 2015:8; Ros & Guillaume, 2020:188). When the selected sample represents the entire population from which it was drawn, the research findings were likely to be generalised to the entire population. To this effect, Manly (2015:7) and Ruel et al. (2016:125), assert that simple random sampling is essential when the researcher wants to draw inferences from the generalisations and basic assumptions made about the entire population based on the study results.

- **Implementation of the simple random sampling technique**

In the present study, the researcher applied the probability simple random method to sample suitable participants for involvement in the study as shown in Figure 2.1. Accordingly, **Sample A**, **Sample B** and **Sample C** were sampled through the simple random sampling method. Clark et al. (2019:166) and Rees (2016:114), propose that simple random selection may occur by placing names in a hat and then drawing names randomly. This may also take place by using a computer programme and selecting participants randomly. However, the researcher used cardboard box to replace the hat selection. The Winelands Police District consist of forty-three (43) serious and violent crime investigators. These investigating officers are responsible for investigating all serious and violent crimes within their respective Police jurisdictions in the Winelands District, WCP. The researcher made a list with all the names of these investigators and allocated a number from one (1) to forty-three (43).

The researcher wrote down these numbers on a piece of paper and placed them in a box, whereupon six (6) numbers were randomly selected. The investigators whose numbers were selected, formed part of the sample referred to as **Sample A**. All the participants were asked the same questions based on the interview schedule compiled (see Annexure D).

For the next sample, the researcher selected Regional Court Prosecutors from the NPA who prosecute serious and violent crime within the Winelands District, WCP. The NPA in the Winelands District consists of eleven (11) Regional Court Prosecutors whose duty it is to prosecute all serious and violent crimes within their respective Court jurisdictions. The researcher applied the same 'box random selection' approach applied for Sample A and drew a list with all the names of these Prosecutors and allocated them a number from one (1) to eleven (11). The researcher wrote down these numbers on a piece of paper and place them in a box or container, from where two (2) numbers were randomly selected from the box. The Prosecutors whose numbers were then selected and formed **Sample B** of the study. All the participants were asked the same questions based on the interview schedule compiled (see Annexure E).

For the next sample, the researcher selected forensic investigators from the DPCI in the Western Cape who work at their digital forensic laboratory. These forensic investigators are responsible for digital investigations on cell phones and computer related investigations in the Western Cape. The DPCI's digital forensic laboratory consists of four (4) staff members. The researcher repeated the sampling procedure already applied for Samples A and B by drawing up a list with all the names of forensic investigators and allocated them a number from 1 (one) to 4 (four). The researcher then wrote down these numbers on a piece of paper and placed them in a box, whereupon 2 (two) numbers were randomly select. The forensic investigators whose numbers were selected then formed **Sample C** of the study.

All the participants were asked the same questions based on the interview schedule compiled (see Annexure D). For reasoned considered to be relevant to this study, the researcher applied the non-probability sampling method for the selection of two other samples of the study; that is **Sample D** and **Sample E** as shown in Figure 2.1. This is discussed in greater detail hereafter.

2.6.2 Non-probability sampling

The non-probability sampling method entails that the chances or opportunities for prospective participants' selection are unknown, uncertain, uneven, or even improbable (unlikely) (Bryman et al., 2014:170; Clark et al., 2019:165). Non-probability sampling is also known as empirically oriented on account of its focused sampling of participants who are representative of a particular occupational or organisational grouping whose characteristics are of major interest to the researcher (Ros & Guillaume, 2020:188). The researcher applied the non-probability sampling on account of the targeted selection of participants with specific workplace knowledge and understanding of the topic under investigation. Since the researcher was known to most of the participants the non-probability mode of sampling was then viewed as also relevant since the researcher could not have known in advance who the sampled participants would be (Bryman et al., 2014:235). For reasons that are commensurate with the aim of the study, the purposive (judgemental or selective) variant of non-probability sampling was also found to be most suited for this study.

2.6.2.1 Purposive sampling

Simple random sampling constitutes an example of the probability type of sampling (Ruel et al., 2016:123; Vallabhaneni, 2015:165). Other probability (random) sampling methods include stratified random, systematic and multi-usage sampling. Purposive (selective or judgemental) sampling is a non-probability sampling type according to which the selection focus is on the researcher's own judgement, rather than on the randomisation of such selection or sampling (Daniel, 2015:522; Thomas, 2017:142).

According to Silverman (2014:60) and Thomas (2017:142), the sampled participants are not selected randomly, but strategically in terms of a case whose characteristics or features fit the researcher's requirements insofar as advancing the research problem and research questions is concerned. As such, purposive (judgemental or selective) sampling ensures that the researcher's possible bias could be critically mediated by the parameters of the case/s and the criteria required from the participants. Furthermore, purposive sampling also has an influential role where organisations or social processes are being studied, rather than cases of

individuals (Bryman et al., 2014:186; Daniel, 2015:522). Accordingly, the researcher uses purposive sampling and purposefully selects the participants of his study considering the set list of characteristics, whilst also considering the population characteristics and nature of the research question. It could then be concluded that purposive sampling is a technique in terms of which the researcher chooses or selects the participants on the basis of the inclusion standard of the study.

- **Implementation of the purposive sampling technique**

Whereas the simple random sampling strategy focused on the selection of Samples A, B and C, the purposive sampling variant was implemented in the selection of Samples D and E as explained below:

- Branch Commander of Stellenbosch detectives;
- Branch Commander of McGregor detectives;
- Branch Commander of Worcester detectives; and
- Cell phone analysist of Worcester SAPS.

The Winelands District, WCP consists of twenty-three (23) Branch Commanders who are responsible for managing investigators under their command within their respective Police jurisdictions. Branch Commanders are managers of the investigators under their command and have more experience, as opposed to investigators who are basically field workers. The researcher purposively selected the above-mentioned Branch Commanders of the detectives (Crime Investigation Department) according to their specific experience, knowledge and expertise in the sphere of cell phone record analysis. This group of Branch Commanders of the detectives (Crime Investigation Department) is referred to as **Sample D** and consists of three (23) participants. The Branch Commander of Stellenbosch SAPS resigned before the interview, and the researcher interviewed a senior member in the SAPS, who serves as a group leader at Stellenbosch detectives.

The group leaders are the senior members (managers/officers) who perform similar functions to those of a Branch Commander and is responsible for managing investigators under their command, overseeing investigations and provide guidance to investigating officers. All the participants were asked the same questions based on the interview schedule compiled (see Annexure D).

The Winelands District, WCP has one (1) cell phone analyst with valuable knowledge concerning the investigation of cell phone records where violent and serious crime has been committed. The researcher selected the above-mentioned individual based on the specific knowledge, experience and expertise in cell phone records analysis. This individual is referred to as **Sample E**. The participant is asked questions based on the interview schedule compiled (see Annexure F). The participant of this sample didn't agree to be interviewed, but instead completed the interview schedule. It is worth stating that the study combined both probability and non-probability sampling methods (i.e. simple random and purposive/selective/judgemental) due to the different categories of samples in respect of their job description and roles (Thomas, 2017:143; Ros & Guillaume, 2020:189).

It is of further noting that the first three samples (A, B and C) were selected with emphasis on random-ness, which emphasises the researcher's detachment from the final sample participants; whereas the selection of the final two sample categories (D and E) is more reflective of the researcher's own criteria which are still objective despite his familiarity and exposure to the research environment and participants (Bryman et al., 2014:236; Vallabhaneni, 2015:165). The next section discusses the data analysis procedures in the study.

2.7 DATA ANALYSIS

Qualitative data analysis relates to the methodical organisation, classification and categorisation of collected raw or verbal data for conversion into implicit and explicit statements of measurements and construction of sensible meanings according to the patterns or frequencies with which such raw data were translated or converted (Ary et al., 2019:456; Flick, 2015:5). In qualitative studies, information remains meaningless until it has been converted or translated into thoughtful ideas pertinent to the study field and its research problem and questions. Whereas data analysis is reflective of a post-data collection process, it is also possible to conduct both the collection and analysis of data concurrently, depending on the researcher's skills and experience (Babbie, 2017:397; Bhattacherjee, 2012:113).

According to Srivastva (2017:2) and Hennink et al. (2020:17), the fact that qualitative data analysis is interpretive in nature emphasises the possibility for the

concurrence of both data collection and analysis; as much as both analysis and interpretation of data could also be conducted concurrently, which still depends on the nous and savvy of the researcher. In qualitative data analysis, there is particular emphasis on “sense making” or understanding a phenomenon, rather than on explanations or predictions, which are the fundamental focus or preserve of quantitative analysis (Bhattacherjee, 2012:113; Harding, 2013:56).

The notion of ‘sense making” implies dependence on the researcher’s rhetorical or integrative ability and his/her personal engagement and knowledge of the research milieu and its social implications; as well as drawing inferences from which meaningful conclusions could be drawn (Srivastva, 2017:1). According to Srivastva (2017:2) and Hennink et al. (2020:17), the fact that qualitative data analysis is interpretive in nature, implies that the analytic process is not an end in itself, but a means towards the ultimate end of describing and explaining the meanings, thoughts, beliefs and experiences of the participants.

Following the collection of the in-depth interviews, the researcher transcribed the respective participants’ narrative statements in conjunction with the observational field notes in pursuance of the following thematic analysis process propounded by Babbie (2017:397), Bazeley (2013:63), Bryman et al. (2014:357), Harding (2013:56), Yin (2009), cited in Bryman et al. (2014:357) and other researchers:

- Downloading the recorded participant statements into digital mode and subsequently transcribing them on Excel sheets;
- Re-reading the transcripts and making notes of the frequently emerging or occurring patterns of narrated statements (themes);
- Comparing and listing themes according to individual or group codes;
- Reviewing the codes and listing them alphabetically, numerically or alpha-numerically (combination of alphabets and numbers;
- Translating the interrelated codes in respect of the study aim and discarding the redundant statements; and
- Preparation of the preliminary research report for authentication by main stakeholders.

Based on the interviews conducted with Sample “A” (six (6) serious and violent crime investigators), the background information gathered from the participants indicates that one (1) participant has been in the position for almost ten (10) years, one (1) participant held the position for more than seven (7) years, two (2) participants has been in the position for eighteen (18) years, one (1) participant held the position for nine (9) years. All of the above participants in the detective environment falls under the serious and violent crime (SVC) investigation group that specialises in serious and violent crime investigation. One (1) participant held the position for fourteen (14) years and serves as a general detective (due to non-specialisation) at the detective branch and the detectives investigate all reported cases. In worth noting, this differ from Police station to Police station and is due to the amount of manpower on the detective branch.

One of these participants in Sample A obtained a Diploma in Policing and two of these participants obtained a Bachelor Degree in Policing. Three of these participants holds no formal qualification. The participants underwent various courses in the field of investigations. When asked if the participants ever received any training regarding cell phone analysis or sim card analysis, all the participants responded affirmatively “no”. As result of their Police experience, most of the participants is self-taught on the field of cell phone record analysis.

Based on the interviews conducted with Sample “B” (two (2) Prosecutors), the background information gathered from the participants indicates that one participant served in the position for a period of twenty-six (26) years and holds a B.Proc. Degree, and completed over twenty (20) courses with a course in cell phone evidence. The other participant serves in the current position for a period of fifteen (15) years and holds a LLB Degree, and completed fifteen (15) courses with a course in RICA training. As result of their experience as Prosecutors, the participants is self-taught on the field of cell phone record analysis. Based on the interviews conducted with Sample “C” (two (2) digital forensic investigators from the DPCI), the background information gathered from the participants indicates that one participant serves in this position for ten (10) years and holds a National Diploma in Forensic Investigation, and the other participant serves in this position for fourteen (14) years and holds no formal qualification.

The participants completed a number of courses regarding digital forensic investigations and completed an international examination, whereby only seven (7) people are qualified in South Africa. Based on the interviews conducted with Sample "D" (three (3) Branch Commanders), the background information gathered from the participants indicates that one participant serves in the position for three (3) years and holds an Advanced Diploma in Management, Forensic Examination, Business Management and have certificates in financial investigations, Senior management certificate in management, public management and Executive Development Programme in Public Administration. Another participant serves in this current position for three years and holds a Diploma in Police Administration and a B-Tech in Policing and one other participant serves in the position for seven (7) years and holds no formal qualification. The participants underwent various courses in the field of investigations. When asked if the participants ever received any training regarding cell phone analysis or sim card analysis, all the participants responded affirmatively "no". As result of their Police experience, most of the participants is self-taught on the field of cell phone record analysis.

Based on the interview conducted with Sample "D" (cell phone analysis expert), the background information gathered from participant, indicates that the participant serves for more than ten (10) years in the current position and holds an M-Tech Forensic Investigations and Techniques. When asked if the participant ever received any training regarding cell phone analysis or sim card analysis, the participant responded affirmatively "no" and noted that the participant obtained an academic qualification and is self-taught in cell record analysis. The next section discusses data interpretation, which is essentially a post-analysis process. The emphasis on interpretation signifies that the analysis of data is not an end, but the means for finalising the reasons for which the study was undertaken in the first place (Creswell, 2014:26; Luton, 2015:33).

2.8 DATA INTERPRETATION

Whereas data analysis was more of a data-centred activity (data speaks for itself), data interpretation is viewed more as a researcher-centric activity in the process of transforming data in order to mine useful information and in terms of which the researcher's sense- or meaning-making skills are brought to the fore (Srivastva,

2017:2). To that effect, Willig (2014:136) propounds that interpretation is about what the researcher brings to the interpretative occasion; that is, this the argument that an interpretation states more about the interpreter than it does about the data that has been interpreted. It is in that regard that very dissimilar interpretations of exactly the same material could be created as a result of asking different questions on the same phenomenon. Therefore, every interpretation is underpinned by the interpreter's assumptions concerning what is significant, worth paying attention to, as well as known about the data (Willig, 2014:137). The interpretation of the findings entails building connections between themes and making reference to the overall salience of the findings in the context of the literature (Bryman et al., 2014:341; Corbin & Strauss, 2015:66).

In this study, the researcher allocated meaning to the findings by compiling their bibliographic details and contextualising them in respect of relevant aspects of the research topic. Furthermore, the researcher ascribed the thematically generated groups of the participants' responses to specific research objectives and questions (Willig, 2014:137). Most importantly, the grouped thematic responses were linked to specific literature references for corroboration or rebuttal (Bryman & Bell, 2015:401).

2.9 TRUSTWORTHINESS OF THE STUDY

Trustworthiness forms an integral part in qualitative research, in which case the term, 'trustworthiness' depicts the extent of the research findings' accuracy, truthfulness and that the study was worthwhile (Daniel, 2019:102). To achieve trustworthiness in qualitative research, the researcher must prove the truth value by providing a platform for testing the relevance of the research findings (Ary et al., 2019:442; Nowell, Norris, White & Moules, 2017:1). For Daniel (2019:103), the process for achieving trustworthiness in the outcomes of qualitative research also requires the prior systematic collection, organisation and interpretation of data, which then ensures the accuracy, verifiability, quality, usefulness and essence of the findings. The quality and trustworthiness standards in qualitative studies are determinable by means of the following criteria: credibility, transferability, dependability, and confirmability (Ary et al., 2019:442; Korstjen & Moser, 2018:120; Yin, 2016:86). These are discussed in greater detail hereafter.

2.9.1 Credibility

Credibility is an essential part of qualitative research, and relates to the truthfulness, accuracy, dependability and relevance of research findings (Ary et al., 2019:442; Daniel, 2019:103). Meanwhile, Bryman et al. (2014:44) and Bryman and Bell (2015:401), suggest that establishing credibility in the findings of research involves guaranteeing that the research study is carried out in accordance with good ethical practices. For Asiamah et al. (2017:1607) and Haven and Van Grootel (2019:237), credibility is at the heart of all research, and is strengthened when the analysis of data forms a solid foundation for the integrity of the self-same findings that the researcher wants to present.

In this study, the researcher strengthened the credibility of the study and its findings through member checking; that is, giving the participants ample time to scrutinise, review and to confirm whether or not the researcher has properly understood and represented what was discussed with him during the in-depth interviews (Daniels, 2019:104). From the viewpoint of this research, post-data analysis member checking could be viewed as a confirmation of the constructivist-interpretivist philosophical paradigm in terms of which a participant-centric interpretation of their experiences and knowledge is not only a matter of enhancing their representativeness; but also ensuring that the findings are credible and not wrought with the researcher's own predilections (Cho, 2018:7).

2.9.2 Transferability

According to Bryman et al. (2014:45) and Cho (2018:7), transferability is premised on the capacity of the research results to be applied from one context to another, each of which has its own group of participants. The implication is that for transferability to happen, the peculiarities of both the original context and the 'new' or another context should be similar to one another. However, there is also the view that in qualitative research, generalisability is rarely possible since the object of the study is to observe, understand explain a phenomenon's manifestation; rather than to quantify its representative occurrence (Alderson & Morrow, 2020:12; Eckhardt, 2018:75).

In this study, the researcher used thick descriptions to provide the reader with detailed contextual information about the research process and its consequent outcomes or findings (Edwards & Holland, 2013:5; Grove, 2021:131). The researcher further provided in-depth details of the exploratory, descriptive and analytic perspectives of both the participants and their environmental surroundings in order to adequately contextualise both the social world and the background information or factors that shaped their responses or understanding of the researched phenomenon.

2.9.3 Dependability

Dependability refers to the stability and consistency of the study results irrespective of the variability of the external environment, based on the notion that qualitative studies are seldom replicable, despite that they are repeatable (Eckhardt, 2018:75). That is to say, a study could be held in a different context, but the similarity of outcomes with its original site is hardly guaranteed. In this study, dependability was applied with the maintenance of the same methodology and interview questions for all sampled groups of participants (Cho, 2018:7).

It is also suggested that researchers should employ an auditing approach, which involves the process of keeping proper records of all stages of the research process (Bryman & Bell, 2015:403; Martin, 2016:34). This includes the problem formulation, the selection of participants for the study, all fieldwork notes and sketches, interview transcripts and recordings, and data analysis decisions. The latter authors suggest further that fellow researchers could fill the role of auditors who will review the research to ensure all processes were duly followed, notwithstanding the type of research being conducted. The researcher discusses confirmability in the next section.

2.9.4 Confirmability

According to Ary et al. (2019:448), the term confirmability in qualitative research relates to the degree of verifiability and validation of the research results by others who are more knowledgeable in the same field of study. Confirmability is also viewed as the extent of authenticity and accuracy of the research findings when viewed from the standpoint of the participants, and not simply the subjective views

and interpretations of the researcher (Rees, 2016:26). For Curtis et al. (2019:97), confirmability is more of an inspection process and analysis for data accuracy and impartiality. In this study, confirmability was applied through peer-debriefing, which is, providing a basis for external reviewers to inspect and examine the consistency of processes, and the objectivity of the research findings (Ary et al., 2019:442). While it enforces unbiased findings, the peer debriefing also ensures that the methodological cohesiveness of the study insofar as the agreeability of the findings and conclusions is concerned. The researcher consulted with experts in the cell phone analysis field who were not involved in the study for their opinions and views about the data collection and analysis processes on the one hand; as well as the compatibility of the findings, conclusions and recommendations on the other (Ary et al., 2019:442).

2.10 ETHICAL CONSIDERATIONS

The term, ‘ethics’ derives from the Greek word ‘ethos’, which translates as “character”, truthfulness, integrity, morality and fairness (Leavy, 2017:24). For Babbie (2017:62), Leavy (2017:24) and Mogorosi (2018:75), ethics are generally related with standards, practices, processes and principles of good and bad, right and wrong, which ought to be central in the planning and decision-making phase of the research in order to render such research acceptable and ethical. Greenfield (2016:46) and Israel (2015:3) further add that honesty must be a key prerequisite throughout every phase of the study and must be the foundation of the ethical codes and principles.

The ethical codes and principles themselves are a set of written or verbal rules which are clearly understood and agreed upon by parties involved in scientific research (Alderson & Morrow, 2020:6). In this study, the applicable ethical considerations are: internal review compliance; informed consent; confidentiality, privacy and anonymity; trust; and no harm to participants. These standards ensure that the dignity of the participants is maintained throughout the study and beyond its execution.

2.10.1 Internal review compliance

Creswell (2013:145) is of the view that obtaining authorisation to conduct worthy qualitative sampling and developing measures for recording information both electronically and on paper, and safekeeping the data are some of the ethical concerns that may arise. Gaining institutional ethical approval from the ethics committees compels the researcher to maintain high ethical standards throughout the study (Mogorosi, 2018:76). Accordingly, the researcher complied with ethical principles as provided for in UNISA's 2016 policy on research ethics in order to obtain ethical clearance from the ethical clearance committee of the UNISA College of Law (UNISA, 2016). Ethical clearance was granted for this study (see Annexure A). The entire dissertation is submitted for a Turnitin software to check and confirm the researcher's originality in his presentation of the final research report (see Annexure G). The researcher also applied for approval from the SAPS (see Annexure B) and the NPA (see Annexure C) to conduct this study with the sampled individuals within the respective organisations.

2.10.2 Informed consent

Informed consent entails that all participants must be fully informed about the research process and consequently agree to be involved voluntarily and uncoerced as competent or autonomous adult individuals (Ary et al., 2019:56; Bryman et al., 2014:124). Wasunna, Tegli and Ndebele (2014:57) advise that prospective participants should be sufficiently knowledgeable about all details of the research study and its consequences to them as individuals, before agreeing to voluntarily participate. Every participant must give voluntary informed consent to participate in the research. The prerequisites for informed consent are sufficient information, a good understanding and to make voluntarily decisions on whether to participate in a research study without undue influence (Wasunna et al., 2014:57).

Alderson and Morrow (2020:17) argue that voluntary consent from a human participant is completely essential and the capability to exercise free will of power to choose without any element of force, other ulterior forms of constraint of coercion, fraud, deceit, duress or overreaching. Kumar (2019b:65) argues that the participants should have sufficient and comprehensive information before giving their informed consent, but warned that the participants must be able to understand

the information provided to them. In that regard, Wasunna et al. (2014:58), argues that informed consent entails more than just simply obtaining the signature of the research participant. This entails a process which includes conveying precise and applicable information about the study, the purpose of the study, possible benefits, recognised risks, alternatives and processes, in a language which the participant understands.

In this study, participants were fully informed about the purpose of this study in order to make a sound and well-informed decision whether to participate or not. Furthermore, the data collection methods, and the assurance of confidentiality and anonymity is discussed. Flick (2015:34) state that the researcher may draw up an agreement which will be signed by both the participant and the researcher to address the issue of informed consent. The signed agreement included the time frames of the research and explanation of the use of the collected data. There was also an indication that they could withdraw from the study at any time of feeling uncomfortable, and they would not be penalised for doing so.

2.10.3 Confidentiality, privacy and anonymity

According to Babbie (2017:67), safekeeping of the participant's personal information and their identity is a huge research concern. Rees (2016:25) and Resnik (2018:149) explain that confidentiality is concerned with the assurance that delicate and private information is protected and withheld from undue publicly scrutiny and disclosure. Both confidentiality and anonymity can be achieved when the researcher does not publish any information which may compromise the identity of participants. On the other hand, anonymity relates to the protection of the participants' identity or the settings of the research by keeping such details and names secret, including characteristics, locations or any other element which may compromise those who are part of the study and providing information (Rees, 2016:6). The researcher did not at any moment publicly disclose the participants' particulars, such as their names, surnames and contact information. Instead, each participant was identified by a code name, such as "Participant 1", "Participant 2", and so on. Moreover, the researcher ensured that none of the participants' information and contribution would be publicised textually or otherwise without their written consent (Petrova, Dewing & Camilleri, 2014:7).

2.10.4 Trust

Trust in research plays a critical role when human participants are involved and is also essential to the success of research (Guillemin, Barnard, Allen, Stewart, Walker, Rosenthal & Gillam, 2018:285). However, there are on-going and diverse debates in the academic world about the definition of trust is. For Resnik (2018:88) and Rompf (2015:377), trust is displayed by having confidence in advance that individuals or groups of individuals will behave ethically and professionally and display competency of skills. Values related to trust include the capacity to keep a promise and all personal information truthful, reliable and confidential.

Resnik (2018:88) submits that trust encompasses vulnerability since the party who places trust in another, can be hurt, abused or exploited by the very same entrusted individual. Therefore, the individual who places trust in the other party ought to trust solely on the goodwill of the other individual being trusted (Guillemin et al., 2018:285; Resnik, 2018:149). In this study, the researcher ensured that a trustworthy relationship is formed with the participants by making full disclosure of the study in the informed consent form prior to the commencement of the interview sessions. Also, the researcher did not make any false promises beyond the scope of their involvement in the study.

2.10.5 No harm to participants

The risk of possible harm to participants is a major ethical issue in social sciences research, and researchers are obliged to guarantee that research is transparent, because research which is likely to harm participants is deemed unacceptable and unethical (Bryman et al., 2014:121; Flick, 2015:33). The harm can either be physical or emotional, harm to the development of the participant or self-esteem, harm of career prospects or future employment opportunities. Kumar (2019a:361) states that the participants' information ought to be used in a manner which will not be harmful to the participants either indirectly or directly. In this study, the researcher has ensured that the letter of request to SAPS included the use of SAPS office space that is sanitised, ventilated and free from outside disturbances or interferences during the interviews. Conducting the interviews in such safe environs ensured that the participant's privacy, confidentiality and anonymity were protected throughout their involvement with the researcher (Mogorosi, 2018:84).

In this regard, all possible risks to participants were reduced, especially from those of their colleagues who could have held contrary views to them in respect of the study and its intended purposes. The next chapter focuses on criminal investigations. The chapter explores, describes and analyses the nature of crime investigation in South Africa, as well as the role of the investigating officer and the Prosecutor. The chapter also discusses the principles, objectives, and evidence in criminal investigation.

2.11 SUMMARY

This chapter presented and discussed the methodological framework of the study in respect of the strategies, plans, techniques, research approaches and methods (research instruments) adopted and applied by the researcher to address the research problem, as well as its associated research questions and objectives. Moreover, the chapter highlighted the philosophical worldview offered in this study, in terms of which the constructivist and pragmatic worldviews were explored and discussed insofar as they apply to this research study.

Most importantly, the chapter presented the study's critical empirical framework in terms of which the methods and procedures for identifying the actual participants (sampling), the research setting; as well as the data collection instruments and data analysis and interpretation processes were highlighted and discussed. The case study research design approach was explored and adequately discussed by the researcher as a viable approach to the practical contextualisation of involving the selected participants in the investigation of violent crimes in the Winelands District, WCP through cell phone record analysis.

Moreover, this chapter outlined the relevant and applicable trustworthiness criteria on whose basis both the scientific and academic integrity and quality assurance of the study and its ultimate findings could be established. Furthermore, the chapter outlined the ethical protocols or considerations to which the researcher adhered throughout the research process. It is on account of these ethical protocols (considerations, principles or standards) that the dignity of the participants is maintained throughout the study and beyond its execution.

Overall, both the trustworthiness criteria and ethical considerations enabled the study's achievement of its stated objectives, while also solidifying its credibility and legitimacy within the research community.

CHAPTER 3: CRIMINAL INVESTIGATION

3.1 INTRODUCTION

The problem of crime is not *sui generis* (unique) to South Africa, but rather a global issue (Lochner, 2014:1). In that particular regard, crime is then prevalent in virtually every society, to the extent that its occurrence places great responsibilities on national governments worldwide to curb its spread from assuming and reaching the proportions of a national security threats or risk (Eterno, 2012:4; Lochner, 2014:1). Throughout history, societies and governments have established rules and laws to regulate the conduct and behaviour of citizens, with applicable penal measures meted against the law breakers or perpetrators of crime (Miller, Hess & Orthmann, 2018:5). Ideally, societies would be free of crime if the prescribed laws and rules were not breached or violated. Dutelle (2022:403) defines crime as the commission of an act which is forbidden by public law, with punitive or retributive measures prescribed against the transgressor for his/ her deeds.

Gardner and Krouskup (2019:1) maintain that crime scene processing is an inherent task in most criminal investigations, because it is often unlikely for a crime to be committed without a crime scene. The processing of crime scenes entails an examination and scrutiny of the scene of the perpetrated crime for the purpose of identifying, documenting and recovering of physical evidence found at the crime scene. Van Rooyen (2012:105) and Lochner (2014:2) believe that when a crime is committed, an in-depth criminal investigation should commence, and the assigned investigating officer should be guided by the rules of evidence in his/ her investigation of the particular scene. Meanwhile, Siegel and Mirakovits (2016:7) and Lochner (2014:1) opine that some degree of confusion is created by television crime series such as ‘Miami CSI (Crime Scene Investigation)’ and ‘NCIS (Naval Crime Scene Investigation)’ which portray the investigating officer as also being the crime scene investigator and forensic analyst who conducts the analysis of the exhibits found at the crime scene.

When viewed in a South African context, these are three distinct and separate functions. In practice, crime scene investigations and analysis of exhibits are two separate and specialised functions conducted under the aegis of the Division:

Detective and Forensic Services of the SAPS. Crime scene investigation is primarily the domain of the LCRC, whereas the FSL is responsible for analysing evidence collected on the crime scenes. Some of the LCRC and FSL functions overlap each other (Siegel & Mirakovits, 2016:7).

In the contemporary technology dominated era, the preponderance of cell phones and their concomitant subscriber explosion has necessitated that the investigation of certain forms of crime should entail the application of cell phone (mobile) forensics as part of the investigation process (Kumar et al., 2016:46; Skulkin, Tindall & Tamma, 2018:5, 6). A detailed cell phone billing record is generated when the subscriber uses the particular cell phone's network, which then records the activity and transactions of the cell phone (Zinn & Dintwe, 2016:328). In the case of a forensic crime investigation involving a cell phone, the investigator depends on the analysis of the suspect's cell phone records as the fundamental basis for resolving the committed crime. Accordingly, investigators request and analyse cell phone records of a specific suspect in a specific case. Depending on the nature of the crime committed, a forensic cell phone records analysis of the self-same crime and its modus operandi could even provide critical information for identifying and linking other suspects to the particular crime or alleged suspect; thus, helping investigators to solve current and previously unresolved cases (Kumar et al., 2016:46-47).

Given the critical value of cell phone record analysis in modern-day criminal investigation, this study focused on the exploration of the investigative value of cell phone record analysis in the investigation of serious and violent crimes in the Winelands District, WCP. Accordingly, this chapter then presents the role of the investigating officer and Prosecutor, followed by the analysis of criminal investigation and the objectives thereof; as well as the principles of criminal investigation and the collection of evidence. Such a trajectory of the chapter is intended to address the first research objective as appearing in Section 1.5 of Chapter 1 in this study, namely: to explore, describe and analyse the nature of crime investigation in South Africa. The role of the investigating officer is presented and discussed in greater detail hereafter.

3.2 THE ROLE OF THE INVESTIGATING OFFICER

In 1892, Sub-inspector Clarke became the first to occupy the building allocated for detectives in Pietermaritzburg, KwaZulu-Natal, and was tasked with the primary function of suspect tracing and the recovery of stolen goods and property (Lochner, 2014:5). In 1898, the first detective branch was subsequently established in KwaZulu-Natal under the leadership of its first commissioned detective, Edward John Tremlett (Lochner, 2014:5). Hess, Orthmann and Cho (2013:365), Lochner (2014:2, 8) and Turvey and Crowder (2017:9) describe an investigator or investigating officer as the trained professional assigned with the responsibility of conducting a careful and detailed examination or investigation of a particular incident, or crime.

The assigned investigating officer should operate within the respective legal and policy frameworks, as well as procedures within which he/she is duty-bound to firmly establish what happened, and who is responsible for committing the crime or incident that has happened. In addition, Sennewald and Tsukayama (2015:1) and Palmiotto (2013:6) describe investigating officers as seekers of truth and gatherers of facts and information to reconstruct the events about a specific crime that has occurred and draw conclusions based on the available (gathered) information. Meanwhile, Honders (2018:9) believes that it is nearly impossible for a single individual to solve a crime. In practice, the investigating officer in a case will be based at the local Police station, or specialised investigation units within the province such, as Organised Crime and the DPCI, to cite a few of the units. The investigating officer is responsible for the entire investigation. However, he/she uses investigative resources and aids, such as the LCRC experts, the FSL analyst, and the Digital forensic investigators/analyst to assist with specialised tasks relevant to the crime in question.

The role of the investigating officer has dramatically changed over the last decade. Amongst other influential factors, changes in the training and education of investigating officers have been induced by the fast development of technology worldwide (Lochner, 2014:1; Osterburg & Ward, 2015:5). Accordingly, criminal investigators are now better educated and trained in the science of detection, they also possess more knowledge concerning complex investigations, and are further

aware of the technologically-driven forensic support available to them (Honders, 2018:4; Lochner, 2014:1; Osterburg & Ward, 2015:5; Monckton-Smith, Adams, Hart & Webb, 2013:25). It is in this regard that Lochner (2014:2) upholds that successful investigating officers possess a particular set of skills, characteristics and qualities that separate them from their peers in the field of investigating crime.

Palmiotto (2013:6), Lochner (2014:5, 6, 9), Suboch (2016:1) and Houck, Crispino and McAdam (2018:16) describe the duties of the investigating officer as follows:

- To establish the nature and circumstances of a committed crime, and to follow a systematic process of identifying evidence, as well as collecting and presenting such evidence to reconstruct the event or incident;
- To collect and preserve physical evidence collected during the investigation process;
- The investigating officer must document the crime scene processing in respect of persons entering the crime scene, and the reasons for such entry;
- Tracing and interviewing of potential witnesses and obtaining written sworn statements, which the witness will present orally in Court;
- Follow-up leads obtained from witness account;
- Identifying and arresting the suspect and presenting prima facie evidence before Court that link the suspect with the crime;
- Retrieval of stolen goods and property;
- Presenting evidence in Court, either by sworn statements or exhibits collected during the course of the investigation; and
- Involvement in the prosecutorial process in order to assist the Prosecutor during Court proceedings – for example, transporting of witnesses to and from Court, bail hearings, presenting exhibits where needed, and obtaining further statement if required.

At paragraph 69 of *Motsagki v S* 2014 ZAGPJHC 260, the Court confirmed that the investigating officers should preferably participate in gathering and presenting evidence to Court, and actively assist the prosecution. In some instances, versions of evidence are disclosed for the first time during cross examination of State witnesses; or aspects of their evidence requires amplification, qualification or simple

explanation. Furthermore, the investigating officer should follow-up on these facts to determine the truthfulness thereof, and obtain further statements if required.

For participants in Samples A, B, C, D and E in the current study, their responses were sought in respect of the following question: “In your opinion, what are the responsibilities of an investigating officer with regards to cell phone record evidence?”

This was an open-ended question, and participants were free to respond in the context of their own understanding and opinions. They were not provided with the option of selecting a possible answer. Some of the participants submitted multiple responses.

Responses for Samples A, C, D and E are reflected as follows:

- Ten (10) participants indicated that the investigating officer needs to complete the Section 205 application;
- Eight (8) participants explained that the investigating officer should draft an affidavit with facts to support the Section 205 application;
- Eight (8) participants mentioned that the investigating officer should take a Section 205 application with statement/s to the Prosecutor for review and approval;
- Eight (8) participants stated that the investigating officer is duty-bound to submit the Section 205 application with statement/s to the Magistrate for final authorisation;
- Seven (7) participants mentioned that the investigating officer ought to take the approved Section 205 subpoena to the TSU for further handling;
- Six (6) participants submitted that the investigating officer ought to gather enough information regarding the suspected cell phone number prior to the Section 205 application for cell phone records;
- Two (2) participants explained that the investigating officer must identify the (potential) evidential value in the event that the cell phone records are linked to the investigation;
- One (1) participant noted that the investigating officer must take the Section 205 application to the Court for the signature of the appropriate judicial officer;

- One (1) participant stated that the investigating officer is solely responsible for handling of the Section 205 application for the purpose of obtaining the cell phone records;
- One (1) participant stated that it is the investigating officer's responsibility to analyse cell phone records; and
- One (1) participant mentioned that it is the investigating officer's responsibility to draw-up the necessary documents and submit them on time.

The responses in Sample B are reflected as follows:

- Two (2) participants stated that the investigating officer should draft an affidavit with facts to support the Section 205 application;
- Two (2) participants mentioned that the investigating officer needs to complete a Section 205 application;
- Two (2) participants stated that the investigating officer is obliged to submit the Section 205 application with a statement to the Magistrate for final authorisation;
- One (1) participant mentioned that the investigating should conduct a thorough investigation in order to present credible facts when submitting the Section 205 application;
- One (1) participant indicated that the investigating officer ought to take a Section 205 application with a statement to the Prosecutor for review and approval; and
- One (1) participant explained that the investigating officer is obliged to conduct a thorough investigation and gather enough information which must be placed in an affidavit.

The majority of the responses from the participants in Samples A, C, D and E cohere with the literature perspective by (Hunter, 2020:15), who explains that the investigating officer needs to complete an application for a Section 205 subpoena in terms of the Criminal Procedure Act/CPA (Act No. 51 of 1977), and that such subpoena is to be issued by the Court. The investigating officer can provide detailed parameters of the alleged crime to the cellular network service provider to narrow the request for the cell phone records, such as specific time frames during which the alleged offence occurred, or a request for cell phone records relating to a specific phone number that is already of interest to the investigation (Hunter, 2020:21).

Accordingly, the researcher concludes that the majority of the participants in Samples A, C, D and E have a good understanding concerning the responsibilities of an investigating officer with regard to obtaining cell phone records from the cellular network service provider. According to the researcher, the participants in Sample B have a good understanding of the responsibilities of an investigating officer with regard to obtaining cell phone records from the cellular network service providers. As such, their responses cohere with the perspective proffered by Hunter (2020:15).

A comparison of the Sample B and Samples A, C, D and E participants show a significant degree of similarities in their responses. Furthermore, the responses of participants in Samples A, B, C, D and E are mostly similar to those found in the literature in relation to Section 205 of the CPA (Act No. 51 of 1977), and are supported by legislation; that is, Section 205 of the CPA (Act No. 51 of 1977), Subsection (4), and Section 15 of the RICA (Act No. 70 of 2002). Only a High Court Judge, a Regional Magistrate, or a Magistrate issues a subpoena for any person who may be required to furnish the Court with relevant information of an alleged offence in order to justify the “seizure” of a mobile device for its records and data from the alleged perpetrator.

From a cell phone investigation viewpoint, the investigating officer can apply for the Section 205 subpoenas in terms of the CPA (Act No. 51 of 1977) in order to obtain cell phone records from the cellular network service provider. Thus, the investigating officer’s affidavit should contain facts pertaining to reasons for the requested cell phone records in the investigation. The investigating officer must also supply detailed facts of the person(s) of interest, reasons for his/her involvement in the investigated matter; as well as the specific time frames of the requested cell phone records. In addition, the investigating officers are responsible to hand over the Section 205 application to the relevant Prosecutor for further processing, recommendations and approval. Thereafter, the Magistrate or Judge will grant the final authorisation. Schönteich (2014:1) maintains that Prosecutors are the gatekeepers to the criminal justice system, and considers them to be the most powerful judicial officials. The role of the Prosecutor is discussed in greater detail hereafter.

3.3 THE ROLE OF THE PROSECUTOR

In terms of Section 179 of the Constitution (Act No. 108 of 1996), a single prosecuting authority should be established. The National Prosecuting Authority Act (Act No. 32 of 1998) provides the legal basis for the establishment of the National Prosecuting Authority (NPA). The National Prosecuting Authority Act (Act No. 32 of 1998) is (hereinafter referred as NPA (Act No. 32 of 1998). The NPA is an organ of the State, and is mandated to give effect to the laws of RSA. As an instrument of justice, the NPA should exercise its Prosecutorial roles independently and without any fear, favour or prejudice, which also accords with its constitutional obligation (National Prosecuting Authority, 2013:2, 3). The NPA is further mandated to exercise its power and responsibility by instituting and conducting criminal proceedings on behalf of the State, and also carry out any necessary functions related thereto (National Prosecuting Authority, 2013:3).

According to the NPA Act (Act No. 32 of 1998), the NPA is headed by the National Director of Public Prosecutions (NDPP), who has four Deputy National Directors reporting to him/ her directly (National Prosecuting Authority, 2013:3). Each of the country's nine provinces has a DPP who is responsible for prosecutions in both the high and lower Courts of South Africa. Below the DPP, are a number of Advocates and Prosecutors who are employed in the High Court, Magistrate and District Courts respectively. Prosecutors are indispensable representatives of the administration of justice, and should respect and protect human dignity; uphold and contribute to human rights; ensure that due processes are followed; and also maintain the smooth functioning of the criminal justice system (United Nations Office on Drugs and Crime/UNODC, 2014:1).

In that regard, Prosecutors have an essential role in protecting society from a culture of impunity and function as gatekeepers to the judiciary. Prosecutors are an important component of the prosecution process because they are lawyers of the community (UNDOC, 2014:1). Lawrence, Gourdet, Banks, Planty, Woods and Jackson (2019:1) report further that Prosecutors have developed partnerships with other entities, and are necessarily, held accountable for their actions and differing litigation strategies. It is expected from Prosecutors to deliver justice fairly in their decision-making, while balancing aspects of resources and budgets (Lawrence et

al., 2019:1). Owing largely to the sophistication of various crimes in the contemporary era, prosecutors are then compelled to work with increasingly voluminous amounts of digital and electronic evidence accruing from technologically driven communication improvements such as social media platforms (Lawrence et al., 2019:1). Prosecutors approach criminal investigations differently from investigating officers. As such, Prosecutors should work closely with the investigating officer by providing legal advice and guidance regarding the investigation; as well as training, where needed (Houck et al., 2018:75, 76).

According to the National Prosecuting Authority (2008:10; 2013:3), Schönteich (2014:1) and the UNODC (2014:1), the key roles of the Prosecutor are the following:

- Assisting the Court to pronounce a just and fair verdict, and in the event of a conviction, a fair sentence based on the evidence presented;
- Representing the community in criminal trials and ensure that the interests of victims and witnesses are promoted, without negating their obligation to act in a balanced and honest manner;
- Deciding whether or not to institute criminal proceedings against an accused person, and whether or not to withdraw charges or stop the prosecution;
- Deciding whether or not to oppose an application for bail, or to release an accused person who is in custody following arrest;
- Deciding about which crimes the accused person will be charged with, and in which Court the prosecution should be instituted;
- Deciding whether or not to enter into a plea or sentence agreement, whether or not the case should be diverted, or whether or not to accept a plea of guilty tendered by an accused person;
- Deciding about which evidence to present during the trial, and which evidence to present during sentence proceedings in the event of a conviction;
- Deciding whether or not to appeal to a higher Court in connection with a question of law, an inappropriate sentence, the improper granting of bail, or to seek a review of proceedings;
- Guiding the Police to collect the correct evidence, and presenting such evidence in Court, and arguing cases for the prosecution;

- Supervising investigators adherence to procedural rules, as well as involvement in bail hearings, plea and sentencing agreements;
- Deciding on alternatives for deviation of offenders to prosecution (especially juvenile first offenders), such as rehabilitation; providing support to affected victims of crime, and making sure that victims and witnesses are treated fairly; and
- Making recommendations regarding sentence and the supervision of the execution of sentences.

The Sample B participants were asked the following open-ended question: “In your experience, what is the role fulfilled by the Prosecutor in Section 205 applications regarding cell phones?”

This was an open-ended question, which allowed participants to respond freely and according to their own understanding and experience. No options were provided to the participants from which to select any possible answer. Some of the participants submitted multiple responses.

Overall, the Sample B responses are reflected as follow:

- One (1) participant noted that the Prosecutor needs to check whether the facts and reasons are proper and valid;
- One (1) participant indicated that the Prosecutor needs to make sure the application is correct and proper;
- One (1) participant noted that the Prosecutor’s role is to oversee the prosecutorial process and ensure its procedural fairness and lawfulness;
- One (1) participant explained that the Prosecutor’s role should be minimal;
- One (1) participant explained that the Prosecutor’s role is to instruct the investigating officer to apply for cell phone records;
- One (1) participant stated that the Prosecutor is duty bound to ensure that the rights of the accused are not being violated;
- One (1) participant mentioned that the Prosecutor must ensure that the Section 205 application is cogent enough to justify limiting the person’s Bill of Rights; and

- One (1) participant mentioned that the application for the Section 205 subpoena should be sent to the Magistrate, and that the Prosecutor cannot be involved because they (Prosecutors) are not part of the investigation. Otherwise, they become witnesses in the case they are prosecuting.

When comparing the responses of the participants in Sample B, it becomes clear that the responses agree with literature as indicated by authors such as the National Prosecuting Authority (2013:3; 2008:10), Schönteich (2014:1) and the UNDOC (2014:1), who assert that Prosecutor should only provide guidance to the Police. According to the researcher, the participants in Sample B have a good understanding of the role fulfilled by the Prosecutor in the application for Section 205 subpoenas to obtain cell phone records. One (1) participant particularly mentioned that the Prosecutor's role should be minimum in the process of obtaining cell phone records.

From the researcher's viewpoint, Prosecutors ought to guide, and not to facilitate the process, provide oversight, and ensure that the process is just and fair. The researcher compared the Sample B responses with the literature, legislation and the researcher's personal experience. It was found that there were elements and aspects of concurrence with the viewpoints raised by Hunter (2020:14), who submits that Section 205 of the CPA (Act No. 51 of 1977) permits a Police official, irrespective of seniority, to request the cell phone record data of any person, provided that such request is authorised by a Prosecutor or Magistrate. Correspondingly, Section 205 of the CPA (Act No. 51 of 1977) stipulates that the application for a Section 205 subpoena should be submitted to the Prosecutor or DPP for authorisation to obtain the required cell phone records. The Prosecutor or DPP will then duly recommend that the cell phone records may be obtained, after which the signed affidavit and application must also be presented to a High Court Judge, a Regional Magistrate or a Magistrate for review.

Although Prosecutors play an oversight role, the researcher concludes that their role is essential in requesting cell phone records from the cellular network service provider. Accordingly, Prosecutors could be viewed as the gateway to obtaining cell phone records from the cellular network service provider. The Prosecutor has an essential duty to seek the truth and present credible evidence before the criminal

Court. From the researcher's viewpoint, it is important for investigating officers to understand the objectives of criminal investigation, which are discussed in greater detail hereafter.

3.4 CRIMINAL INVESTIGATION

Stelfox (2013:7) and Tilstone, Hastrup, and Hald (2013:3) intimate that crime is basically concerned with people's behaviour towards each other, and that all criminal activity is also concerned with people because crime can only be committed by people. On the other hand, Hess et al. (2013:365) and Stelfox (2013:1, 20), state that criminal investigation is regarded as a one of the primary interventions to control crime. Criminal investigation is categorised into three main spheres, namely: establishing whether an offence was committed, the collection of sufficient and relevant evidence to submit before Court, and establishing the identity of the person responsible for committing such offence.

Criminal investigation is a step-by-step process of discovering, recording and collecting evidence and carefully analysing it for the purpose of establishing what happened and identifying the responsible perpetrator or person (Del Carmen & Hemmens, 2017:33; Hess, Orthmann & Cho, 2017:8; Lochner, 2014:6; Tilstone et al., 2013:3; Turvey & Crowder, 2017:9; Van Rooyen, 2012:13). Hess et al. (2017:8), mention that criminal investigation is a logical reconstructive process that utilises deductive reasoning for drawing cogent conclusions on the basis of particular facts and evidence. Applied in the criminal investigation realm, criminal investigation refers to the processes applied in collecting evidence and information about a crime or incident in order to establish whether a crime was committed; whether evidence was left on the crime scene and collecting such evidence; establishing the identity of the responsible person/persons involved; arresting the responsible perpetrator; and providing evidence before Court that could lead to the successful prosecution of the accused.

Criminal investigations instituted by law enforcement agencies occur either reactively or proactively. Reactive criminal investigations are largely characterised by instantaneous response to a crime situation or incident. Contrastingly, proactive criminal investigation occurs when an instant response is not an imperative, and law

enforcement agencies do not require approval from the prosecuting authority to initiate any investigations (Case, Johnson, Manlow, Smith & Williams, 2017:32; Davis, 2019:19). However, in terms of Section 205 (3) of the Constitution (Act No. 108 of 1996), the Police are mandated to investigate all crimes brought to their attention, which is consistent with preventing, combating and investigating all crimes.

The following question was posed to participants in Samples A, B, C, D and E: “In your understanding, how would you define criminal investigation?”

This was an open-ended question, which allowed the participants to respond freely and spontaneously according to their own understanding. No option was provided to the participants from which to select a possible answer. Some of the participants submitted multiple responses.

The participants in Samples A, C, D and E responded thus:

- Eight (8) participants explained that criminal investigation entails the investigation of a committed crime;
- Four (4) participants responded that criminal investigation is concerned with suspect identification and arrest;
- Two (2) participants mentioned that criminal investigations are concerned with gathering all available evidence;
- Two (2) participants averred that criminal investigations involve gathering of information and facts;
- Two (2) participants mentioned that criminal investigation is concerned with instituting a criminal trial against a suspect(s);
- One (1) participant commented that criminal investigation involves seeking for the truth;
- One (1) participant stated that criminal investigation is concerned with identifying elements of a crime;
- One (1) participant described criminal investigation as a systematic search for the truth to prove the guilt of a person before a Court of law;

- One (1) participant intimated that criminal investigation entails the lawful search for people and things (evidence) which can be useful in reconstructing an illegal act or omission;
- One (1) participant replied that criminal investigation is concerned with investigating a case properly;
- One (1) participant explained that criminal investigation is premised on solving crime;
- One (1) participant stated that criminal investigation includes placing the suspect before a Court of law;
- One (1) participant noted that criminal investigation includes upholding the law.

In addition, one participant indicated that a criminal investigation occurs when:

> "a case docket is registered and the case docket is criminal" and that "criminal investigation is where the South African Police Service gets involved to investigate crime" and to "investigate a case docket thoroughly, then send it to a Prosecutor, so the Prosecutor … can make an informed decision to prosecute or not".

The researcher agrees that, for a criminal investigation to commence, a criminal case docket must first be registered with the SAPS. Although the participant above did not accurately answer the question relating to a criminal investigation, this response does not entirely match the definition of a criminal investigation, but explains the process thereof. Correspondingly, Dutelle and Becker (2019:3) submit that criminal investigation refers to the processes associated with criminal investigation.

Meanwhile, the Sample B responses are reflected thus:

- Two (2) participants stated that criminal investigations are the gathering of all available evidence;
- One (1) participant mentioned that criminal investigations involve gathering of information and facts;
- One (1) participant explained that criminal investigation entails investigating a crime that was committed.
- One (1) participant stated that criminal investigation involves seeking for the truth;

- One (1) participant mentioned that criminal investigation is concerned with instituting a criminal trial against a suspect; and
- One (1) participant mentioned that criminal investigation includes a determination of the most useful evidence.

The researcher critically analysed the responses of the participants in Samples A, C, D and E and established that the majority of the participants have a good understanding of what criminal investigation entails. There were similarities in the participants' responses with some recognisable perspectives from the reviewed literature. The responses of the participants are supported by Hess et al. (2013:365), Hess et al. (2017:10), Lochner (2014:7) and McMahon (2014:3), all of whom explain that the primary goal of criminal investigation is to investigate and solve a crime by means of collecting subjective and objective evidence left behind on the crime scene. Additionally, criminal investigation provides a chance to identify and collect evidence that is required by the Court to hear and prosecute a particular case (Stelfox, 2013:16).

When comparing the responses of the Sample B participants, it is clear that these are in agreement with other literature perspectives as proffered by authors such as Dutelle and Becker (2019:30) and Stelfox (2013:16). According to the researcher, the participants in Sample B have a good understanding of what criminal investigation entails. Evidently, the above-cited participant extracts are emblematic of the participants' varying versions of understanding the concept, 'criminal investigation'. Notwithstanding the varied responses and understanding of criminal investigation by participants in Samples A, B, C, D and E, there are still essential elements of their definitions that cohere with the definition provided by Sennewald and Tsukayama (2015:1).

The latter authors point out that an investigation gravitates on studying, examining, searching, tracking and gathering factual information that leads to the resolution of problems and answering related questions. Irrespective of the type or purpose of an investigation, it is always based on the collection of factual information as the most vital aspect of solving a crime (McMahon, 2014:3). The researcher then concludes that each of the participants has his/ her own version of understanding the concept, 'criminal investigation', but their definitions are not peripheral to the

conventionally known perspectives as articulated by (Stelfox, 2013:16). When taking into account the responses from the research participants in Samples A, B, C, D and E, and those derived from the different authors, it becomes abundantly clear that criminal investigation is concerned with ascertaining whether or not a crime was committed, collecting sufficient and relevant evidence in order to establish the identity of the person responsible for the crime, and bringing such a person before Court to prove his/ her guilt or otherwise.

From a cell phone investigation point of view, the analysis of cell phone records as part of the investigation of serious and violent crimes can provide significant leads and evidence to assist the investigating officer in proving a case beyond reasonable doubt. Any successful criminal investigation derives from the investigator's consciousness and comprehension of the broader objectives of the particular criminal investigation attendant to the committed crime. The researcher explored the concept of criminal investigation, whose objectives are discussed in greater detail hereafter.

3.4.1 Objectives of Criminal Investigation

It is imperative for the criminal investigator to be adequately conversant with the objectives of criminal investigations, as well as their importance in the criminal investigation process. In that regard, Dutelle and Becker (2019:7), Lochner, Benson and Horne (2012:54, 71) assert that the primary objective of any investigation is to successfully investigate crime or offences by scientifically discovering relevant facts and revealing the truth in order to finally secure a conviction in Court against the offender. Therefore, the investigating officer ought to reconstruct the scene of the crime thoroughly in order to be successful in Court for having discovered the truth and answered the basic questions of what, where, when, why, who and how regarding the crime incident that transpired (Monckton-Smith et al., 2013:3; Reilly, 2019:2; Sennewald & Tsukayama, 2015:4).

According to Dutelle and Becker (2019:17), Hess et al. (2013:365), Hess et al. (2017:10) and Osterburg and Ward (2015:5 & 6), the primary objective of any criminal investigation are:

- Crime detection by establishing whether an offence was committed or not;

- Legally gathering objective and subjective evidence through investigation in order to obtain relevant or useful information;
- Suspect identification and arresting of the perpetrator;
- Recovery of any stolen property; and
- Presenting the best and completed case to the Prosecutor for prosecution, and testifying and assisting in the presentation of legally obtained objective and subjective evidence.

Participants in Samples A, B, C, D and E were asked the following question: “In your understanding, what are the objectives of criminal investigation?”

This question is open-ended, and allowed for participants’ freely and spontaneously expressed responses based on their own understanding. They were also not provided with the option of selection from a list of possible answers. Some of the participants submitted multiple responses.

The Samples A, C, D and E responses are reflected as follows:

- Six (6) participants stated that the objectives of criminal investigation entails obtaining evidence for successful prosecution;
- Four (4) participants mentioned that the objectives of criminal investigation entails establishing whether or not a crime was committed;
- Four (4) participants stated that the objectives of criminal investigation encompass the gathering of evidence to prove a person’s guilt;
- Four (4) participants stated that the objective of criminal investigation is to establish what happened and why it happened;
- Three (3) participants noted that the objectives of criminal investigation premise on suspect identification and arrest;
- Two (2) participants explained that the objectives of criminal investigation entail the recovery of any stolen property;
- Two (2) participants mentioned that the objectives of criminal investigation include searching for the truth;
- Two (2) participants noted that the objectives of criminal investigation include solving of crime; and

- One (1) participant mentioned that the objectives of criminal investigation require bringing the suspect to justice.

The Sample B responses are reflected as follows:

- One (1) participant explained that the objective of criminal investigation is to gather evidence to prove a person's guilt;
- One (1) participant stated that the objective of criminal investigation is to obtain evidence for a successful prosecution; and
- One (1) participant mentioned that the objective of criminal investigation is to seek for the truth.

After the researcher's critical analysis of the responses of the participants in Samples A, C, D and E, it was established that the majority of the participants have a good understanding of the objectives of criminal investigation. In that regard, the question was generally well answered by the participants, whose responses support the perspectives proffered by authors such as Dutelle and Becker (2019:17), Hess et al. (2013:365), Hess et al. (2017:10) and Osterburg and Ward (2015:5 & 6). Based on the responses of the participants in Sample B, it is evident that their viewpoints are in concurrence with literature perspectives of authors such as Dutelle and Becker (2019:17), Hess et al. (2013:365), Hess et al. (2017:10) and Osterburg and Ward (2015:5, 6). The researcher concludes that the participants don't have a good understanding of the objectives of criminal investigation. Their responses focused more on criminal law rather than criminal investigation.

With reference to the reviewed literature and responses from the Samples A, B, C, D and E participants, the researcher concludes that it is essential to firstly establish whether a crime was committed. Thereafter, the collection of evidence is an essential phase, followed by the identification and consequent arrest of the responsible person, and ultimately prosecuting the responsible person. In addition, the researcher concludes that the objectives of criminal investigation are important during the course of the investigation, and a systematic plan of action should be devised and followed in order to achieve these objectives.

From a cell phone investigation viewpoint, the investigating officer ought to obtain evidence in relation to the prescribed laws of the RSA. Section 205 of the CPA (Act No. 51 of 1977) allows the investigating officer to obtain private information, such as cell phone records of the person under investigation. An analysis of cell phone records could provide valuable evidence that leads the investigating officer to the arrest of the perpetrator and recovery of stolen property. The investigating officer may even establish the existence of a link or association between the co-accused or accomplices and the perpetrator. The collection of evidence allows for the investigating officer to present the best compiled case docket to the Prosecutor.

The following objectives of criminal investigation are discussed in order to address the research aim, research objectives and research questions in this study, namely: crime detection to establish whether an offence was committed; investigating and obtaining information and legally gathering objective and subjective evidence; suspect identification and arrest of the perpetrator; recovering any stolen property; presenting the most cogent and completed case possible to the Prosecutor; and testifying and assisting in the presentation of legally obtained objective and subjective evidence. The objectives are discussed in greater detail hereafter.

3.4.1.1 Crime detection to establish whether an offence was committed

Lochner (2014:7) maintains that criminal investigation is instituted when crimes are reported to the Police. In most instances, such crimes are reported to the Police by persons who are directly or indirectly involved in the crime (victims of the crime or witnesses) for investigation (Stelfox, 2013:18). Community members also report all their crime-related grievances to the Police, which necessitates that the Police officials should ascertain whether an incident is criminal or civil in nature (Joubert, 2015:32, 33).

According to Hess et al. (2013:366), Hess et al. (2017:15) and Siegel and Mirakovits (2016:39), there are three ways in which a crime is detected:

- The victim of the crime reports the crime to the Police;
- A witness to the crime being committed in his/her presence provides information to the Police about the crime; and/or
- The discovery of the crime in progress by the Police.

Hess et al. (2013:370) and Siegel and Mirakovits (2016:36), explain further that the Latin term, *corpus delicti* (which means “body of crime”) suggests that it should be proved that a crime was committed before any person’s conviction of an offence. In order to establish whether an offence has been committed or not, it is crucial for the investigating officer in particular (and Police in general) to have a broad understanding of criminal law and the elements of crime (Osterburg & Ward, 2015:6). In concurrence, Joubert (2015:46) states that the four general elements of an offence should materialise in order to establish whether or not a crime was committed. Furthermore, it is crucial for the State to prove that all four elements existed at the time of committing the crime, which ensures the conviction of the accused person/s by a Court of law (Joubert, 2015:86). Every crime is defined in the context of human conduct that must match the description or definition of the crime (Burchell, 2013:73).

Joubert (2015:86) further corroborates that completed crimes should entail the conduct of the accused person, which should meet all the requirements pertinent to the definition of that particular crime. The researcher is of view that it is imperative to adequately understand each category of crime and its attendant definition in order to establish the nature of the offence that has been committed. In practice, it is normally the task of the first responder to establish the nature and specific circumstances of a crime that has been committed. Hess et al. (2017:16) and Siegel and Mirakovits (2016:36), describe the first responders as the initial Police official attending to the crime scene.

The first responder can be either the patrol officer (visible policing member), the investigating officer or even a senior officer (Hess et al., 2017:12, 16). According to Palmiotto (2013:4), the first responder complements the investigating officer. Nowadays, investigating officers have a variety of investigating aids and resources at their disposal to enhance their criminal investigations (Courtney, 2012:20). In the context of cell phone investigations, the investigating officer can use digital investigators from the DPCI or War Room to assist with cell phone investigations. Additionally, the investigating officer can also apply for a Section 205 subpoena in terms of the CPA (Act No. 51 of 1977) in order to obtain cell phone records from the affected cellular network service provider.

Following hereafter is a discussion on another objective of crime investigation, namely: investigating and obtaining information and legally gathering objective and subjective evidence.

3.4.1.2 Investigating and obtaining information and legally gathering objective and subjective evidence

Amongst some of its functions, the law defines particular types of criminal actions and behaviours. The law also provides a framework for specific rules, regulations and processes that investigating officers should pursue in establishing the worth of any required evidence before prosecution can be instituted against the suspected individual (Stelfox, 2013:6). For Gardner and Krouskup (2019:1), the recovery and collection of physical evidence constitutes a major aspect of crime investigation, which also entails the analysis and evaluation of the crime scene itself. Anything recovered from the crime scene is considered an exhibit (Tilstone et al., 2013:10). Tilstone et al. (2013:10), add further that an exhibit is something that is presented before Court and serves as evidence. Meanwhile, Dutelle and Becker (2019:18) aver that objective and subjective evidence ought to be materially relevant and probative in order to prove a case beyond any reasonable reproach doubt.

Probative evidence rests on proving or disproving a fact or assertion Siegel and Mirakovits (2016:37), and is essential in the criminal investigation and prosecution phases to determine and prove the guilt or otherwise of a person (Hess et al., 2013:370). Impartiality and objectivity on the part of the investigating officer are an absolute requirement in determining and proving the innocence or guilt of an individual; which is sacrosanct for the maintenance of the integrity of the investigation and prosecutorial processes (Palmiotto, 2013:5). From the researcher's point of view, reaction time is of the essence in criminal investigation. Therefore, the longer the time it takes for the Police to arrive at the crime scene, the more the possibility exists that evidence or exhibits could either be lost or contaminated (Palmiotto, 2013:4).

To that effect, Dutelle and Becker (2019:17) propound that the reconstruction of the crime scene and search for the truth becomes insignificant when the exhibits of the committed crime are lost. Dutelle and Becker (2019:16) advise further that the

evidence should be collected as soon as it is discovered, marked and packaged to avoid contamination. Such a course of action is necessitated by the obligation on the part of the investigating officer to gather all the facts that may relate to solving the incident (Brown & Davenport, 2016:9; Palmiotto, 2013:6). According to Dutelle and Becker (2019:18), the investigating officer should only locate and identify the potential evidence and allow trained technicians to collect such evidence, while the forensic scientist will process the evidence. The value of an exhibit is not determined by its mere collection, but on the analysis of the exhibit to provide value to the investigation (Gardner & Krouskup, 2019:6).

Once the investigating officer has examined all evidence and interviewed possible witnesses, a working hypothesis ought to be established to determine the nature and circumstances of the crime incident or event (Dutelle & Becker, 2019:15). A hypothesis is an incomplete jigsaw puzzle that will be completed once the investigation is completed and supported by data (Dutelle & Becker, 2019:15; Osterburg & Ward, 2015:8). There is a greater need for investigating officers to think ‘outside the box’ and not only focusses on the basics of crime investigation. From the researcher’s viewpoint, the investigator should improvise but still stay within the framework of the law (Osterburg & Ward, 2015:3). In the context of cell phone investigations, digital evidence contained on a cell phone device contains information that could be relevant to the investigation of crimes (Belshaw, 2019:2).

Rapid advancements in information and communication technologies in modern times now provides law enforcement agencies with new possibilities for criminal investigation. In that regard, a cell phone has become an essential tool in the investigation of crime – also considering their preponderant use in the various sophisticated forms of crime (Ali, Abd Razak, Othman, Mohammed & Saeed, 2017:1; Lochner & Zinn, 2014:161). According to the Lochner Principle, the presence of a cell phone signal at the crime scene as a trace implies or suggest that the evidence of such signal is only found in an electronical database of the cellular network service provider (Lochner, 2014:7; Lochner & Zinn, 2014:160). The electronic evidence itself is stored and kept at an offsite location away from the crime scene.

Lochner and Zinn (2014:161) state that the cellular network service provider's database always configures the geographical location of an active cell phone device electronically, regardless of the cellular network initiating or receiving a call, sending or receiving an SMS notification; or by automatic continuous registration of the cell phone device – whether or not the subscriber is using the device for communication at the particular time. Therefore, the geographical location system is important for placing or positioning the device within the proximity of the place at which the alleged crime was committed (Lochner & Zinn, 2014:161). The only prerequisite for connecting or linking the cell phone device to the scene of a crime is that the device in question is switched on for the trace to be left on the computer database (Lochner & Zinn, 2014:161). Moreover, any conclusions and findings must be based on factual information and evidence (Palmiotto, 2013:5). The ensuing section focuses on a discussion concerning another objective of crime investigation, namely: suspect identification and arrest of the perpetrator.

3.4.1.3 Suspect identification and arrest of the perpetrator

One central problem in criminal investigation relates to establishing the identity of the alleged crime's perpetrator (Kruse, 2016:6). In the pre-arrest phase of the investigation, the Police will investigate the reported incident to establish whether or not an offence was committed with the view to determining any possible criminal prosecution (Stelfox, 2013:18). The investigation process allows for legal and ethical information and evidence gathering in order to establish the identity of the responsible perpetrator (Kingshott, 2015:92). Once the identity of the perpetrator is established, the Police may arrest the person and placed him/her before Court. Solving a crime has different meanings and implications to different people. In that regard, the preliminary crime investigation presages the actual criminal committed (Palmiotto, 2013:14). The community may believe that a crime is solved once the perpetrator/s is/are identified and arrested, which is a depiction of one of the broader objectives of a criminal investigation (Dutelle & Becker, 2019:17).

In the latter regard, an investigating officer has an obligation to determine the identity of the perpetrator, subsequently arrest him/her, and bring him/her to justice (Lochner, 2014:6). It is essential for investigators to establish the nature and circumstances of the crime that has been committed, if any, and then seek evidence

in a systematic manner to establish the identity of the perpetrator and ultimately apprehend such perpetrator or suspect - which is considered the primary goal of criminal investigation (Hess et al., 2017:10; Osterburg & Ward, 2015:7, 8).

Saravanan, Thayyil and Narayanan (2013:125) state that an essential phase of a criminal investigation is to identify suspects involved in the crime. According to Fish, Miller, Braswell and Wallace Jr. (2015:15), when physical evidence is correctly identified, collected, preserved and analysed, such evidence could link or connect the perpetrator to the victim or crime scene. Osterburg and Ward (2015:9) state that the linkage or connection is achievable by means of fingerprints; finding stolen property in the possession of the suspect, or by means or physical characteristics such as the physical description of the suspect/perpetrator by the victim or eyewitness. When the victim or eyewitness knows the identity of the suspect but unable to provide the suspect's location, other records and information may provide sufficient information regarding the suspect's location and the possible modus operandi of crimes committed previously (Osterburg & Ward, 2015:9).

Engel, Worden, Corsaro, McManus, Reynolds, Cochran, Isaza and Cherkauskas (2019:1) state that Police officers play a very important role of activating the criminal justice process and through their authority in the arrest of perpetrators of crime. The power of arrest is vested on Police officials without having to first obtain a warrant of arrest. However, the arrest of any individual ought to be executed lawfully, when and where a crime is committed (Africa Criminal Justice Reform, 2019b:1). In addition, such arrest is intended to place the suspected individual or perpetrator under the custody of a law enforcement authority for the purpose of interrogation and/or prosecution (Del Carmen & Hemmens, 2017:35; Dutelle & Becker, 2019:20).

There are two kinds of arrest – an arrest with a warrant, and an arrest without a warrant (Del Carmen & Hemmens, 2017:35). Section 39 (1) of the CPA (Act No. 51 of 1977) provides for both types of arrest, and further stipulates that the arresting officer shall at the time of the arrest or immediately thereafter, inform the arrested person of the cause of the arrest, or provide a copy of the arrest warrant if the arrest was effected by means of a warrant of arrest. The Second-hand Goods Act (Act No. 6 of 2009) provides that the Police may arrest a dealer and buyer of stolen goods. In *Gosschalk v Rossouw* 1966 (2) SA 476 (C) at 490 – 493, the Court held that

when the Police have legally acquired access to a suspect, either by means of legal arrest or by permission from the suspected person, he/she may be questioned within reasonable and lawful limits. In terms of the Constitution (Act No. 108 of 1996), an arrested person should be informed of his/her constitutional rights immediately upon arrest. Del Carmen and Hemmens (2017:38) report that the arrested person ought to be detained at the nearest Police station and brought before Court as soon as possible. Moreover, the arrested person should also be brought before a Magistrate or Judge without any delay. Upon the arrest of a perpetrator, the Police have a duty to identify and collect all stolen property. Joubert (2015:141) maintains that an individual's property (provided it is not stolen) is a great asset, and the law seeks to protect the property rights of all individuals. The next section discusses another significant of criminal investigation, namely, the recovery of any stolen property.

3.4.1.4 Recover of any stolen property

The description of stolen property is essential when identifying recovered property, and should be drafted in the statement provided by the victim in order to assist the Police in determining ownership once such stolen items have been recovered (Osterburg & Ward, 2015:8). In such instances, it is crucial to document every detail accurately (Sammons, 2012:34). Victims of crime should also provide detailed descriptions of the make, model, serial numbers, and other unique distinguishable characteristics of the stolen items that could possibly assist the Police in their investigation (Osterburg & Ward, 2015:8). In *Mahlangu v S* 2019 ZAGPPHC 35, the witness identified a stolen cell phone by recognising the scratches found on the cell phone. It is the researcher's contention that complainants should provide detailed descriptions and serial numbers where possible, as proposed by Osterburg and Ward (2015:8).

Osterburg and Ward (2015:8) illuminate that the tracking and recovery of stolen property could be facilitated by the Police enquiring at places such as pawnshops, second-hand dealers, flea markets and even investigate via the Internet. These are the most common places where stolen items and other forms of contraband are found. In *S v Mani* 2002 (2) SACR 393 (E) and *S v Siebert* 1998 (1) SACR 554 (SCA), the Court convicted the offenders for receiving stolen motor vehicles with full

knowledge that such property (motor vehicles) was stolen. The accused were found guilty in terms of Section 37 of the General Laws Amendment Act (Act No. 62 of 1955).

Furthermore, Section 37 of the self-same Act (General Laws Amendment Act (Act No. 62 of 1955)) and the Second-hand Goods Act (Act No. 6 of 2009), stipulate that any individual who acquires, receives or possesses stolen goods without reasonable cause to believe that such goods or property are those of the person handing the very goods to him/her, or that the owner provided authorisation to dispose or deal with such property, shall be guilty of an offence. Therefore, the Police may arrest the individual who obtains/obtained such stolen goods or property and seize such property.

In terms of Section 36 of the General Laws Amendment Act (Act No. 6 of 2009), any individual who is apprehended with any goods in his/her possession and is unable to provide a satisfactory explanation for the property in his/her possession, and where reasonable suspicion exists that the property may have been stolen, such individual will be guilty of an offence and will be liable on conviction to the penalties which may be imposed on such conviction of theft. In that regard the Police may arrest such a person, and seize the stolen property as evidence. In *Sebaka v S* 2019 ZAGPPHC 196, the accused pleaded guilty of unlawful possession of property/ goods knowingly. In another case, *Khanye v S* 2017 ZAGPJHC 251, the accused were found in possession of stolen property with the full knowledge that such property belonged to Pep Stores. As such, the accused persons in both matters were found guilty of theft under Section 36 of the General Laws Amendment Act (Act No. 62 of 1955).

Section 20 of the CPA (Act No. 51 of 1977) lists certain articles and items which the Police may seize in the event that an offence may have been committed, and may provide evidence that such offence or suspected offence has been committed, and where it is suspected that such items may be the proceeds of an offence. Section 21 of the afore-sited Act allows for the seizure of articles listed in Section 20 of the self-same Act with a search warrant. However, Section 22 of the CPA (Act No. 51 of 1977) stipulates that a Police official may seize items listed in Section 20 (of the

same Act) without obtaining a search warrant on the basis that the person concerned provided consent to such search and seizure.

Dutelle and Becker (2019:21) note that the success of a case of theft or stolen property depends on the probative value of the evidence collected and presented before Court. In the next section, the researcher discusses another objective of criminal investigations, namely: testifying and assisting in the presentation of legally obtained objective and subjective evidence.

3.4.1.5 Testifying and assisting in the presentation of legally obtained objective and subjective evidence

Osterburg and Ward (2015:8) proffer that investigating officers should always investigate each case on its merit when tried before Court. Therefore, it is required of the investigating officer to follow due processes and procedures when investigating a case. The investigating officer should be able to identify the nature of evidence required in order to establish the issue of guilt, and whether such evidence will prove the State's case beyond reasonable doubt (Dutelle & Becker, 2019:21; Hess et al., 2017:8). Part of the investigating officer's duty is to collect all available subjective and objective evidence, while the Prosecutor and the Court establishes the significance and relevance of the evidence (Dutelle & Becker, 2019:21; Joubert, 2015:43). Meanwhile, Case et al. (2017:56), state that the Police and the prosecution authority can bring suspected persons or perpetrators before Court on suspicious of committing a crime, and have a case to explain before the Court. The partnership between the Prosecutor and the investigating officer is important insofar as presenting a well prepared case to the Court is concerned (Joubert, 2015:43).

The Prosecutor relies on the evidence and information obtained by the investigating officer in order to make appropriate decisions regarding the particular case, and deciding on the prosecution or otherwise (Joubert, 2015:43). In Paragraph 65 of *Motsagki v S* 2014 ZAGPJHC 260, the Court held that a Prosecutor cannot present a case before Court through randomly selected facts. Moreover, the Court held that such practices (of randomly selected facts) are unfair towards the Court, and undermine the very aim of a fair trial. For this reason, the investigating officer should ensure that all factual evidence is obtained and filed. Given the need for proper

documentation and preparation of evidence, it is the imperative for the investigating officer to present the best possible case to the Prosecutor, also obtain statements where required.

Joubert (2015:44) intimates that the completed case docket ought to be submitted to the Prosecutor for the review of evidence and information. It is a truism that the Prosecutor will only prosecute a case when there is prima facie evidence. Del Carmen and Hemmens (2017:56) describe prima facie evidence as a case whose merits are strong and reliable enough to succeed, and not contradicted by the opposing defence counsel. In such instances, the Prosecutor will identify and establish a strategy of presenting evidence in Court (Fish et al., 2015:11). In *S v Ntsele* 1998 (2) SACR 178 (SCA), the Court held that the onus rests on the State to prove the guilt of the accused beyond reasonable doubt in a criminal case, and not beyond all shadow of doubt.

Dutelle and Becker (2019:21) state that all evidence has a particular predicate that should be fulfilled before its submission as evidence in Court. These above cited authors maintain that any item of evidence will have no bearing on the outcome of the trial, although handled, labelled and package in accordance with the rules of evidence, if the probative value is lacking. Once evidence has been admitted and constitutes part of the Court record, it may influence the outcome of the trial based on the probative value it presents. In the context of cell phone investigation, the investigating officer has to testify on the process followed in obtaining the Section 205 subpoenas in terms of the CPA (Act No. 51 of 1977) for the purpose of obtaining cell phone records from the affected cellular network service provider.

The investigating officers should also provide details of the manner in which such evidence was identified, documented, collected and preserved; as well as the arrest procedure leading to the matter being presented before the Court. Osterburg and Ward (2015:10) explain that the testimony of a witness is only effective once it is deemed credible by the Court. Therefore, credibility is established when facts are placed before Court in an impartial and objective manner. According to Home Office (2020:6), as a general rule, honesty and impartiality are part of expected behaviour and conduct when giving evidence. Investigating officers should follow the advice of Home Office (2020:9) and Fish et al. (2015:11), which accentuates the

importance of witnesses to review their statements and notes made during the course of the investigation before presenting evidence in Court. Furthermore, the investigating officers should understand the law of evidence and cross examination procedures in the questioning of a witness by the opposing sides (Prosecutor or defence) during trial (Osterburg & Ward, 2015:10; Swanepoel et al., 2014:261). The researcher is of the view that the investigating officer is tasked with gathering of facts and evidence legally. The evidence is then placed into the case file and presented to the Prosecutor, who will present such evidence in Court. Characteristically, the evidence should include exhibits, objects, photographs and documents, amongst others. It should also be noted that criminal investigation is based on certain principles that should be adhered to, in order to achieve successful criminal investigation. In order to address and achieve the research aim, objectives and questions of this study, the researcher discusses the two primary principles of criminal investigation in greater detail in the ensuing section.

3.5 PRINCIPLES IN CRIMINAL INVESTIGATION

According to Lochner (2014:2), criminal investigation is based on two prominent principles which serve as the foundation of criminal investigation, namely: the principle of individuality and the Locard Exchange Principle. However, due to technological developments, the Lochner Principle also warrants mentioning. Edmond Locard is considered by many scholars in this field to be the founding figure and father of the modern-day crime laboratory and forensic science (Gardner & Krouskup, 2019:21). Miller (2018:13) and Houck et al. (2018:27), mention further that the foundation of criminal investigation is based on the Locard Exchange Principle. The researcher explored various principles of criminal investigation and found it necessary to discuss each of these in greater detail in order to determine their importance in the criminal investigation process. The researcher is of view that the Locard Exchange Principle and the Lochner Principle play important roles in criminal investigations. These principles are discussed in greater detail in the next section.

3.5.1 The Locard Exchange Principle

The French scientist, Edmond Locard is considered one of the founding persons in forensic science which encompasses the Locard Exchange Principle founded in the

early 1900s. Dutelle and Becker (2019:9) further confirm that the work of Edmond Locard beginning in the 1900s, was foundational to theories on criminal investigations. According to the Locard Exchange Principle, when two objects come into contact with each other, the cross-transfer of evidence will inevitably occur. As such, Locard believed that every suspect, victim or witness can be connected to the scene of a crime in one way or another; which has widely become known as the Locard Exchange Principle (Dutelle & Becker, 2019:9). The Locard Exchange Principle could then be summarised according to the following maxim: “every contact leaves a trace” (Roncacè & Nicosia, 2016:1008; Gardner & Krouskup, 2019:21).

Hess et al. (2013:370) and Hess et al. (2017:16), maintain that considerations of crime scene preservation and investigation require an understanding of the Locard Exchange Principle. This exchange principle postulates that when two objects come into contact, they exchange residual traces on each other. Based on this principle, it is highly improbable for criminals to commit a traceless crime, particularly when considering the intensity of the crime in question (Gardner & Krouskup, 2019:21; Roncacè & Nicosia, 2016:1008). On the other hand, Robertson, Vignaux and Berger (2016:1) believe that “every contact leaves a trace”. However, this quote is misplaced, because Edmond Locard did not make such a claim.

According to Lochner and Zinn (2014:161), most investigators based their investigations on the Locard Exchange Principle as the starting point in searching for traces of evidence in the area where the alleged perpetrator has made contact with objects, places, or persons at the crime scene. From a cell phone investigation perspective, the cell phone records of a particular device are not left at the scene of crime because cell phone evidence pertains to the invisible traces that are located, captured, and stored with the network service provider at an offsite location that is not part of the crime scene.

Lochner and Zinn (2014:161) are of the view that in modern-day crime investigation and crime scene management, the Locard Exchange Principle still forms the foundational basis of searching for evidence. The Locard Exchange Principle was formulated in 1926 and still have significance, but was formulated decades before

the technological developments and improvements that constitute a modern society.
For participants in Samples A, B, C, D and E, the following question was posed: “In your understanding, how would you describe the Locard Exchange Principle?”

This was an open-ended question, in terms of which the participants were free to respond according to their own understanding. The participants had no other option of selecting their responses from a list of possible answers. Some of the participants submitted multiple responses.

The responses in Samples A, C, D and E are reflected as follows:

- Six (6) participants explained that the Locard Exchange Principle arises from the notion that two objects coming into contact inevitably exchange traces that are left on both objects;
- Three (3) participants noted that the Locard Exchange Principle involves someone leaving a trace in the form of touch DNA or fingerprints;
- Two (2) participants stated that the Locard Exchange Principle could be summarised as every trace left during a contact; and
- Two (2) participants did not know what the Locard Exchange Principle refers to.

The responses in Sample B are reflected thus:

- One (1) participant did not know what the Locard Exchange Principle refers to;
- One (1) participant explained that the Locard Exchange Principle is based on the view that when two objects come into contact, an exchange of their traces are left on both objects; and
- One (1) participant noted that the Locard Exchange Principle involves someone leaving a trace in the form of touch DNA or fingerprints.

Evidently, a comparison of the responses of the participants in Samples A, C, D and E shows that the majority of the participants agree with the dominant literature perspectives as indicated by authors such as Robertson et al. (2016:1) and Suboch (2016:1). These authors emphasise the Locard Exchange Principle’s premise that the contact factor will cause a criminal to either leave his/her traces at the crime scene, or carry such traces away from the crime scene with him/her. For example,

when a vehicle is driven on sand, the sand particles will be stuck in the groves of the tyre threads, which simultaneously leave them behind on the sand.
Based on their responses, the majority of the participants in Samples A, C, D and E have a good understanding of the Locard Exchange Principle. However, two (2) of the participants were unaware of the Locard Exchange Principle and did know what it entails. Meanwhile, the participants in Sample B explained that as Prosecutors, they are not trained in principles of criminal investigation, as they (principles) do not form part of their studies during training. Although the Sample B participants are not trained in criminal investigation, the researcher observed that one (1) participant has a good understanding of what the Locard Exchange Principle entails. The responses of the participant are supported by Gardner and Krouskup (2019:21) and Roncacè and Nicosia (2016:1008).

An analysis of the responses of the Samples A, B, C, D and E participants and the views of the different authors lead to the conclusion that the Locard Exchange Principle is foundational to all criminal investigations. The researcher established further that most Prosecutors may not be familiar with the Locard Exchange Principle because it does not form part of criminal law, but rather criminal investigation. The Lochner Principle is discussed in greater detail hereafter.

3.5.2 The Lochner Principle

In 2006, the Lochner Principle was established and registered as patent 2006-00361. This principle is designed to: “reveal invisible technological traces left at a crime scene by mapping them through telecommunication techniques and to render on a scientifically and technological basis a technological service to examine a crime scene with the aim of making the invisible trace visible” (Lochner & Zinn, 2014:171). The Lochner Principle transcends physical contact between two objects, but concludes that something, comparable to the Locard Exchange Principle, does exist in cyber space without physical contact (Lochner et al., 2012:71, 72). Dutelle and Becker (2019:17) conquer, stating that not all perpetrators leave traces behind at the crime scene that will lead the Police to their arrest.

From the viewpoint of cell phone investigation, the cell phone record/activity are not left behind at the crime scene. However, such records are captured and stored by

the cellular network service provider at their offsite locations which are not part of the crime scene. Lochner and Zinn (2014:161) maintain that the Locard Exchange Principle does not present clear and detailed guidelines or description of the nature of the transferable traces, nor the recording thereof; as well as the traces which could provide supportive and conclusive evidence that a cell phone was used in the commission of a crime. In many instances, the investigating officer is faced with the difficulty of substantiating that a cell phone was used at the crime scene (Lochner & Zinn, 2014:161). Lochner et al. (2012:71), questioned the probability of physical contact in cyber space between an invisible cell phone signal and the actual cell tower when trying to apply the Locard Exchange Principle in cyber space. Additionally, Lochner and Zinn (2014:161) believe that the trace or recorded activity of cell phone signals, when present at the crime scene, are continuously documented offsite as data on the cellular network service provider's computer software that operates the server.

The traces produced by the utilisation of the cell phone means that the Locard Exchange Principle cannot be regarded as the only valid recommendation to detect traces which were transferred during the commission of a crime (Lochner & Zinn, 2014:161). The latter authors are of the view that trace can be divided into two categories. Firstly, when the cell phone comes into direct contact with the crime scene or any object on the crime scene. Secondly, electronic contact in terms of which electronic data is transmitted and received by the cell phone while the user or alleged perpetrator is at the crime scene.

The electronic contact is generated by the signals which are transmitted and received by the cell phone. The electronic contact itself is an invisible and electronic trace which is visible only by means of computer printouts from the cellular service provider (Lochner & Zinn, 2014:160). Lochner (as quoted in Lochner and Zinn, 2014:171) refer to the traces as technological footprints left behind during the time of making and receiving calls. However, these footprints also include automatic and continuous registration of the cell phone without any communication transaction taking place. The trace left at the crime scene plays an essential role in securing a conviction, which is also the primary idea propelling and sustaining both the Locard Exchange Principle and Lochner Principle (Lochner et al., 2012:72).

For participants in Samples A, B, C, D and E, they responded to the question: “In your understanding, how would you describe the Lochner Principle?”
This was an open-ended question which presented the participants an opportunity to respond spontaneously according to their own understanding and ideas. No options were provided to the participants from which to select a possible answer. Some of the participants submitted multiple responses.

The responses for Samples A, C, D and E are reflected as follows:

- Five (5) participants did not know what the Lochner Principle refers to;
- Three (3) participants mentioned that the Lochner Principle is based on intangible evidence, which is present at the crime scene, but cannot be seen and physically collected. This is only available on the databases of the cellular network service providers;
- Two (2) participants described the Lochner Principle as the tracing of cell phone signals or records activity of cell phone signals;
- Two (2) participants explained that the Lochner Principle is concerned with cell phones;
- One (1) participant stated that the Lochner Principle involves the rendering of invisible cell phone signals to be visible;
- One (1) participant commented that the Lochner Principle is concerned with technology induced crimes;
- One (1) participant described the Lochner Principle as a digital version of the Locard Exchange Principle; and
- One (1) participant mentioned that the Lochner Principle is concerned with the identification of evidence, but did not explain further.

One of the participants explained the Lochner Principle thus:

> “The Lochner Principle is fundamentally based on intangible evidence. It is present at the crime scene, but cannot be seen with the human eye nor physically collected when investigating the crime scene. The investigating officer can make use different “resources and channels” to obtain such evidence. When looking at a cell phone, the cell phone signals everywhere and it roams around, but it must be download at the cellular network service providers. The cellular network service providers download it from the cell towers to get the evidence in order to prove that

> the cell phone device was in that area of reception when the crime was committed. In short, it cannot be touched and it has no physical presence".

The responses of the Sample B participants are as follows:

- One (1) participant did not know what the Lochner Principle refers to;
- One (1) participant described the Lochner Principle as the tracing of cell phone signals or records activity of cell phone signals;
- One (1) participant mentioned that the Lochner Principle is concerned with tracing of a digital footprint; and
- One (1) participant explained that the Lochner Principle is concerned with cell phones.

The majority of the participants in Samples A, C, D and E, did not understand the nature of and foundational tenets of the Lochner Principle. Some participants had a reasonably fair understanding of what the Lochner Principle entails. The responses provided by some of the participants are supported by Lochner and Zinn (2014:161), who explain that cell phone signals could be present at the crime scene, and are stored by the cellular network service providers at their offsite location. It is evident from the above extracts and answers that the participants' understanding of the Lochner Principle is not as expected. Each of the participants has his/her own version of the concept. The researcher then concludes that the Lochner Principle is relatively new to the participants. Based on the researcher's own experience, the SAPS members are trained with the focus on the physical evidence collection, instead of cell phone records – which are characteristically electronic and/or digital.

According to the researcher, one (1) participant in Sample B had fairly good understanding of what the Lochner Principle entails. The responses of this participant are supported by Lochner and Zinn (2014:161). The researcher further established that the other participants were unable to provide a clear answer regarding this question, mainly because the Prosecutors themselves were not well trained in criminal investigation. Based on the views proffered by Lochner and Zinn (2014:161), the researcher found that new opportunities for criminal investigation and crime scene processing have emerged, and that new possibilities become

available because technology is improving rapidly. Furthermore, the researcher believes that both the Locard Exchange Principle and the Lochner Principle are valid and relevant in criminal investigation. Identification of the evidence or perpetrator is imperative in criminal investigations (Tilstone et al., 2013:13).
The researcher believes that identification and individualisation of physical evidence are of importance, as discussed in greater detail hereafter.

3.5.3 Identification

Tilstone et al. (2013:13), are of the view that the term, 'identity' derived from, and signifies the distinctiveness and act of allocating a unique property or characteristic to something or someone else. This does not always correspond to identity in the natural sciences, and particularly in forensic science. In essence then identification means that objects or items share a mutual source or possess the same properties (Tilstone et al., 2013:13). In forensic science, objects are frequently identified by comparing a selected class of characteristics of an unidentified object with similar characteristics to those of a recognised standard (Lee & Pagliaro, 2013:4).

The latter authors add that when the selected class characteristics are the same between the recognised and unfamiliar samples, the unfamiliar object could then be classified with the known. Identification involves the examination of the physical and chemical properties of an object in order to characterise the object according to a group or class (Girard, 2018:34; Houck & Siegel, 2015:51). Identification entails the classification process according to which a unit or class of properties are placed in a predefined, restricted or limited class, but excluded to a particular source (Fish et al., 2015:17; Osterburg & Ward, 2015:34). Class characteristics could be probative in value and used as evidence, although such evidence may not be sufficiently decisive and conclusive to indicate a suspect's involvement in a crime (Osterburg & Ward, 2015:35).

According to the above-mentioned authors, a piece of evidence could be collected and identified within a group. However, individualisation still needs to happen. It is the researcher's contention that no single source can be identified outside of its own group. For example, a cell phone is found on the crime scene and can be identified as a Samsung cell phone. However, ownership of that cell phone still needs to be

established. In a cell phone investigation context-as evidenced in *Mahlangu v S* 2019 ZAGPPHC 35 at Paragraph 14 - the witnesses testified before Court including the alleged buyer of the cell phone, could not provide specific features that identify the cell phone except the scratches on it; and that their niece used it. The Court held further that the State could have produced better evidence on identification of the cell phone by means of obtaining ownership information from the cellular network service provider. The Court held further that the State should have obtained the ownership details through RICA (Act No. 70 of 2002), and the identification by means of scratches was not enough to prove beyond reasonable doubt that the cell phone belonged to the complainant. When viewed from the perspective of criminal investigation and identification, the case of *S V Mthetwa* 1972 (3) SA 766 (A) at 768 A-C asserted that evidence concerning the identification of an accused person must be approached with some modicum of caution because of the fallibility of human observation. In the case of *Naki v S* 2018 ZAGPJHC 509 at paragraph 8, it was clear that the Court ought to exercise caution when dealing with evidence of identification of the accused by a witness.

For participants in Samples A, B, C, D and E, the question was posed: “In your understanding, how would you describe identification?”

This was an open-ended question, and the participants were free to respond according to their own understanding and views. There was no provision for selecting a possible answer from a list of possible options. Some of the participants submitted multiple responses.

The participants in Samples A, C, D and E responded as follows:

- Five (5) participants mentioned that identification entails the identification of a perpetrator or witness;
- Four (4) participants mentioned that identification includes the identification of the type of crime scene they are dealing with;
- Two (2) participants stated that identification is a broad term with different meanings;
- One (1) participant described identification as an act of finding out who someone is or what something is;

- One (1) participant explained that identification entails proving before Court that the suspect is actually the exact person who committed the crime in question;
- One (1) participant opined that there are different kinds of identifications, and one can identify a person as either a complainant, a witness or a suspect. Stolen property can be identified, and identification for an instrument used in the commission of a crime;
- One (1) participant stated that identification relates to the unique identity of someone or something; and
- One (1) participant did not provide any answer to the question.

In their response to the question regarding identification, the Sample B participants reflected thus:

- Two (2) participants stated that identification is the most crucial part of the criminal investigation for identifying a perpetrator or perpetrators;
- One (1) participant commented that identification entails proving that the suspect before Court was the actual suspect who committed the crime; and
- One (1) participant mentioned that identification entails the identification of a perpetrator or witness.

According to the researcher, the participants' perspectives show that they had a good understanding of aspects considered relevant to identification. This was in spite of the fact that the responses of the Samples A, C, D and E participants differed slightly from the literature perspectives proffered by authors such as Girard (2018:34), Houck and Siegel (2015:51), Lee and Pagliaro (2013:4), Osterburg and Ward (2015:35) and documents analysed by the researcher. Therefore, their comprehension was not significantly different from that found in the conventional literature. Accordingly, to the researcher, the majority of the participants have a relatively good understanding of what identification entails. However, the above-cited participant answers indicate that their understanding of identification is not comprehensive. Notwithstanding these varied responses and understanding of the participants, there are still essential elements of the definition that is resonant with the definition provided by Tilstone et al. (2013:13).

According to the researcher, the Sample B participants' responses differed slightly from the literature by authors such as Girard (2018:34), Houck and Siegel (2015:51), Lee and Pagliaro (2013:4), Osterburg and Ward (2015:35) as well as documents analysed by the researcher. Overall, the participants' perspectives show that they had a good understanding of aspects considered applicable to the definition of 'identification'. Therefore, their comprehension was not significantly different from that found in several literature sources. Based on and analysis of these eclectically derived sources and responses, the researcher concludes that identification is important in criminal investigation. However, the term is broad and cannot be ascribed to any particular meaning or field of study alone.

In the realm of cell phone investigation, it is important for the investigating officer to establish the possible suspect and identify a particular cell phone number before applying for access to cell phone records. The requested information from the cellular network service provider is based on the particular cell phone number provided for the Section 205 subpoenas in terms of the CPA (Act No. 51 of 1977). Houck and Siegel (2015:58) contend that after identification, individualisation and comparison is the next logic step determining the source of evidence. The researcher discusses individualisation in greater detail hereafter.

3.5.4 Individualisation

Gardner and Krouskup (2019:20) and Fennelly and Perry (2018:24) describe individualisation as the careful and critical analysis of evidence for the purpose of identifying individual characteristics thereof. Individual characteristics allow forensic analysts to conduct or perform a comparison of the evidence with a particular object or person in order to either include or exclude such evidence into the record of the investigation. Individual characteristics are distinctive dissimilarities found in physical or biological evidence which permit the identification of the donor/ owner with a degree of high certainty (Fish et al., 2015:17). Meanwhile, Girard (2018:35) and Tilstone et al. (2013:13), maintain that the individualisation of an item reduces the possible source to the most irreducible level on the basis of the uniqueness of the item.

Fish et al. (2015:17), maintain that it is mathematically improbable for a single piece of evidence to be donated by two identical sources, given the uniqueness of the particular piece of evidence. The majority of criminals devote their knowledge to concealment of their identity and covering or disguising their activities to hide their true origin (Saini & Kapoor, 2016:1). Traced evidence rests on objects collected at the crime scene that may provide clues in order to establish the identity of the suspect and/or victim (Uzabakiriho, 2015:2). Lee and Pagliaro (2013:4) maintain that after the identification process, forensic scientists will continue with their analysis to determine whether a particular sample is unique even among other members of the same class. This process is described as individualisation, which is unique in forensic evidence analysis (Lee & Pagliaro, 2013:4). This is also the area that is mostly criticised and challenged in Courts. Houck and Siegel (2015:53) believe that the concept of individualisation is based on two assumptions, namely that everything is unique in space and time; and the characteristics by which an object is categorised are consistent over time.

The researcher is of view that the symbiotic characteristics or resemblance of objects does not necessarily imply or suggest these objects are devoid of any distinctive differences. Millions of subscribers use cell phones globally. Notwithstanding, the aspect of individualisation implies that the investigating officer can confidently identify the cell phone records as those of the suspect, based on the RICA information provided by the cellular network service provider. The cell phone number is unique to a subscriber, so is the IMEI of the cell phone.

For participants in Samples A, B, C, D and E, the question was posed: “In your understanding, how would you describe individualisation?”

This was an open-ended question that allowed the participants to freely respond according to their own understanding and knowledge of the subject. They were not provided with any alternative options from which to select a possible answer. Some of the participants submitted multiple responses.

The responses for Samples A, C, D and E participants were as follows:

- Four (4) participants mentioned that individualisation means an origin from a unique source that needs to be identified;
- Three (3) participants averred that individualisation means an individual is identified by certain characteristics that exclude him/her from others;
- Three (3) participants submitted that individualisation relates to identifying a specific person who is under investigation;
- Two (2) participants explained that individualisation is a supportive structure to identification;
- Two (2) participants commented that individualisation is a broad term;
- One (1) participant mentioned that individualisation is based on the view that everybody cannot be categorised as the same because every person is different;
- One (1) participant stated that individualisation is based on identifying individual characteristics of something or someone;
- One (1) participant alluded that individualisation relates to doing a similar thing in one place;
- One (1) participant stated that individualisation is concerned with proving a particular person is associated with specific device (mobile forensic viewpoint); and
- One (1) participant did not provide any answer to the question.

One (1) of the participants mentioned further:

> "Individualization, I don't categorise everybody as the same, every person is different, every person is handling stuff differently or seeing stuff differently or would say things different to another person".

Another participant provided an example of individualisation as follows:

> "Like when I do a tower dump ... I would identify one specific number and I will ask the network to look for that specific number for me, to see if you pick it up in that specific crime scene".

The responses of the Sample B participants are reflected thus:

- Two (2) participants alluded that individualisation is based on the premise of identifying individual characteristics of something or someone;
- One (1) participant mentioned that individualisation narrows down the investigation;

- One (1) participant described individualisation as the identification of an individual by means of certain characteristics that exclude him/ her from others;
- One (1) participant mentioned that individualisation is premised on the identification of a specific person who is the subject of a criminal investigation; and
- One (1) participant mentioned that individualisation is a broad term.

A comparison of the responses of the participants in Samples A, C, D and E demonstrates clearly that the majority of the participants agree with the literature as indicated by authors such as Fish et al. (2015:17), Girard (2018:35), Houck and Siegel (2015:53), Lee and Pagliaro (2013:4), Tilstone et al. (2013:13) and Uzabakiriho (2015:2). The researcher concludes that the majority of the participants in Samples A, C, D and E have a relatively good understanding of the nature and foundational tenets of individualisation. However, each participant has his/her own version and understanding of the concept. Furthermore, there were similarities in the participants' responses that are in consonance with perspectives from the reviewed literature as they are linked to the identification of the particular source.

When comparing the responses of the participants in Samples B, it is evident that there is agreement with literature perspectives proffered by authors such as Fish et al. (2015:17), Girard (2018:35), Houck and Siegel (2015:53), Lee and Pagliaro (2013:4), Tilstone et al. (2013:13) and Uzabakiriho (2015:2). The participants in Sample B are viewed as having a good understanding of what individualisation entails. Although each participant has his/her own conceptualisation of the concept, there were similarities in their responses in relation to perspectives from the reviewed literature as they (perspectives) apply to the identification of the particular source.

Based on the different literature perspectives and responses of the Samples A, B, C, D and E participants, the researcher concludes that individualisation proceeds from the premise that everything can be categorised as the same. People and objects could appear or look similar, but still have distinctive characteristics. When viewed in a cell phone investigation viewpoint, RICA details can be used to individualise a specific subscriber to the retrieved cell phone records. The cell phone

number and SIM card number of each SIM card is unique to each subscriber, and may serve as valuable evidence.

True administration of justice depends on the probative value of the evidence obtained for securing a conviction in Court (Osterburg & Ward, 2015:8). The researcher discusses the issue of evidence in greater detail hereafter in order to address the research aim, research objectives and research questions of this study.

3.6 EVIDENCE

Evidence relates to the substantive proof that is legally placed before the Court to either corroborate or refute facts (Dutelle, 2022:404; Fennelly & Perry, 2018:24; Gardner & Krouskup, 2019:5; Houck & Siegel, 2015:627; Monaghan, 2015:2; Swanepoel et al., 2014:261; Tilstone et al., 2013:10; Siegel & Mirakovits, 2016:58). Houck and Siegel (2015:44) provides a clearer description, stating that evidence is information (whether in oral testimony, documents or objects) which is presented in Court to contest against, or substantiate facts under dispute in a legal matter. According to the Centre for Legal Terminology in African Languages (2015:94), evidence consists of all the unpresumptuous materials or facts produced before Court to determine the truthfulness or otherwise of a matter on which judicial notice is taken. In virtually all cases, the successful investigation and prosecution of crimes necessitates the collection, safeguarding and forensic analysis of evidence (Federal Bureau of Investigation Laboratory Division, 2019:6).

In order to solve crime, the crime scene examiner ought to find relevant evidence at the crime scene (Petrisor, 2014:3). Such evidence entails objects that should first be identified and recognised as such prior to its collection (Siegel & Mirakovits, 2016:48). The forensic analysis of evidence is regularly critical in determining the guilt or innocence of the accused, and the investigating officer should pursue the evidence if he/she intends to solve the crime successfully (Federal Bureau of Investigation Laboratory Division, 2019:6; Petrisor, 2014:3). Gardner and Krouskup (2019:5) maintains that in any investigation, the evidence collected and presented in Court is itself viewed as either testimonial or physical evidence which should then be placed before Court for evaluation and informed decision-making on the facts or matter before Court.

In *S v Sibisi and Another* 2019 ZAGPJHC 3, the Court held that the State's case was still subject to evaluation in order to determine whether or not it proves the guilt of the accused beyond any reasonable doubt. In that regard, the Prosecutor or defence counsel will present evidence and facts that are advantageous to their position (Gardner & Anderson, 2016:34). The latter authors note also that reliable evidence is relatively the most satisfactory, most credible, most accurate and most reliable.

On the other hand, competent evidence includes all relevant and reliable evidence that will not be deemed inadmissible by the Court (Gardner & Anderson, 2016:39). Additionally, exculpatory evidence is utilised to prove that an incident did not occur, and ultimately exonerates the innocent party (Tilstone et al., 2013:12; Del Carmen & Hemmens, 2017:42). Meanwhile, exculpatory evidence is mostly concerned with the identity of an individual under investigation, such as DNA profiling of possible blood found on the scene, or fingerprints collected (Tilstone et al., 2013:12).

Inculpatory evidence is helpful for supporting the findings and in keeping with the hypothesised events, but other explanations are possible (Tilstone et al., 2013:12). For example, the firearm residue found on the clothes of a witness may create the assumption that the witness himself/herself could be the possible shooter. However, it is also possible that the witness is not the shooter, but was only very close during the shooting, such that the firearm residue landed on his/her clothes. From a cell phone investigation viewpoint, cell phone records provide valuable evidence that can assist the investigating officer in proving the case beyond reasonable doubts and have become essential in criminal investigations. Daltur and Hajdarević (2014:265) believes that electronic devices have become more regularly involved a number of crimes and the electronic trace left can be a vital part of the investigation process.

For participants in Samples A, B, C, D and E, the following question was asked: "In your understanding, how would you define evidence?"

The participants were free to answer this open-ended question in their own words according to their thoughts, understanding and ideas. No options were provided to

the participants from which to choose a possible answer. Some of the participants submitted multiple responses.

The responses for Samples A, C, D and E are reflected as follows:

- Four (4) participants stated that evidence necessitates exhibit collection on the scene;
- Three (3) participants described evidence as anything that directs the investigation to the suspect, or how a crime was committed, and to prove a case before Court;
- Two (2) participants mentioned that evidence is anything that can prove the guilt of another person;
- Two (2) participants submitted that evidence is the most valuable part of any criminal investigation;
- Two (2) participants stated that evidence includes each and every piece of information, whether it is a cell phone or an exhibit;
- One (1) participant describe evidence as substantial proof to corroborate or to refute facts;
- One (1) participant mentioned that evidence is information presented before Court;
- One (1) participant alluded that evidence consists of all the materials produced before Court to prove a person's guilt;
- One (1) participant explained that evidence includes direct and indirect evidence;
- One (1) participant mentioned that evidence is anything that can add value to the case;
- One (1) participant stated that evidence is part of a jigsaw puzzle to a bigger picture; and
- One (1) participant explained that evidence can bring clarity to the Court and improve the credibility of witnesses.

Additionally, one of the participants also explained that:

> "evidence is any material or item that can be used to proof the guilt of an offender or clears a person of blame or legal guilt. During cell phone

> investigations the mapping of base stations and crime scenes can be used as evidence".

The responses for the Sample B participants are reflected as follows:

- Two (2) participants describe evidence as anything that directs the investigation to either the suspect or the nature of the committed crime, and to prove a case before Court;
- One (1) participant explained that evidence includes documentary or real evidence; and
- One (1) participant mentioned that evidence is anything that could result in a prima facie case.

When comparing the responses of the participants in Samples A, C, D and E, it becomes clear that the participants agree with the literature perspectives as indicated by the Centre for Legal Terminology in African Languages (2015:94), Dutelle (2022:404), Fennelly and Perry (2018:24), Gardner and Krouskup (2019:5), Houck and Siegel (2015:627), Monaghan (2015:2), Swanepoel et al. (2014:261), Tilstone et al. (2013:10) and Siegel and Mirakovits (2016:58). Based on the critical analyses of the participants' responses in comparison with the literature, the researcher concludes that the participants in Samples A, C, D and E have a good understanding of evidence and its nature. There were similarities in the participants' responses in comparison with perspectives from the reviewed literature.

When comparing the responses of the participants in Sample B, it becomes clear that there is a significant degree of agreement with the literature perspectives from diverse sources, including the Centre for Legal Terminology in African Languages (2015:94), Dutelle (2022:404), Fennelly and Perry (2018:24), Gardner and Krouskup (2019:5), Houck and Siegel (2015:44, 627), Monaghan (2015:2), Siegel and Mirakovits (2016:58), Swanepoel et al. (2014:261) and Tilstone et al. (2013:10). The researcher concludes that the participants in Sample B have a good conceptualisation of evidence. With reference to the different literature-based views and the Samples A, B, C, D and E participants, the researcher concludes that understanding of the concept, 'evidence' is indispensable considering that that no case can be proven without evidence to sustain such proof. All of the participants understood the concept of evidence in the context of the views espoused by

Gardner and Krouskup (2019:5). The researcher discusses the different kinds of evidence in greater detail hereafter.

3.6.1 The different kinds of evidence

In this section, the different kinds of evidence refer specifically to: real or objective evidence, testimonial or subjective evidence and documentary evidence. To a great extent, a discussion of these variants of evidence also address the research aim, research objectives and research questions entailed in this study.

3.6.1.1 Real or objective evidence

Real or objective evidence is physical in nature, and encompasses anything with size, shape and dimension (Dutelle, 2022:408). Physical evidence is real, tangible and cannot be denied (Gardner & Krouskup, 2019:5; Girard, 2018:28; Hess et al., 2013:370). Objective or physical evidence is evidence that has the form of an object, trace, substance or impression found on the crime scene (Gardner & Krouskup, 2019:5; Houck & Siegel, 2015:627; Van Rooyen, 2012:16). According to Tilstone et al. (2013:11), physical evidence is objective and reliable, compared to subjective evidence that is sometimes unreliable. Furthermore, Tilstone et al. (2013:11), Van Rooyen (2012:16) and Walton (2014:70) state that physical evidence includes fingerprints, handwriting, money, shoe impressions, DNA, tool marks, hair and fibres, bite marks or anything that visibly indicates that a crime was committed; with focus more on objects than on people.

Fish et al. (2015:18) and Lochner (2014:7), state that objective evidence is commonly known as circumstantial or indirect evidence, the value of which must be drafted in a sworn statement by the witness. On the other hand, real evidence is commonly referred to as physical or objective evidence, and consists of objects or materials that are palpable and visible. Meanwhile, circumstantial evidence is indirect evidence that requires an inference to be drawn in order to connect it to the conclusion or facts (Dutelle, 2022:402; Swanepoel et al., 2014:260). Physical evidence is also viewed as utterly truthful (Gardner & Krouskup, 2019:5). According to the latter authors, objective or physical evidence has a greater evidential value in comparison with subjective or testimonial evidence. Such evidence holds crucial

information that is unknown to the lay observer, and can provide captivating information compared to testimonial evidence (Tilstone et al., 2013:11).

Recognition of physical evidence is an essential phase in the evidence gathering process (Lee & Pagliaro, 2013:1). The forensic value of the evidence may be reduced or even lost permanently in the event that physical evidence is not recognised, properly collected and preserved, and analysed (Lee & Pagliaro, 2013:1; Girard, 2018:3). According to Lee and Pagliaro (2013:3), not all crime scenes will have a “smoking-gun” or eyewitnesses present. Nonetheless, the crime scene will certainly contain physical evidence which can be utilised by investigating officers to provide leads. Physical evidence can provide valuable leads and identify a substance, instrument or object used in the commission of a crime; determining the links between the physical evidence and the victim, suspect and scene; reconstructing the event to establish what happened and how it happened; collecting and analysing evidence that can exonerate the innocent when presented before Court (Osterburg & Ward, 2015:23, 24). Physical evidence can also be removed from, or placed at the crime scene (Osterburg & Ward, 2015:43).

From a cell phone investigation viewpoint, the investigating officer will have to apply for a search warrant to seize items listed under Section 20 of the CPA (Act No. 51 of 1977) to obtain the suspect’s cell phone. Section 22 of the CPA (Act No. 51 of 1977) allocates certain powers to the Police to execute a search and seizure without a search warrant. The seizure of the suspect’s cell phone presents the investigator with an opportunity to seize valuable evidence stored on the device. From the researcher’s experience, real evidence is collected on crime scenes, the perpetrators residence or work and admitted in Court to prove or disprove the facts in dispute. Real evidence will be admitted in Court, but should be relevant and have evidential value to the facts that are being disputed.

Girard (2018:28) believes that physical evidence is only a piece to the bigger puzzle in the process of proving a case beyond reasonable doubt. In many instances, physical evidence is a crucial aspect in proving the link between the suspect or victim and scene of the crime. In many cases, physical evidence is substantiated by testimony of other witnesses (Girard, 2018:28). Gardner and Krouskup (2019:19) and Tilstone et al. (2013:11), contend that physical evidence has greater value,

advantage and ability when compared to testimonial evidence, which cannot be excluded or ignored at any rate (Gardner & Krouskup, 2019:19). The researcher discusses testimonial or subjective evidence in more detail hereafter.

3.6.1.2 Testimonial or subjective evidence

Testimonial evidence is provided in Court by a witness who is knowledgeable about the incident or facts being disputed, and presents such evidence under oath (Girard, 2018:28). Tilstone et al. (2013:11), illuminate that testimonial evidence is provided by means of statements made under oath by a witness, mostly in response to questions being asked regarding his/her recollection of what he/she saw or experienced. Gardner and Krouskup (2019:5), Houck and Siegel (2015:627), Lochner (2014:7) and Van Rooyen (2012:16) describe subjective evidence as case-related information which is gathered from individuals directly or indirectly involved in the crime or incident under investigation. The individuals concerned, include complainants, eyewitnesses, victims or suspects.

Lochner (2014:7) state that the individuals' evidence is collected in a sworn statement which will be presented orally in Court. Correctly so, all evidence is generally presented orally in Court by the person who supplied the investigating officer with a written sworn statement. A witness will be sworn in by the Court before oral evidence will be provided (Lochner, 2014:7). In addition, the witness will swear to provide the truthful facts of what he/she has witnessed during the course of the crime or investigation thereof. Gardner and Krouskup (2019:5) caution that testimonial evidence could be disadvantageous in that people may change their testimony based on their perceive perception or understanding. It is a given fact that any witness is capable of presenting inconsistencies when testifying (Gardner & Krouskup, 2019:19).

From a cell phone investigation viewpoint, the investigating officer will testify regarding the cell phone records that were obtained in terms of Section 205 of the CPA (Act No. 51 of 1977). The digital forensic investigator or analyst will provide testimony on the basis of the analysed and the acquired evidence, and according to what was determined during the analysis. The researcher discusses documentary evidence in greater detail hereafter.

3.6.1.3 Documentary evidence

Documentary evidence relates to evidence in the form of writing, sound or video recordings. This evidence is normally authenticated by expert testimony in Court (Girard, 2018:3; Hess et al., 2013:370). In terms of Section 33 of the Civil Proceedings Evidence Act (Act No. 25 of 1965), which is applicable to criminal proceedings by virtue of Section 222 of the CPA (Act No. 51 of 1977), the term, 'document' includes books, photographs, maps, letters, drawings, maps, plans and photographs. In terms of Section 221 (5) of the CPA (Act No. 51 of 1977), a document includes any device by means of which information is recorded or stored. Furthermore, Section 246 of the CPA (Act No. 51 of 1977) alludes that the term, 'document; includes books, newspapers, pamphlets, letters, circular letters, periodicals, lists, records, placards and posters. Therefore, documentary evidence conforms to the evidence that is in document form, and encompasses bank statements, cell phone records, letters, dairies, and payslips.

In *Seccombe and Others v Attorney-General* 1919 TPD 270 at page 277, the Court held that the term 'document' "is a very wide term and includes everything that contains the written or pictorial proof of something. It does not matter of what material it is made". From a cell phone investigation point of view, the investigating officer requests the cell phone records as documentary evidence from the cellular network service provider. The cell phone records are then captured and stored digitally with such cellular network service provider. The investigating officer will apply for a Section 205 subpoenas in terms of the CPA (Act No. 51 of 1977) to obtain cell phone records from the said cellular network service providers.

The Section 205 application must be submitted to the Prosecutor for reviewing and recommendation. Thereafter, the application for Section 205 subpoenas in terms of the CPA (Act No. 51 of 1977) to obtain cell phone records from the cellular network service providers will be submitted to a Magistrate or Judge for approval. The approved Section 205 subpoena is then handed over to the TSU for submission to the cellular network service provider. The ECTA (Act No. 25 of 2002) addresses computer generated documents or printouts which will be used in criminal proceedings by approval of the Court (Swanepoel et al., 2014:307). According to Section 1 of the ECTA (Act No. 25 of 2002), a data message is the text-based

information generated and sent, received or stored by electronic means and includes the (a) voice which used in an automated transaction, and (b) a stored record.
Section 15 (1) of the ECTA (Act No. 25 of 2002) further stipulates that a data message cannot be ruled inadmissible only by virtue of the intangible digital evidence. Section 1 of the CCA (Act No. 19 of 2020) also defines a data message as data generated, sent, received or stored by electronic means, where any data output is in intelligible form.

Section 15(3) of the ECTA (Act No. 25 of 2002) which controls the evaluation and admission of data messages provides that:

- Data messages can be admitted as evidence although such evidence may not be original;
- The evidential value of such evidence must be evaluated by the Court;
- When the Court considers the evidential value of the data messages, the following factors ought to be taken into account: reliability of the manner in which the evidence was generated, stored and communicated; the reliability in the manner on how the integrity of the data messages was maintained; as well as the manner in which the originator was identified; and
- Whether the production of the original data message, certified copy or printout will be admissible as evidence by its mere production in criminal proceedings.

Hess et al. (2013:375), proffer that the fast-paced growth of electronic devices and their capacity to hold and store crucial information has progressively essentialised the value of digital evidence in many criminal investigations. Dodge (2017:2) allude further that the incorporation of digital evidence in the investigation of crime can expedite the possibility of prosecutions and convictions by providing the cell phone as an ideal and unbiased digital witness. In the realm of criminal investigation, the investigating officer will apply for cell phone records via the Court, and ultimately from the cellular network service provider.

Therefore, digital evidence is the data and information that is stored, received or transmitted by an electronic device, and adds value to the investigation of a crime incident (Dutelle, 2017:374; Dutelle, 2022:404; Phillips, Godfrey, Steuart & Brown,

2014:20). Consistent with institutional responsiveness to the digital age, the justice system and its prosecutorial authorities are increasingly relying on electronic evidence such as cell phone records to prove the accused's involvement in incidents of crime (Phillips et al., 2014:3; Swanepoel et al., 2014:307). It is in this regard that Section 221 of the CPA (Act No. 51 of 1977) makes provision for the acceptance of computer-generated documents or printouts as evidence in Court. In *S v Dos Santos* 2010 (2) SACR 382 (SCA) and *Mdlongwa* 2010 (2) SACR 419 (SCA), the use of computer printouts of cell phone records can be accepted as evidence in Court. From a cell phone investigation viewpoint, in *Fisher v S* 2018 ZAWCHC 15 at Paragraph 11, the Police did not apply for cell phone records in terms of Section 205 of the CPA (Act No. 51 of 1977). Since no cell phone records were obtained from the cellular service provider, the witness was not able to provide evidence relating to direct cell phone communication between the accused's Blackberry and M's Nokia (the victim).

For participants in Samples A, B, C, D and E, the following question was posed: "In your opinion what type of evidence is cell phone records?"

This was an open-ended question, and participants were free to respond according to their own knowledge and understanding. No alternative answers were provided to the participants from which to select a possible answer. Some of the participants submitted multiple responses.

The responses of the participants in Samples A, C, D and E are reflected as follows:

- Seven (7) participants described cell phone records as documentary evidence;
- Four (4) participants mentioned that cell phone records relate to real or objective evidence;
- Two (2) participants commented that cell phone records refer to digital/ electronic evidence;
- One (1) participant alluded that cell phone records refers to supportive evidence;
- One (1) participant explained that cell phone records relate to indirect evidence initially, but could become direct evidence after analysis; and
- One (1) participant stated it differs from case to case, depending on the intended demonstration to the Court.

The responses of the participants in Sample B are reflected as follows:

- Two (2) participants mentioned that cell phone records mean real or objective evidence;
- Two (2) participants described cell phone records as documentary evidence;
- One (1) participant stated that cell phone records refer to digital or electronic evidence; and
- One (1) participant stated that the definition of cell phone records depends on the merits of each case, and in accordance with what was to be demonstrated to the Court.

Additionally, one (1) participant from sample B also contributed an example of what type of evidence is cell phone records?

> "Firstly, it depends from case to case, but at face value it is documentary evidence. If the cell phone records is going to be used to prove a case and the prosecution have nothing else, then that cell phone records will become documentary evidence which means the prosecution must prove the authenticity of such document. To prove the authenticity of such document, there will be a trail within a trail whereby the cellular network service provider will have to authenticate, that the cell phone records has been "pulled" from that number and it is "RICA'd" and belong to the accused. If it used as electronic evidence, in a sense that it is printed from a computer, than it is regarded as an original. "Because you say the original is inside, so whatever you print from there will become an original". It can become real evidence also, depending on what it is used for and how the prosecution will argue it. When cell phone records is used to corroborate your case it become real evidence".

When comparing the responses of the participants in Samples A, C, D and E, it is evident that the majority of the participants are in concurrence with the literature perspectives as indicated by authors such as Girard (2018:3), Hess et al. (2013:370), Swanepoel et al. (2014:307) as well as those entailed in Section 246 of the CPA (Act No. 51 of 1977), Section 1 and Section 15 (1) of the ECTA (Act No. 25 of 2002), and Section 221 of the CPA (Act No. 51 of 1977). When viewed in the context of cell phone investigation, the cases of *S v Dos Santos* 2010 (2) SACR 382 (SCA) and *Mdlongwa* 2010 (2) SACR 419 (SCA) demonstrate the Court's address of computer printouts of cell phone records and their acceptance as evidence.

Based on the critical analysis of the responses of the participants in Samples A, C, D and E, the researcher concludes that the majority of participants have a good understanding of the cell phone records as providing a form of digital evidence. Accordingly, the researcher upholds that the participants' perspectives were not significantly different from those obtained in the reviewed literature. When comparing the responses of the participants in Sample B, it becomes clear that the participants agree with the dominant literature perspectives as derived from authors such as Dutelle (2017:374), Dutelle (2022:404), Girard (2018:3), Hess et al. (2013:370) and Phillips et al. (2014:20). Accordingly, the researcher concludes that the majority of participants Sample B have a good understanding of the cell phone as a type of evidence. With reference to the responses of the participants in Samples A, B, C, D and E and the available literature, the researcher then concludes that cell phone records can be presented as digital or electronic, documentary, or real evidence based on what will be proved before Court by the Prosecution or defence counsel.

The researcher then concludes that automatically-generated computer printouts of cell phone records are printed and presented as documentary or electronic evidence. Based on the findings in *Fisher v S* 2018 ZAWCHC 15 and the analysis of the reviewed literature, the researcher concludes confidently that cell phone records constitute an essential form of evidence that could assist the Court in making an independent and informed decision for the benefit of all the parties concerned. It became evident that cell phone records are still an indispensable part of evidence, and could be supportive to other forms of evidence in the event that contamination happens at any point or phase of the investigation process (Forensic Science Regulator, 2020:5). The researcher discusses contamination of evidence in greater detail hereafter.

3.6.2 Contamination of evidence

Millen (2015:31) refers to contamination of evidence as the accidental, negligent or deliberate transfer of unwanted materials to physical evidence, which will undermine and affect the integrity of the original evidence collected and examined. In this regard, contamination of evidence refers to the undesirable transfer of material from another source to the physical evidence that was initially collected (Gehl & Plecas,

2016:4; Hess et al., 2013:370). Furthermore, any collected and contaminated evidence that becomes degenerated or degraded is of limited, or no value at all (Siegel & Mirakovits, 2016:47; Uzabakiriho, 2015:2). On the other hand, Siegel and Mirakovits (2016:47) maintains that the proper collection, preservation and packaging of evidence is instrumental in the successful investigation of crime. Therefore, it is essential for evidence to be packaged in tamper-proof containers or bags. In this regard, Fick (2020:13) suggests that the cell phone should either be switched to flight mode or placed in a 'faraday bag' to prevent any connections to the network service provider. The 'faraday method' serves to prevent any interruptions and circumvents any wireless signal from reaching the intended targeted device (Bair, 2018:18).

The latter author states further that wireless connectivity could alter data in many ways. Therefore, only one specific item of evidence should be packaged in an evidence container or bag (Siegel & Mirakovits, 2016:50). From the perspective of cell phone records investigation, the Section 205 application and its supporting statement from the investigating officer, the authorised subpoena, and actual cell phone records received from the cellular network service provider all form part of documentary evidence. The cell phone records should be in a Portable Document Format (PDF) format and presented as such in Court, while the Excel spreadsheets or Comma-Separated Values (CSV) format is used for purposes of analysis by the Police during the investigations. The Excel spreadsheets or CSV format are not rights- protected.

As such, and when questions arise in Court, the cellular network service provider can produce the original records to prove the authenticity of such records. It is advisable for investigators to make extra copies in order to safeguard themselves against contamination, and also book the original copy in the SAPS 13 register book for safekeeping. The researcher discusses the chain of custody in greater detail hereafter, in order to address the research aim, research objectives and research questions of this study.

3.7 CHAIN OF CUSTODY

Hess et al. (2013:378), are of the view that a detailed chain of custody ought to be kept, irrespective of the nature of the evidence the Police are dealing with. Baxter (2015:217), Fish et al. (2015:23) and Girard (2018:18) describe the term 'chain of custody' as the detailed and chronological record-keeping of evidence insofar as it relates to the persons who had access to, or possession of the evidence; as well as the reasons for their possession of such evidence. For Dutelle (2022:402) and Siegel and Mirakovits (2016:36), the chain of custody refers to a physical log for a specific exhibit and tracks the movement of the evidence or exhibit, and the identity of the persons in whose possession or custody the exhibit was entrusted, and for what reason.

There are two ways of establishing the chain of custody for evidence related reasons. Firstly, it should be proved that the evidence was safe throughout the process (Baxter, 2015:217; Siegel & Mirakovits, 2016:50). Secondly, it should be proved that the evidence was securely packaged in a tamper-proof and sealed container from its collection until it reaches Court. Poole (2015:29), Baxter (2015:217) and Siegel and Mirakovits (2016:50) note that the prosecution will prove a person's guilt by showing that the evidence collected on the crime scene is the same evidence produced in Court; and that no tampering with the evidence occurred from its collection phase until its presentation in Court. When a case is placed before Court, all evidence should be probed to establish adherence to the chain of custody (Girard, 2018:18).

In that regard, the prosecution should provide a detailed account of what happened with the evidence from its discovery and collection to the analysis phase, the storage and transfer thereof until it reached the Court. Since the management of evidence is imperative to the outcome of a criminal prosecution, it is then necessary for the prosecution to prove the chain of custody in order to confirm that the evidence was not tampered with (Poole, 2015:29). Daltur and Hajdarević (2014:270) advise that every individual who handled evidence from its collection until its presentation in Court, may be required to testify about the veracity of the evidence before Court as the same when it was collected and processed during the investigation.

In *Gcaza v S* 2017 ZASCA 92, the Court held that the chain of custody provided by the witnesses and the Section 212 affidavits submitted by consent were sufficient

to constitute proof of the chain of custody. Accordingly, there was no evidence that the seals of the sample bags might have been tampered with. In terms of cell phone investigation, cell phone records are kept with the cellular network service providers, and cannot be randomly accessed by any person. However, a Section 205 application should be completed with and accompanying statement by the investigating officer to enable the Prosecutor to process the availability of the cell phone records. Accordingly, the Prosecutor will recommend for the acquisition of such cell phone records by the Magistrate or Judge for final approval and authorisation. Once the approval is granted, the subpoena will be handed over to the TSU to subpoena the cellular network service providers, whose technicians are the only people who can accessed these records.

3.8 SUMMARY

In this chapter, the researcher has examined the role of the investigating officer and Prosecutor to determine the importance thereof. The duties and responsibilities of the investigating officer and Prosecutor in terms of obtaining cell phone records from the cellular network service providers was discussed. Furthermore, this chapter discussed criminal investigation, the objectives of criminal investigation and how it has evolved over time into a more sophisticated approaches to investigate and solve crime. The Locard Exchange Principles and the Lochner Principle was examined to determine the role both principles play and the relevance within criminal investigations, and the topic of evidence and the various types of evidence was explored. In conclusion, the researcher is of view that the rapid pace of technological developments demonstrates the need for accelerated and reconfigured approaches to criminal investigation.

In this regard, both the Locard Exchange Principle and Lochner Principle are then viewed as indispensable in criminal investigation. The next chapter focuses on cell phone record analysis and explores, describes and analyses the meaning and value of analysed cell phone records in investigating serious and violent crime; the cellular network, cell phone records, and legal framework for acquisition of cell phone records.

CHAPTER 4: CELL PHONE RECORD ANALYSIS

4.1 INTRODUCTION

Given their contemporary value and relevance in cell phone record analysis in modern-day criminal investigation, this study focused and explored the investigative value of cell phone record analysis in the investigation of serious and violent crimes in the Winelands District, WCP actually. In this regard, the chapter explores and provides a descriptive analysis of pivotal concepts such as the cellular network and the cell phone record. This chapter further explores the legislative framework that deals with cell phone records and the evidential value thereof. The researcher further provides a hypothetical example to illustrate the analysis of cell phone record data based on the researcher's experience and research.

In this regard, the researcher intends to address the research objectives as appearing in Section 1.5 of Chapter 1, namely:

- To explore and describe the meaning of analysed cell phone records; and
- To determine how cell phones records are analysed and add value in the investigation of serious and violent crime.

The Minister of Police Bheki Cele (as quoted in Masweneng, 2021:1) stated that the crime statistics for October to December 2020, "*do not paint a good picture*" and that the Police should "*dig deep*" to resolve and decrease crime. Masweneng (2021:1) state that the top four causes of death can be ascribed to gang-related killings, robberies at households and business, arguments and mob justice incidents. The preponderance of these crimes shows that the Police are struggling to curb the rise of serious and violent crimes. This has become evident when reviewing the crime statistics released for period the October to December 2020 by Police Minister Bheki Cele, whose words yeah indicate that the SAPS needs to find solutions to address the issues and curb the rise of crime. The Police Minister stated that the statistics exposed certain gaps that exist in policing and in some crime categories. It is evident that the predominant methods employed by the SAPS needs to be replaced with modern means of investigating crime.

Fick (2020:12) emphasises that technology has provided an opportunity for the expansion in new ways of doing things. One of the most important breakthroughs in the improvement of cell phone relates to the development of what is commonly known as smartphones (Alamin & Mustafa, 2015:15). Ayers, Brothers and Jansen (2014:3) and Al-Hadadi and AlShidhani (2013:576) describe mobile devices as cell phones with the primary functions of simply voicing and messaging communication and compromises of advanced abilities and services similar to computers. As opposed to traditional cell phones, smart phones are equipped with a complete operating system and other mobile applications that enable users to interact with different data and voice services.

In this regard, the cell phone has developed in such a way that it has the same computer capabilities and functions, such as calling, emails, messaging, sending multimedia messages, photography, internet browsing, navigation through maps and many more (Al-Hadadi & AlShidhani, 2013:576; Alamin & Mustafa, 2015:15; Ali et al., 2017:2; Graves, 2014:307). Lochner et al. (2012:69), maintains that cell phones influence people's everyday lives, and play a central part in the commission of crime and the people with subsequent investigation thereof. Owners of smartphone mobile devices normally keep their devices closely to themselves, which increases the possibility that perpetrators may use these devices at the very scene where they are committing the crime by robbing the cell phone owners (Walnycky, Baggili, Marrington, Moore & Breitinger, 2015:77).

In addition, Fick (2020:12) emphasises that the cell phone has also created an opportunity for criminals to expand their *modus operandi* by deviating from the traditional ways of committing crime. In this regard, the perpetrators of crime are now progressively utilising sophisticated methods to avoid detection while committing serious and violent crime. When perpetrators take their cell phones to crime scenes, their communication activity is recorded by the cellular network service providers and can later be used in the investigation of crime. Walnycky et al. (2015:77), is of view that cell phones nowadays have great storage capacity which permits the capturing of the cell phone operator's activities in detail, as well as private information.

Subscribers use smartphones as their ‘mobile office’ or ‘entertainment centre’, as well as their basic requirements for communications with family and friends (Al-Hadadi & AlShidhani, 2013:576). Afonin and Katalov (2016:10) add that people use smart phones to socialise, which has resulted in cell phones keeping very sensitive and private information about the user. The technological improvements and developments also opened new opportunities for criminal enterprises. Fick (2020:12) maintains that nowadays, there is no better starting point than with cell phone analysis when law enforcement agencies conduct an investigation.

Furthermore, Fick (2020:12) maintains that a cell phone is considered the equivalent of a computer, and in some instances, comprises of more personal information compared to our computers. Van Rooyen (2012:3) is of the view that technology used in the investigation process has enhanced the capacity of the investigation process. This is believed by many to be the hallmark of modern-day crime investigation. Investigating officers play an essential role in ensuring that a prima facie case is placed before Court in the quest to seek justice for all victims of crime. The investigating officer will be tasked to investigate serious and violent crime within their respective policing areas and collecting evidence to prove a case beyond reasonable doubt.

From a cell phone investigation viewpoint, the investigating officer will apply for a Section 205 subpoenas in terms of the CPA (Act No. 51 of 1977) to obtain cell phone records from the cellular service providers. It is imperative for investigating officers to understand how a cell phone operates. In order to address and achieve the research aim, research objectives and questions of this study, the researcher discuss the cellular concept in greater detail below.

4.2 THE CELLULAR CONCEPT

Daniel (2017:2) describes a cell phone as a two-way radio which utilise a radio connection to wirelessly communicate with cell towers when phone calls are made. The phone call moves wirelessly from the cell tower antenna to a standard landline telephone system. In addition, Graves (2014:308) describes a cell phone as a full-duplex device which allows for two people to communicate at the same time; whereas a half-duplex device such as a two-way radio or ‘walkie talkie’ allows for

one person to communicate at a given time. A cell phone has an unrestricted distance of communication, in contrast to a half-duplex device which is limited to a distance of between one (1) and eight (8) kilometres (Graves, 2014:308). Daniel (2017:4) states further that, for a cell phone to function properly, it requires two types of radios, namely: classified as a transmitter and receiver radios built into the cell phone. In order to make or receive phone calls, the cell phone must utilise two radio channels to send voice transmissions wirelessly to a wireless telephone network and have a channel to receive voice transmissions from the wireless network (Daniel, 2017:4). It is important for investigators to understand the functioning of the cell phone in order to understand where the data can be found when conducting an investigation (Bair, 2018:55; Graves, 2014:308). The researcher explored the cellular concept, which is discussed in greater detail hereafter.

4.2.1 The Cellular Network

South Africa has four (4) major cellular network service providers, namely: MTN, Vodacom, Cell C and Telkom, as well as supplementary cellular network service providers such as Virgin Mobile, Hello Mobile, and Trace Mobile; all of which utilise related services from the above mentioned four major cellular network service providers. Faruque (2019:3) describes a cellular network as a wireless telephone system through which all cell phone users connect to the base station. All base stations connect to the Mobile Switching Centre (MSC) through transmission lines. Cellular networks comprise a huge number of radio cells covering a specific and limited geographical location. Each radio cell is allocated with a specific Cell ID which is recorded in the billing record/ statement when calls are made (Hoy, 2015:1; Kumar, 2015:457; Sammons, 2015:146).

Daniel (2017:11) maintains further that cell towers or base stations are placed strategically in geographical areas taking into consideration the number of users in a specific geographical location which utilises the specific base station to make calls. Cell towers or base stations consist of a structure with radio antennas mounted to it, the equipment responsible for managing mobile stations (also known as cell phones) in the area of service; as well as a backup battery system or generator when there is power failure (Daniel, 2017:8; Faruque, 2019:3).

Cell towers or base stations have specialised equipment to handle the radio signals within range and processing phone calls, data communication and text messages. Additionally, cell towers or base stations can handle a limited capacity of users at a specific time (Daniel, 2017:10). Graves (2014:309) asserts that when a cell phone user calls another person on a landline telephone, the process is fairly simple. The cell phone call travels to the base tower closest to the caller and gets transferred to the receiver, which is then transferred to the landline telephone. Cell phone to cell phone communication is based on the same concept. The cell phone call travels to the base tower closest to the caller and is transferred to the receiver, which is then transferred to the landline system, and to the receiver on the cell phone tower closest to receiving cell phone which will then receive the phone call (Graves, 2014:309).

Graves (2014:309) and Lochner and Zinn (2014:166) maintain that the cell phone tower is designed to measure the relative distance of the cell phone from the cell tower in order to transfer the signal of a cell phone to a neighbouring tower closer to the location of the cell phone. The cell towers function on different wavelengths in order to prevent overlying and distortion of calls. In some instances, the signal is transferred to a cell tower, not normally the closets cell tower to the cell phone, but the cell tower provides better coverage and a stronger signal for the cell phone (Lochner & Zinn, 2014:166). Each cell tower has a restricted geographical area of cover and functions on an explicitly assigned radio frequency channel which allow cell towers to be spaced in a specific manner far apart from each other; and also use the same channels (Lochner & Zinn, 2014:166).

When the cell phone is within the radio range of the cell tower, the cell phone will be able to make and receive phone calls utilising the wireless telephone system (Daniel, 2017:4). The phone call is held by the cell tower closest to the caller, and the closer the caller to the cell tower, the stronger the signal. Correspondingly, the further the caller moves from the cell tower that held the call, the weaker the signal becomes, and the next nearby cell tower to the caller will receive the call (Graves, 2014:309). Although the cell phone is not being used to initiate any call or sending of SMS’s at a particular time, an automatic activation of the cell phone tower is still initiated by a handset which is switched on and moving between cell tower locations

(Lochner & Zinn, 2014:168). When a cell phone is moved from the reception region of one cell tower to another cell tower, the movement is captured and documented on the Home Location Register (HLR) as movement from the current location (LA) to a new location, referred to as the Visitor Location Register (VLR) (Lochner & Zinn, 2014:168). From a cell phone investigation viewpoint, the cell towers will capture all cellular related activities of each subscriber connected to the cell tower, and include SMS and internet activity.

Bair (2018:65, 66), Graves (2014:310) and Sammons (2015:147) describe the key components of the cellular network as follows:

- The Base Transceiver Stations (BST): a radio transceiver that is responsible for communicating with cell phones wirelessly and managing the transceiver equipment and performs channel assignments;
- The Mobile Switching Centre (MSC): the switching system for the network responsible for managing communication within the network, and interfaces with the public switch phone network. The MSC should be a focus point for investigators, as the bulk of evidence and call records is stored therein;
- The MSC contains two (2) databases, namely the HLR and VLR which possess account-related information such as billing information of the particular subscriber, the location updates last registered by the network and subscribed services;
- The Home Location Register (HLR): an important database which collects and keeps valuable user data and service information of each individual subscriber;
- The Visitor Location Register (VLR): a database that is used for cell phones roaming out of their service area, and captures and records cell phone transactions; and
- Mobile stations (MS): the cell phones making the call (Daniel, 2017:8).

For the participant in Sample E, the following question was posed: “In your opinion, what are the key components of a cellular network?”

This was an open-ended question that allowed the participant to freely respond according to their own experiences. No options were provided to the participant from which to select any possible answer.

The responses provided by the participant in Sample E reflected the key components of a cellular network as encompassing the following:

- Cell phones, Base Stations, Base Transceiver Stations, Radio Network Controllers, Mobile Switching Centre, Visitor Location Register and Home Location Register.

When comparing the response of the participant in Sample E, it becomes clear that these responses are in agreement with the literature perspectives as indicated by authors, Bair (2018:65, 66), Graves (2014:310) and Sammons (2015:147). Following the analysis of the literature and responses of the Sample E participant, it is evident that the participant has a good understanding of what the key components of a cellular network entail. In the context of cell phone investigation, cell phone records relate to information that consists of basic information relating to communication transactions from the user (Guigourés, Gay, Boullé, Clérot, & Rossi, 2015:1). The cell phone record is discussed in greater detail hereafter.

4.3 THE CELL PHONE RECORD

Lochner and Zinn (2014:169) differentiate between a cell phone record and a cell phone account, although similarities between the two exists. Cell phone records pertain to a document which shows the detailed transactions of the cell phone and the particulars of a cell phone account documents, although it is more for billing purposes. A cell phone account provides similar information to a cell phone record. However, account statements do not give the accurate duration of the call, because the subscriber is billed for the next minute as well; irrespective of whether the subscriber talked the full minute or not (Lochner & Zinn, 2014:169).

Guigourés et al. (2015:1) and Kumar et al. (2016:47), assert that a call detail record comprises of meta-data fields that describe detailed instances of telecommunication. The content of the communication is not included, and the record comprises of various characteristics of the call, such as time and duration of the call, completion status, source cell number, and the destination cell number. Meta-data relates to all cellular activity information generated or processed by the cellular network service provider as a consequence of a communication transmission (Right2Know, 2016:2).

Meta data also comprises of detailed communication entries, such as traffic data, location data, user data and the subscriber data of the device/service being used (e.g., cellular network service provider or Internet service provider), rather than the content of the recorded communication. It also includes the individual caller's personal information, call logs and related information about the e-mails and messages they send or receive; as well as their location and online activities (Right2Know, 2016:2). Meta-data is also viewed as a rich source of personal information and reveals information about the individual's every electronic communication made, beliefs, preferences and behaviour. Moreover, meta-data are storable, accessible and searchable by the cellular network service providers (Right2Know, 2016:2).

Copious information sources are found in cell phone records which may be relevant to the investigation, and covers three years of communication information of persons of interest to the investigation (Schmitz & Cooper, 2016:332). It is in this regard that the cellular network service provider either connects or terminates services rendered to the targeted cell phone in the form of the Call Detail Records (CDR) (Bair, 2018:9; Sammons, 2015:152). The Call Detail Records (CDR) themselves contain the duration and time of the call and data, all incoming and outgoing calls, the cell tower ID used for the connecting and terminating calls; as well as the possible location of the caller (Abba, Aibinu & Alhassan, 2019:258; Sultan, Ali & Zhang, 2018:41730; Zare, Olsen, Zare & Azadi, 2019:30).

For participant in Sample E, the following question was posed: "In your opinion, how are cell phone records generated?"

The participants were free to answer this open-ended question in their own words, and according to their thoughts and understanding. No options were provided to the participants from which to choose a possible answer.

The response provided by the participant in Sample E was that a cell phone record is created when a "turned on cell phone registers with the cellular system by contacting the base station with the strongest signal – via radio waves". When comparing the response of the participant in Sample E, it becomes clear that the participant's response agrees with the literature perspectives as indicated by

authors, Guigourés et al. (2015:1) and Schmitz and Cooper (2016:328). The latter authors assert that a detailed cell phone billing record is generated when the subscriber utilises the cellular network service provider by recording the activity and transactions of the cell phone, that includes the source and destination of the transaction, and the date and time of the transaction (Guigourés et al., 2015:1; Schmitz & Cooper, 2016:328). Based on the analyses of the literature and the response of the Sample E participant, it is evident that the participant has a good understanding of how cell phone records are generated.

In addition, for the participants in Samples A, B, C, D and E, the following question was posed: “In your opinion, what is a cell phone record?”

This was an open-ended question, and participants were free to respond according to their own understanding and opinion. The participants were not given an option of selecting a possible answer from a list. Some of the participants submitted multiple responses.

The responses of Samples A, C, D and E are reflected as follows:

- Three (3) participants stated that a cell phone record could be described as detailed billing of activity for a specific cell phone number;
- Two (2) participants mentioned that a cell phone record relates to communication transactions;
- One (1) participant described a cell phone record as itemised billing;
- One (1) participant noted that a cell phone record is an electronic history of a specific cell phone number that is stored on a database of the cellular network service provider, and that indicates all the activities on that particular cell phone;
- One (1) participant explained that a cell phone record is an important source of information pertaining to activities and/ or movement of individuals who handled the cell phone, or detection of whether the cell phone was moving (travelling);
- One (1) participant stated that a cell phone record refers to all cell phone activities captured in a document that was recorded by a cellular network service provider for forensic purposes;
- One (1) participant noted that a cell phone record refers to the results of the cell phone which was used for a period of time;

- One (1) participant mentioned that a cell phone record relates to all technology records regarding calls made or received, SMS's sent or received; as well as the use of social media such as WhatsApp;
- One (1) participant explained that a cell phone record is a printout showing how a particular cell phone was used in terms of calls that were made, and SMS's sent and received; and
- One (1) participant stated that a cell phone record refers to all the transactions that took place during the period which a call was received or made.

The responses from the Sample B participants are reflected as follow:

- Two (2) participants explained that cell phone records relate to communication transactions;
- One (1) participant explained that cell phone records are all cell phone activities captured in the document recorded by a cellular network service provider for forensic purposes; and
- One (1) participant explained that cell phone records relate to everything that the cell phone subscriber does on his/ her cell phone and a record is kept thereof.

When comparing the response of the participants in Samples A, C, D and E, it becomes clear that the participants agree with the literature views as indicated by authors, Lochner and Zinn (2014:169) who explain the difference between a cell phone record and cell phone account statements. Bair (2018:9) and Ayers et al. (2014:52), assert further that Call Detail Records (CDR) show the parties involved in communication by means of calls or SMS transactions. However, the content of the SMS is not recorded. Overall, the responses of the participants support the literature perspectives of authors such as Guigourés et al. (2015:1), Kumar et al. (2016:47) and Right2Know (2016:2). According to the researcher, the participants in Samples A, C, D and E have a good understanding regarding the functionality of a cell phone and utilitarian value of its records.

According to the researcher, the participants in Sample B have a good understanding of what a cell phone record is, and their views are supported by the literature perspectives posited by authors such as Lochner and Zinn (2014:169) and Right2Know (2016:2). Following a critical analysis of the literature and the

responses of the participants in Samples A, B, C, D and E, the researcher concludes that cell phone records or Call Detail Records (CDR) are the electronic or digital history or records of all cellular activities of the subscriber which is stored with the cellular network service provider.

Additionally, for participants in Samples A, B, C, D and E, the following question was posed: “In your experience, what information is displayed on a cell phone record?”

This was an open-ended question that allowed the participants to freely respond according to their own experiences and understanding. No other options were provided from which to select other possible answers. Some of the participants submitted multiple responses.

The responses from the Samples A, C, D and E participants are reflected as follows:

- Nine (9) participants stated that the duration and time of all incoming and outgoing calls of user (call history) is displayed;
- Eight (8) participants mentioned that the cell number of other parties who received or made the call is recorded;
- Eight (8) participants explained that the locational/movement data (Cell tower ID) is recorded and displayed;
- Six (6) participants stated that the cell number of the user (subscriber) is recorded;
- Six (6) participants noted that the SMS transactions are displayed;
- Five (5) participants mentioned that the RICA information of the subscriber is recorded;
- Three (3) participants mentioned that the internet activity as General Packet Radio System (GPRS) is displayed;
- Three (3) participants stated when call forwarding is activated, it is recorded and displayed;
- Three (3) participants explained that the handset profile (IMEI usage is displayed to see what SIM cards were inserted into the device);
- Three (3) participants explained that the SIM card profile (to see the different devices where SIM card were inserted) is displayed;

- Two (2) participants explained that the usage pattern (how the cell phone was used) is recorded;
- Two (2) participants explained that the cellular network service provider's information is displayed;
- One (1) participant mentioned that the SIM card with serial that was placed in the device (cell phone) is recorded and displayed for identification;
- One (1) participant mentioned that the recorded details include the place where the SIM card was purchased, or the SIM swap took place; as well as the place where the recording happened;
- One (1) participant stated that "Elke diensverskaffer se data lyk verskillend", meaning that every cellular network service provider's data looks different;
- One (1) participant mentioned that the originating and terminating base stations and suburbs is recorded and displayed;
- One (1) participant stated that the AMA (Automatic Message Accounting) is displayed;
- One (1) participant noted that the e-mails sent and received are displayed;
- One (1) participant mentioned that the pictures are displayed;
- One (1) participant explained that if the recipient did not answer the call, then the call will most probably be recorded by the cellular network service provider in the form of a message for the subscriber;
- One (1) participant explained that if a call is transferred to a secondary cell phone and the recipient answers that cell phone, both cell numbers will be recorded;
- One (1) participant mentioned that the ICCID number or IMSI number (which is the SIM card number) is displayed; and
- One (1) participant stated that the subscriber's contacts are displayed.

Additionally, one of the participants also contributed the following data that is displayed on a cell phone record:

> "A WhatsApp's messages and SMS's is displayed, but the challenge is that no content could be retrieved unless the cell phone is seized and downloaded forensically. It is important to note that on the phone record (detailed billing), some of the calls might appear on your cell phone's phonebook as missed calls, but it will not be on your cell phone record (detailed billing). This is due to the fact that the cell phone only rang for a certain amount of seconds and it is dropped prior to the starting of the

> billing. In this regard, it can be explained to the Court that the billing has not started yet, however it will be visible on the cell phone itself".

It is worth noting, one participant explained:

> "that it is crucial for investigating officers to always question the suspect on whether he/she possess a cell phone? If the answer is yes, further questions should be posted on what is the suspect's cell phone number? In addition, follow up questions such as who except the suspect uses the cell phone and if he/she mentions that "it is only me that uses my cell phone, then you know that there is no other way that another person could of used your cell phone" except the suspect". The participant advised that investigating officers should always record these questions and answers in the suspect's warning statement".

From the researcher's viewpoint, it is important for the suspect to sign next to the information because this will remove the question of how the investigating officer obtained the cell phone number. Moreover, the warning statement of the suspect can be used as evidence in Court to prove that the suspect gave the cell phone number, after which he/ she signed as confirmation of the correctness of the number given. This will pre-empt or obviate the chance of a trial within a trial that seeks to determine how the cell phone number was obtained by the investigating officer when applying for cell phone records

Another (1) participant provided a detailed explanation and example thus:

> "… on the cell phone record, there the call duration, date and time of the call, the cell phone tower and a code of the cell phone tower e.g. Boston. In Boston there is cell tower for instance Boston 1, Boston 2 or Boston 3 etc., and each cell towers is divided into different sectors as they rotate pass one (1) to three (3). It is possible to determine on what side of the tower that person was when communication took place and it allows the investigating officer to narrow down the geographical area. The investigating officer can request a detailed cell phone tower mapping from the cellular network service provider that covers Boston and then the crime scene can be plotted in that area".

The researcher concludes that the above statements concur with the view that the investigating officer is enabled to establish a possible location of the subscriber when the communication was either initiated or terminated. This can present valuable evidence in criminal investigations.

The responses of the participants in Sample B are reflected as follows:

- One (1) participant mentioned the cell phone number of the other party who received or made the call is recorded;
- One (1) participant state that the cell number of the user (subscriber) is recorded;
- One (1) participant noted that the SMS transactions are displayed; and
- One (1) participant mentioned that the internet activity of the General Packet Radio System (GPRS) is displayed.

When comparing the responses of the participants in Samples A, C, D and E, it becomes clear that the majority of the participants agree with the literature as indicated by authors, Abba et al. (2019:2580), Bair (2018:9), Guigourés et al. (2015:1), Kumar et al. (2016:47), Lochner and Zinn (2014:169), Right2Know (2016:2), Sammons (2015:152), Sultan et al. (2018:41730), Schmitz and Cooper (2016:328) and Zare et al. (2019:30).

Ayers et al. (2014:52) and Schmitz and Cooper (2016:328), maintain that the activity and transactions contain all incoming and outgoing calls; the identity of the subscriber or device initiating the call, short message service (SMS) and multimedia messaging service (MMS) transactions but no content are recorded; as well as internet activity indicated on as General Packet Radio System (GPRS) on the billing record. The General Packet Radio System (GPRS) is mostly applicable to smartphones (Schmitz & Cooper, 2016:328). Schmitz and Cooper (2016:328) explain that the contents of the SMS are not captured in the cell phone records and any attempted call - whether connected or not are displayed.

After the analyses of the literature and the responses of the participants, it is evident that the participants in Samples A, C, D and E have a good understanding of the nature of the information displayed on a cell phone record. Furthermore, the above extracts indicate the participants' understanding in relation to the cell phone record. When comparing the responses of the participants in Samples B, it becomes clear that the participants agree with the literature as indicated by authors such as Abba et al. (2019:258), Ayers et al. (2014:52), Bair (2018:9), Guigourés et al. (2015:1), Kumar et al. (2016:47), Sultan et al. (2018:41730), Schmitz and Cooper (2016:328) and Zare et al. (2019:30).

After the analyses of the literature and the responses of the participants, it is evident that the participants in Sample B have a relatively fair understanding of what information is displayed on a cell phone record. Therefore, the above extracts indicate the participants' understanding of the information displayed on a cell phone record is not uniformed. Each of the participants has his/her own understanding of the concept. The researcher concludes that the terms, 'Call Detail Records (CDR)' and 'cell phone records' are the same. This includes the Mobile Subscriber Integrated Services Digital Network (MSISDN/cell phone number) of the user, the duration of the call made or received by the user (subscriber), the other party which received or made the call, the cell phone tower which captured the call; as well as the SMS details. Emails sent and received, pictures, contacts and WhatsApp's messages are not displayed. However, WhatsApp messages are indicated as General Packet Radio System (GPRS).

Fick (2020:14) believes that cell phone records provide an interesting story when analysed. However, one should be able to understand the various abbreviations and terminology used on the cell phone record extracted by the cellular network service providers as received by the investigating officer. Such extracted record will necessarily include a list of the abbreviations and terminology, which will allow the investigating officer to interpret and understand the details in full. Based on the propositions by Fick (2020:14), the researcher established that it is important to explore and describe the cell phone terminology that appears on the cell phone record. From a cell phone investigation viewpoint, when the cellular network service providers have been subpoenaed, the cell phone records will be provided with a list of abbreviations and terminology. These abbreviations and attendant terminology are illustrated and described in Table 4.1 overleaf.

Table 4.1: Explanation of abbreviations and terminology on a cell phone record

Call Type	The call type refers to the activity of the subscriber (making of a call or received/ SMS send or received or internet usage)
Mosms	SMS originating, meaning, outgoing SMS (Short Message Service)
Mtsms	SMS terminating, meaning, incoming SMS (Short Message Service)
Mtc	Mobile terminating call, meaning, the cell phone has received an incoming call
Moc	Mobile Originating Call (outgoing call made by the subscriber)

Call Type	The call type refers to the activity of the subscriber (making of a call or received/ SMS send or received or internet usage)
Cf	Call forward, meaning, the cell phone was not available to receive the call and the call was forwarded to the messaging service of the service provider
GPRS	General Packet Radio System (GPRS) which get listed in the Call Type column when the subscriber uses the cell phone to access the internet
MSISDN	Mobile Subscriber Integrated Services Digital Network (the number of the sim card number/ cell number)
IMEI	International Mobile Equipment Identity (unique serial number of the cell phone)
Call Date	The date when the call was made or received by the subscriber
Call Time	The time when the call was made or received by the subscriber
Call Duration	The duration of the call which is the seconds of the received calls or outgoing calls
Other Party	Number of other party receiving or making calls/sending or receiving SMS
Cell ID	The reference code of the base station
Cell Name	The name of the base station activated

(Source: Adapted by researcher from Schmitz & Cooper, 2016:328, 336; Fick, 2020:13-14)

Following discussions on the use and significance of the cell phone record and its use in obtaining cell phone records, the next section presents the legal framework and process of obtaining cell phone records from the cellular service provider in greater detail. Such discussion is consonant with pertinent aspects of the research aim, research objectives and research questions of this study.

4.4 THE LEGAL FRAMEWORK AND PROCESS OF OBTAINING CELL PHONE RECORDS FROM THE CELLULAR SERVICE PROVIDER

The investigating officer can seize an individual's personal communications records from the cellular network service providers when proper authorisation has been granted by the Courts using an order or subpoena. Cell phone devices and SIM cards are not the only places where evidence is located. Cellular network service providers also have such capacity (Sammons, 2015:146; Sultan, Ali, Ahmad & Zhang, 2019:2). Therefore, it is important to distinguish what kind of evidence can be obtained from a mobile device itself, and what can be obtained from the cellular network service provider (Fick, 2020:12). Under strict laws and regulations, cellular network service providers are able to provide detailed call records of the requested cell phone, as well as location details of the specific cell tower that was used by the targeted cell phone (Ayers et al., 2014:53; Hoy, 2015:1).

The request for Section 205 subpoenas in terms of the CPA (Act No. 51 of 1977) for cell phone records are predominantly documented surveillance tools used by the state in South Africa (Hunter, 2020:5). It is in that regard that cell phone records will only be provided by the cellular network service providers once the request has been made in accordance with the mandatory legal procedures (Kumar et al., 2016:48). Geldenhuys (2017a:18) corroborates that no cellular network service provider can provide cell phone records without obtaining prior approval and authorisation of the Section 205 subpoena in terms of the CPA (Act No. 51 of 1977). Therefore, the investigating officer has to follow strict protocols and procedures as guided in terms of Section 205 of the CPA (Act No. 51 of 1977) to obtain cell phone records from the cellular service providers.

In terms of Section 7 and Section 8 of the RICA (Act No. 70 of 2002), cases where an emergency arises (such as kidnapping) or where the lives of human beings are under threat, cell phone records may be provided without a Section 205 subpoena. In terms of the RICA (Act No. 70 of 2002), the law provides that the cell phone records must be provided immediately in the event that the process of obtaining a Section 205 subpoenas in terms of the CPA (Act No. 51 of 1977) is deemed to prolong the process. Such urgent request is handled via the RICA (Act No. 70 of 2002), and not the provisions of Section 205 of the CPA (Act No. 51 of 1977). The SAPS and the cellular network service provider have a duty to immediately inform the designated Judge of such request (Geldenhuys, 2017a:18).

From a cell phone investigation viewpoint, the investigating officer must establish a possible suspect and establish whether the suspect owns a cell phone registered to him/her before applying for a Section 205 subpoena in terms of the CPA (Act No. 51 of 1977) for the purpose of obtaining cell phone records from the cellular network service provider in question. It is important for the investigating officer to establish the cell phone number or IMEI number of the device that is applicable to an investigation. It is equally important to establish the particular cellular network service provider to which the cell phone number belongs (Fick, 2020:14; Hunter, 2020:150; Shavers & Bair, 2016:39). Geldenhuys (2017a:20) believes that a large number of citizens in the RSA uses prepaid cell phone services. There is also a misconception that no data can be retrieved from prepaid numbers. However, such

retrieval is possible once the investigating officer discovers a prepaid voucher as evidence, and the place and time of the airtime or data purchase is established, as well as the MSISDN/cell phone number which activated with the prepaid voucher. Fick (2020:14) advises that the investigating officer should make use of the Centralised Reference Database (https://www.porting.co.za/PublicWebsite/) that can be accessed freely. The investigating officer will login on the portal and type in the cell phone number in question in order to obtain information to establish whether or not the cell phone number has been ported (transferred to another cellular network service provider) and check with which cellular network is/ was the cell phone number registered.

From a cell phone investigation viewpoint, establishing the correct cellular network service provider that services the cell phone number is essential in the investigation. This will ensure that the Section 205 subpoena in terms of the CPA (Act No. 51 of 1977) is submitted to the relevant cellular network service provider. In the event that the Section 205 subpoena in terms of the CPA (Act No. 51 of 1977) is sent to the wrong cellular network service provider, the cellular network service provider will report back with no cell phone records because the cell phone number is not serviced by them. This will delay the receiving time of the cell phone records from the relevant cellular network service provider.

The investigating officer can make a request in respect of any offence, but first needs to complete the application for a Section 205 subpoena in terms of the CPA (Act No. 51 of 1977) to be issued by the Court (Hunter, 2020:15). Additionally, the investigating officer must provide a sworn affidavit which includes specific details of the case and any relevant evidence to support the issuance of such subpoena (Hunter, 2020:15). Fay (2016:1) describe an affidavit as a document made under oath by a law enforcement officer to justify and substantiate the need for a search or arrest warrant. The investigator submits a Section 205 application, accompanied by a signed affidavit providing grounds for the issue of a Section 205 subpoena in terms of the CPA (Act No. 51 of 1977) to the Prosecutor for review and approval. This will include reasons why the person is suspected to be involved in the crime and the specific time frames; the location of the cell phone; and the communication for the specific cell phone number will be cited. The application for a Section 205

subpoena in terms of the CPA (Act No. 51 of 1977) will be handed to the Prosecutor or DPP for authorisation to obtain cell phone records. The Prosecutor or DPP will recommend that the cell phone records may be duly obtained. The Prosecutor or DPP will also present the signed affidavit and application to a High Court Judge, a Regional Magistrate or a Magistrate for review.

Section 205 of the CPA (Act No. 51 of 1977) and sub-Section (4) and Section 15 of the RICA (Act No. 70 of 2002) provide for a High Court Judge, a Regional Magistrate or a Magistrate to issue such a subpoena for any person who may furnish the Court with relevant information of an alleged offence that was committed. Once the High Court Judge, Regional Magistrate or Magistrate find that there are reasonable grounds to issue such a subpoena, authority will be given to obtain cell phone records from the relevant cellular network service provider. The extracted cell phone records are permanently archived electronically by the cellular network service providers.

At paragraph 11 of *S v De Vries and Others* 2008 ZAWCHC 38, the Senior Magistrate of the Cape District testified that the general procedure which he follows in instances of Section 205 subpoena in terms of the CPA (Act No. 51 of 1977) is to consider the written statements in the case docket placed before him by the investigating officer together with the application. He further testified that he perused the documents to check whether the application is made by the DPP or a person authorised by him to do so, and whether he is satisfied with the application, where after authority is then granted for the issuance of these subpoenas.

In another case, *S v Miller and Another* 2015 ZAWCHC 118, the Court held that once the Magistrate is satisfied upon perusal of the Section 205 application and attendant statements that the person subpoenaed was likely to give the material evidence referred to in the subpoena, the Magistrate was then dutifully bound to authorise the subpoena. The Court also held that in the event that the subpoenaed person wished to contest the validity of the subpoena, the onus was then on that person to produce contrasting evidence to persuade the Magistrate that the subpoena was not validly authorised. It was concluded that the duty of the Magistrate is not simply that of a "*rubberstamp*". Therefore, the subpoena must be drafted in such a fashion that it is "*as narrowly tailored as possible to meet the*

legitimate State interest of investigating and prosecuting crime". In *Haysom v Additional Magistrate*, *Cape Town and Another* 1979 (3) SA 155 (C), the Court held that, once the Section 205 subpoenas in terms of the CPA (Act No. 51 of 1977) had been authorised, could be expected in the absence of evidence to the contrary, that the Magistrate may authorise the subpoena after the exercise of a proper judgement.

In *S v Miller and Another* 2015 ZAWCHC 118 at paragraph 22, the Court held that in the matter of *Haysom v Additional Magistrate, Cape Town and Another* 1979 (3) SA 155 (C), once the Magistrate was satisfied upon the examination of those documents, that the individual subpoenaed was likely to give the material evidence referred to in the subpoena, the Magistrate was under a duty to then authorise the subpoena. The Section 205 processes allow investigators to access three years of the private communication records of a person, in respect of any offence committed or suspected of being committed, with the proper approval of even the most junior Magistrate (Hunter, 2020:7).

From a cell phone investigation viewpoint, the investigating officer will hand over the authorised Section 205 subpoenas in terms of the CPA (Act No. 51 of 1977) to one of the nine Provincial Office Communication, Interception and Monitoring Offices, commonly known as the TSU that forms part of Crime Intelligence in the SAPS. The TSU is duty bound to subpoena the respective cellular network service provider to obtain the requested cell phone records, citing the specific periods requested from the investigating officer; and thereafter hand over the requested cell phone records to the investigating officer who made the request. Fick (2020:14) is of view that the investigating officer must serve a subpoena as soon as possible. Once the cellular network service provider receives the request from the law enforcement agency, the cell phone records must be accessed and supplied.

In *S v De Vries and Others* 2008 ZAWCHC 38 at paragraph 10, the Court held that Section 205 subpoenas in terms of the CPA (Act No. 51 of 1977) calls for the cellular network service providers to appear before a Magistrate and give evidence sought in respect of the cell phone numbers and furnish such information in the form of records to the investigating officer. Once the cellular network service provider provides the information to the investigating officer, the responsible individual from

the cellular network service provider will not be obliged to appear before the Magistrate. However, the prosecution may request the responsible individual from the cellular network service provider to provide evidence based on the cell phone records provided to the investigating officer. In another case *S v Brown* (CC54/2014) 2015 ZAWCHC 128, Bozalek, J at paragraph 30 held that Section 205, read with other provisions of the CPA (Act No. 51 of 1977) are frequently used to obtain documents that include cell phone records which are kept by the major cellular network service providers, where such records are considered as essential for the investigation of crime.

Cellular network service providers must capture and store cell phone records which contains all call information, SMS's and other cell phone related information generated by the device when connected to a cellular network (Fick, 2020:14). Furthermore, communication-related information (whether real-time or archived records) should be stored for a period of three years (Fick, 2020:14). It is essential for all investigating officers to be conversant with collection of evidence in a forensically sound manner, and determine the type of information that can be requested from the cellular network service provider when applying for cell phone records (Fick, 2020:14). The latter author further states that requesting the RICA information can assist the investigating officer in establishing the identity of the person who registered a particular SIM card with the cellular network service provider. Investigating officers should be aware that some of the RICA information could be unreliable, but as a rule, should still request the RICA information.

In addition, Fick (2020:14) explains that, despite the cellular network service provider implementing several measures to ensure the correctness of the subscriber's information, this is not guaranteed. It is advisable for investigators to always request a handset profiling which will provide information on which SIM cards were placed into the cell phone device, since each SIM card has a unique number (Fick, 2020:14). From a cell phone investigation viewpoint, this will enable investigators to detect other cell phones which the perpetrator may have used. In detecting the different cell phones used by the perpetrator, the investigator could also detect other cell phone numbers or SIM cards that were used.

The specific information requested should include details such as description of any information sought and the date range thereof. Fick (2020:12) advises that it is of utmost importance for investigating officers to be aware that not all the information that is captured and stored on the cell phone can be requested from cellular network service providers. A common misunderstanding exists that cellular network service providers store the content of WhatsApp communications. WhatsApp communications and calls are only data transactions that have end-to-end encryptions, while the cellular network service providers only provide a channel through which the communication is passed from one device to another (Fick, 2020:12). Similar to WhatsApp communications, the content of SMS's is not captured and stored by the cellular network service providers. As such the content of these messages are not obtainable when requesting cell phone records from the cellular network service providers (Fick, 2020:12).

In some instances, the subpoena could merely be submitted for the account owner's details (Hunter, 2020:15). In most circumstances, the investigating officer will subpoena a cellular network service provider for cell phone records of the targeted cell phone, which includes the following information (Lochner & Zinn, 2014:169):

- The cell phone utilised and the Subscriber Identity Module (SIM) card number;
- The phone calls generated or received, SMS's generated or received;
- The date and time when the phone calls or SMS's were generated or received,
- The duration of the phone calls generated or received; and
- The cell phone tower that records the phone calls or SMS's when the cellular network was activated.

For participants in Samples A, B, C, D and E, the question was posed: "In your opinion, what are the specific procedures that have to be followed by the investigating officer to obtain cell phone records?"

This was an open-ended question which allowed the participants to freely respond according to their own experiences and understanding. No alternative options were provided to the participants from which to select a possible answer. Some of the participants submitted multiple responses.

The responses for the Samples A, C, D and E participants are reflected as follow:

- Ten (10) participants mentioned that the signed Section 205 application must be presented to Magistrate or Judge for final authorisation;
- Nine (9) participants mentioned that the investigating officer needs to draft a statement based on facts to accompany Section 205 application and provide reasons to justify the need for the cell phone records in the investigation;
- Nine (9) participants explained that the Section 205 application, statement and case docket ought to be handed to Prosecutor for recommendation and approval;
- Nine (9) participants stated that the authorised Section 205 subpoena ought to be handed to the TSU for the subpoena of, and liaison with the respective cellular network service providers;
- Seven (7) participants explained that the investigating officer needs to complete a Section 205 application forms based on the facts gathered;
- Five (5) participants stated that the investigating officer needs to apply for cell phone records via Court, in terms of Section 205 subpoena of the CPA (No. 51 of 1977);
- Five (5) participants mentioned that the investigating officer ought to obtain information regarding a specific cell phone number, and the cell phone number needs to feature in an investigation prior to the Section 205 application;
- Three (3) participants stated that there should be a causal link between the cell phone number and the alleged offence under investigation;
- Three (3) participants explained that the Section subpoena should be directed at a specific cellular network service provider with whom the cell phone is registered to;
- One (1) participant explained that the investigating officer's affidavit must indicate a prima facie case and reasons for the cell phone record' needed in the investigation; and
- One (1) participant explained that a crime must have been committed first, and a case opened for investigation.

When comparing the responses of the participants in Samples A, C, D and E, it was evident that the majority of the participants agree with the literature as indicated by authors such as Ayers et al. (2014:53), Fick (2020:14), Geldenhuys (2017a:18), Hoy (2015:1), Hunter (2020:7, 15) and Kumar et al. (2016:48). Examples of the applicable case law in this regard, are: *S v De Vries and Others* 2008 ZAWCHC 38, *S v Miller and Another* 2015 ZAWCHC 118, *Haysom v Additional Magistrate, Cape Town and another* 1979 (3) SA 155 (C) and in *S v Miller and Another* 2015 ZAWCHC 118. After the critical analyses of the literature, the CPA (Act No. 51 of 1977), case law and the responses of the participants, it is evident that the participants in Samples A, C, D and E have a good understanding of the specific procedures that have to be followed by the investigating officer to obtain cell phone records.

The responses in Sample B are reflected as follow:

- Two (2) participants explained that the investigating officer needs to complete a Section 205 application form based on facts gathered;
- Two (2) participants mentioned that the investigating officer needs to draft a statement based on facts to accompany the Section 205 application and provide reasons for the need of the cell phone records in respect of the investigation;
- Two (2) participants mentioned that the signed Section 205 application must be presented to Magistrate or Judge for final authorisation;
- One (1) participant explained that firstly, a crime must have been committed and a case opened for investigation;
- One (1) participant explained that the Section 205 application, statement and case docket must be handed to Prosecutor for recommendation and approval; and
- One (1) participant noted that the investigating officer should attach any extra affidavits that was acquired from any other person if necessary.

Additionally, one of the participants provided a detailed explanation and contributed:

> "The Section 205 application process is a two-way approval system. Firstly, the Prosecutor must review the Section 205 application and apply his/her mind whether or not to relax the bill of rights of the person in question. Once the Prosecutor is satisfied and he/she signed the application, it must go by a Magistrate or Judge, usually a Senior Magistrate or Judge for review and confirmation".

When comparing the responses of the participants in Sample B, it becomes clear that the participants' views agree with the literature perspectives posited by authors, Ayers et al. (2014:53), Fick (2020:14), Geldenhuys (2017a:18), Hoy (2015:1), Hunter (2020:7, 15) and Kumar et al. (2016:48). Based on the analyses of the literature, the CPA (Act No. 51 of 1977), case law and the responses of these particular participants, it is evident that they have a good understanding of the specific procedures that have to be followed by the investigating officer to obtain cell phone records. The researcher concludes that Section 205 of the CPA (Act No. 51 of 1977) outlines the process that one should follow in requesting cell phone records from the cellular network service providers. The process is relatively uncomplicated.

In addition, for Samples A, B, C, D and E, the questioned was posed: "In your experience, what happens to the statement of the investigating officer that is submitted to request cell phone records?"

This was an open-ended question which allowed the participants to freely respond according to their own experience and understanding. No alternative responses were provided to the participants from which to select a possible answer. Some of the participants submitted multiple responses.

The participants in Samples A, C, D and E responded as follows:

- Eleven (11) participants mentioned that the original statement is filed in the case docket as evidence;
- Eight (8) participants stated that a copy of the statement should accompany the Section 205 application and submitted to the Magistrate for filing at the Court;
- Two (2) participants explains that a copy is filed with the TSU to subpoena the cellular network service providers; and
- One (1) participant mentioned that the original copy of the Section 205 subpoena is submitted to the cell phone network provider.

Additionally, one participant explained the process of the investigating officer statement as follows:

> "The statement of the investigating officer is handed in at Court, where the investigating officer will receive a reference number under which the Section 205 application is filed".

The majority of the participants in Samples A, C, D and E have a good understanding of what happens to the statement of the investigating officer that is submitted to request cell phone records. The responses are supported by case law, such as *S v De Vries and Others* 2008 ZAWCHC 38 and Section 205 of the CPA (Act No. 51 of 1977).

The responses of the Sample B participants are reflected as follows:

- One (1) participant stated that a copy of statement is submitted to the Magistrate and is filed at the Court;
- One (1) participant mentioned that the original statement is filed in the case docket as evidence; and
- One (1) participant explained that the statement of the investigating officer is submitted to the Magistrate, because the Magistrate is the person who issues and gives authorisation for the Section 205 subpoena.

Additionally, one participant explained:

> "The statement of the investigating officer is attached to the Section 205 application, the Prosecutor reads the statement and after recommendation, it goes to a Clerk of the Court. It must be filed with the Clerk of the Court, because no Magistrate or Judge will see the investigating officer immediately sue to their workload. The Section 205 application is placed in a file, thereafter, the file is handed over to the Magistrate or Judge. The Magistrate or Judge will during the course of his/her duties assess the application and read the statement of the investigating officer and when satisfied with the content thereof, the Magistrate or Judge will authorise the Section 205 subpoena. The statement of the investigating officer cannot be separate to the application, it must always be together and be separated."

After the analyses of the responses of the Sample B participants, it is evident that they have a good understanding of what happens to the statement of the investigating officer that is submitted to request cell phone records. The responses are supported by case law such as, *S v De Vries and Others* 2008 ZAWCHC 38,

and Section 205 of the CPA (Act No. 51 of 1977). Based on the analysis of the responses provide by the participants in Samples A, B, C, D and E, the researcher concludes that it is essential for the Section 205 application and the attendant statement of the investigating officer to be filed in the case docket as evidence. This is proof of the process followed by the investigating officer to obtain cell phone records from the cellular network service providers. This also strengthened the chain of custody.

Based on the literature review and the responses of the participants in Samples A, B, C, D and E, the researcher developed a four-step investigation framework, illustrating the operational steps that have to be followed by the investigating officer to obtain cell phone records. The operational steps are presented in Table 4.2 below.

Table 4.2: Operational steps to be followed by the investigating officer to obtain cell phone records

Step1: Obtaining a cell phone number or IMEI number • The investigating officer must obtain information regarding a specific cell phone number, and the cell phone number needs to feature in the investigation prior to the Section 205 application. There should be a causal link between the cell phone number and the crime investigated. • The investigating officer should think 'out of the box', but still stay within the boundaries of the law. If the accused is known in the matter, the investigating officer may interview family members, spouses/partner or even friends to obtain the accused's cell phone number. If the accused is employed, the employer can also be interviewed to obtain contact details provided by the employee. A statement should be obtained from the person from which the contact details were obtained from. • In the instance of the seizure of a cell phone either from a crime scene or the suspect, and where the IMEI number is unknown, the investigating officers should make use of the following function, *#06# which can be accessed freely in order to obtain the IMEI of that specific cell phone.
Step 2: Completion of the Section 205 application and drafting of the investigating officer's affidavit • A Section 205 application form should be completed, citing a detailed request of information required from the cellular network service provider. • The investigating officer should draft a detailed affidavit that will accompany the Section 205 application form, the affidavit should indicate what *prima facie* evidence links the suspect to the crime being investigated and why the cell phone records are needed in the investigation. • The detailed affidavit should include facts of the case; the particular charge under investigation and the seriousness of the offence is; the address where the crime occurred; citing specific facts based on evidence collected; the cell phone numbers or IMEI and how it link to the investigation. The date and time range of the request, as well as the details of the investigating officers and contact details.

• The investigating officer's affidavit is central in the approval of such subpoena since it outlines specific information for Magistrate to review and use his/ her discretion to authorise the Section 205 subpoena in terms of the CPA (Act No. 51 of 1977). Additional affidavits of witnesses can be attached, if needed.
Step 3: The application process at Court • No cellular service provider can provide cell phone records without obtaining prior approval and authorisation of the Section 205 subpoena in terms of the CPA (Act No. 51 of 1977). • The Section 205 application process is a two-way approval system that allows for the investigating officer to submit the Section 205 application, statement and case docket to the Prosecutor for recommendation and approval. • The Prosecutor ought to review the Section 205 application and apply his/her mind in relation to relaxing the bill of rights of the person in question. Once the Prosecutor is satisfied and signs the application, it ought to be submitted to a Magistrate or Judge, usually a Senior Magistrate or Judge for review and confirmation. • After the Prosecutor has signed, the investigating officer ought to submit the Section 205 and statement to the Clerk of the Court. The Section 205 is registered with the Clerk of the Court, where the investigating officer will receive a reference number under which the application is filed. • The Magistrate or Judge will then review the application and authorise the issuance of the Section 205 subpoena once he/ she is satisfied.
Step 4: Subpoena the cellular network service providers • A copy of the authorised Section 205 subpoena ought to be handed to the TSU, who will then subpoena and laisse with the respective cellular network service provider/s. • The respective cellular network service provider/s will laisse with the TSU and subsequently provide the requested cell phone records to them. • The TSU is dutifully bound to communicate with the investigating officer and provide the requested cell phone records to them.

(Source: Concept developed by researcher)

The operational steps that have to be followed by the investigating officer to obtain cell phone records above, cover obtaining a cell phone number or IMEI number, completion of the Section 205 application and drafting of the investigating officer's statement, the application process at Court and subpoena the cellular network service providers. Based on these, it is both prudent and professional for investigating officers to know how to analyse and interpret cell phone records that have been obtained. In order to address and achieve the research aim, research objectives and questions of this study, it is then logical for the researcher to illustrate how to analyse cell phone record in greater detail in the next section.

4.5 ILLUSTRATION OF CELL PHONE RECORD ANALYSIS

Saravanan et al. (2013:125), propound that cell phone records refer to the documented cellular activity and data of the subscriber which is collected by the

cellular network service provider generally for billing purposes. The systematic analysis of this data can possibly establish the activity of the person under investigation and determine the human behavioural patterns associated with their daily life. In addition, Saravanan et al. (2013:125), intimate that cell phone usage has increased significantly as a way of communication between individuals, as well as between criminals in their criminal empires. Accordingly, a possibility exists that large numbers of crimes can be traced by analysing the cell phone footprint, which refers to the individual's cell phone records and location data of the cell tower where the calls were generated or received. In most circumstances, criminals use cell phones as means to communicate with their criminal counterparts, with whom they share instructions on how to execute their criminal plans (Saravanan et al., 2013:125).

Cell phone evidence is an instrumental tool in any investigation, whether the evidence is extracted from a cell phone, or in the analysis and interpretation of cell phone records that are stored with the cellular network service providers (Fick, 2020:14). Lochner and Zinn (2014:161) maintain that the cell phone should be on, in order to leave a trace on the computer database and in instances of a call or text message, there is contact between the two cell phones, or a cell phone and landline or vice versa. When the cell phone is switched on but not utilised, the cellular network service provider maintains communications with the device continuously (Lochner & Zinn, 2014:161). Saravanan et al. (2013:125), state that, given the evidential value of cell phone records in criminal investigations, law enforcement agencies are motivated to use cell phone records analysis as a source of evidence to solve crime effectively and expeditiously.

Cell phone records analysis is a daunting and tiring assignment that requires cell phone analysis software and tools to assist the law enforcement in their task (Abba et al., 2019:261; Kumar et al., 2016:46). Law enforcement organisations use internal custom-made tools to perform the cell phone record analysis (Geldenhuys, 2017a:18; Kumar et al., 2016:48). Meanwhile, Hunter (2020:7) states that the most commonly used cell phone records analysis tools in the SAPS are the IBM-made software called i2 Analyst's Notebook for analysing cell phone records. This tool also allows the operator to create visual maps of people's associations and

acquaintances, and links constructed on a spreadsheet of call records, bank statements and other relevant data. This tool has the capacity to access data from a range of sources, and can also be utilised to construct a full picture of an investigation. The data is stored as entities, links, and properties within the Analyst's Notebook, whose entities represent real world objects such as telephone accounts, jobs and cell phone records, bank account transactions or events such as appointments, relationships and meetings between people; as well as ownership of vehicles. In *S v Miller and Another* 2015 ZAWCHC 118 at Paragraph 18, the Court held that it is essential to observe that the Analyst Notebook does not interfere with the data that is required for analysis in any way. Moreover, in the Court's understanding, it is merely an organisational investigative tool that is used to save the investigating officer or analyst the daunting and tiring task of performing the exercise manually.

Kumar et al. (2016:46, 47), are of view that investigators request and collect cell phone records of a specific suspect(s) in a specific case for analysis, but never against unsolved cases which may have the same modus operandi. Kumar et al. (2016:46), maintain that cell phone records analysis can help investigators to solve current and unsolved cases, and may provide critical information to identify and link other suspects to the crime or suspect. Cell phone records obtained from the cellular network service providers are usually in a standard tabular format such as Excel spreadsheet or CSV file format (Kumar et al., 2016:48). In South Africa, the cell phone records are provided in either PDF document or Excel spreadsheet format (Geldenhuys, 2017a:17).

The received cell phone records may be analysed for any information that may present leads for the investigating officer to act upon. Schmitz and Cooper (2016:330) assert that crucial information provided by the cell phone record analysis includes: the numbers used by the perpetrator or people of interest; the geographical location of the cell tower triggered during the cellular activity; and the date and time of the cellular activity. The investigative leads may be in the form of as a suspect's possible identity and locations. Kumar et al. (2016:48), asserts that the information obtained from the analysed cell phone records may yield evidence which will corroborate any existing theory of the investigator.

Saravanan et al. (2013:125), upholds that an essential phase of a criminal investigation is to identify suspects involved in the crime and where possible, linking the crimes committed in the past with the same modus operandi. Kumar et al. (2016:48), believe that the evidence may refute alibis of the perpetrator(s) and might link fellow perpetrators with each other. Frequent cellular contact between two (2) identified numbers could imply that the perpetrators know each other well, or even suggest they planned the crime jointly. The investigative leads produced by the received data could provide investigators with insight and understanding of the relationship between the perpetrators (Kumar et al., 2016:48).

Hunter (2020:19) mentions further that when the call records of a known cell phone record are properly analysed, the use of locational data enables investigating officers to corroborate circumstantial evidence, especially when no credible witnesses could be found. As such, cell phone record analysis is performed to determine linkages in communications between various cell phone numbers, providing timelines and sequence of events (Geldenhuys, 2017b:28; 2018:13). In essence, then, cell phone records analysis can be used to establish the network behaviour of the particular subscriber under investigation (Sultan et al., 2018:417).

For participants in Samples A, C, D and E, the question was posed: “In your opinion, how are cell phone records analysed?”

This was an open-ended question which allowed the participants to freely respond according to their own experiences and understanding. No options were provided to the participants from which to select a possible answer. Some of the participants submitted multiple responses.

The responses for Samples A, C, D and E are reflected as follow:

- Five (5) participants explained that the investigating officer can check the locational data and time frames against the time the crime was committed;
- Five (5) participants noted that the date and time frames of calls/communication must be checked;

- Three (3) participants mentioned that the investigating officer can view the IMEI/Handset profiling to determine whether SIM cards were placed in the cell phone;
- Three (3) participants explained that the investigating officer can check the detailed communication between the various parties;
- Three (3) participants mentioned that the investigating officer can check for communication amongst suspects;
- Two (2) participants mentioned that the investigating officer should identify and highlight the cell phone numbers that are relevant to the investigation;
- Two (2) participants stated that the RICA information can be utilised to identify the subscriber;
- Two (2) participants noted that the investigating officer can show movement of the suspect/s based on their locational data;
- One (1) participant noted that the duration of calls can be checked to establish if it was long or short conversations;
- One (1) participant stated that it depends on what the investigating officer wants to prove in Court;
- One (1) participant explained that the investigating officer should scrutinise and inspect the report to make links in communication;
- One (1) participant stated that it is sometimes difficult for investigating officers to understand, in which case the investigating officer will contact Cybercrime for assistance;
- One (1) participant mentioned that it depends on individuals;
- One (1) participant remarked on the lack of training in cell phone record analysis;
- One (1) participant stated that the date when the crime was committed must be checked and compared;
- One (1) participant expressed that cell phone record analysis is a very ‘grey area’ regarding the number of people who can actually read the information;
- One (1) participant explained that the analysis is normally performed by the investigating officer, which did not directly respond to the question posed;
- One (1) participant mentioned that basic human observation is used to analyse cell phone records; and

- One (1) participant stated that it is of utmost importance that the analyst should have insight in the docket (in the event that the analyst is not the investigating officer).

One participant added further that:

> "cell phone record analysis must be kept as easy as possible and add a lot of colour".

When comparing the responses of the participants in Samples A, C, D and E, it becomes clear that the majority participants agree with dominant literature as indicated by authors, Geldenhuys (2017b:28), Geldenhuys (2018:13), Hunter (2020:19), Kumar et al. (2016:48), Schmitz and Cooper (2016:330) and Saravanan et al. (2013:125). The responses of the participants are supported by Sultan et al. (2018:41730) who maintain that cell phone records contain critical information relating to the number of voice calls generated or received; the duration of voice calls and caller ID; as well as the number of SMS generated or received of cell phone records spanning over several months or even years. Investigators can predict the mobile subscribers' behaviour in relation to the frequency and duration of calls. An analysis of the literature and the response of the participant in Samples A, C, and D, shows that some of the participants' lack understanding on how cell phone records are analysed.

According to the researcher, this can be ascribed to the lack of training in cell phone record analysis. Furthermore, the researcher asserts that the responses of the participants (notwithstanding their valuable contribution) differ slightly from the conventional literature perspectives. From the researcher's viewpoint, keeping cell phone record analysis simple and easy will allow the Court to understand the information better. The communications of individuals should be colour coded to provide easy distinction in terms of the original source of the communication. For example, 'Suspect one (1)' should be colour coded as blue, 'Suspect two (2)' as red, and 'Suspect three (3)' as yellow. In this regard, it would be easy to distinguish and locate the exact source of originator of the communication transactions amongst these three suspects. The researcher agrees that the placement of different colours in the report makes it easy for the Courts to understand and read.

It is important for investigating officers to know how to interpret the cell phone records that have been obtained (Fick, 2020:14). Lochner et al. (2012:69), maintain that with a proper exploration and understanding of the value of mapping cell phone records and their presentation as physical evidence in Court, will be an advantage to the criminal justice system. Based on the viewpoints presented by Fick (2020:14) and Lochner et al. (2012:69), the researcher is of view that illustration of a cell phone record's presentation and analysis will help the reader to understand the concept of cell phone record analysis better. The researcher concludes that the use of cell phone records analysis should be considered one of the starting points because cell phones are gradually becoming a common denominator in the commission of various sophisticated crimes.

In most cases, the investigator depends on cell phone records of the suspect, which are analysed to solve these crimes. The researcher provided a hypothetical example of two (2) cell phone records to show the type of information is recorded by the cellular network service providers. Notwithstanding the hypothetical nature of cell phone records exemplified by the researcher, the information and format contained therein remains an accurate version of a cell phone record. The researcher shows the links in communication between cell phone record one (1) and two (2).

A complex case can be illustrated in one single picture and 'a picture paints a thousand words' (Schmitz & Cooper, 2016:340). From the researcher's viewpoint, visually illustrating the analyses process will help the investigating officer in his/her quest to analyse cell phone records. The information found on a cell phone record can provide valuable evidence when analysed. However, it is essential for investigating officers to understand the information on the cell phone record. Table 4.3 depicts two (2) cell phone records with the terminology used on a cell phone record obtained from the cellular network service provider. The two (2) cell phone records illustrated in Table 4.3 are discussed in greater detail hereafter.

From a cell phone investigation viewpoint, when the cellular network service providers have been subpoenaed, the cell phone records will be provided in a format illustrated in Table 4.3. The investigating officer is duty bound to analyse the cell phone records received from the cellular network service providers. In addition, the

two (2) hypothetical cell phone records illustrated in Table 4.3 are analysed by the researcher to determine links and communication between cell phone record one (1) and cell phone record two (2).

Table 4.3: Illustration of two (2) hypothetical cell phone records

	MSIDN	IMSI	IMEI	Call date	Call time	Call type	Call duration	Other party	Cell ID	Cell name
HYPOTHETICAL CELL PHONE RECORD 1										
1	27834556164	9912000000000444427	877755029765248	2021/12/01	10:25:58	MOC	185	27844421473	10-45164	Central, Wellington
2	27834556164	9912000000000444427	877755029765248	2021/12/01	10:35:50	MTC	240	27844421473	10-45164	Central, Wellington
3	27834556164	9912000000000444427	877755029765248	2021/12/01	11:39:15	MTC	300	27844421473	10-45164	Central, Wellington
4	27834556164	9912000000000444427	877755029768796	2021/12/01	14:16:32	MOC	159	27844421473	10-66897	New Orleans, Paarl
5	27834556164	9912000000000444427	877755029768796	2021/02/01	14:25:58	MOC	145	27844421473	10-66898	Huguenot, Paarl
6	27834556164	9912000000000444427	877755029765248	2021/02/01	18:25:28	MOSMS	1	27844421473	10-89892	Amstelhof, Paarl
7	27834556164	9912000000000444427	877755029765248	2021/02/01	18:40:05	MTC	320	27844421473	10-89892	Amstelhof, Paarl
8	27834556164	9912000000000444427	877755029765248	2021/02/01	19:00:29	MTC	180	27844421473	10-89892	Amstelhof, Paarl
HYPOTHETICAL CELL PHONE RECORD 2										
1	27844421473	4443658999980000211	922364555897878	2021/12/01	10:25:58	MTC	185	27834556164	10-45164	Central, Wellington
2	27844421473	4443658999980000211	922364555897878	2021/12/01	10:35:50	MOC	240	27834556164	10-45164	Central, Wellington
3	27844421473	4443658999980000211	922364555897878	2021/12/01	11:39:15	MOC	300	27834556164	10-45164	Central, Wellington
4	27844421473	4443658999980000211	922364555897878	2021/12/01	14:16:32	MTC	159	27834556164	10-89856	Northern Paarl, Paarl
5	27844421473	4443658999980000211	922364555897878	2021/02/01	14:25:58	MTC	145	27834556164	10-66985	Lemoenkloof, Paarl
6	27844421473	4443658999980000211	922364555897878	2021/02/01	18:25:28	MTSMS	1	27834556164	10-89892	Amstelhof, Paarl
7	27844421473	4443658999980000211	922364555897878	2021/02/01	18:40:05	MOC	320	27834556164	10-89892	Amstelhof, Paarl
8	27844421473	4443658999980000211	922364555897878	2021/02/01	19:00:29	MOC	180	27834556164	10-89892	Amstelhof, Paarl

(Source: Adapted by the researcher from Schmitz & Cooper, 2016:328)

4.5.1 Cell Phone Record One (1)

The researcher presents the analyses of cell phone record one (1), which is one of the cell phone records presented in Table 4.3 above. The analysed information contained in the hypothetical cell phone record one (1) and the following evidence were generated from the cell phone record one (1):

- Cell phone 1 received four (4) phone calls as illustrated (see numbers call type 2, 3, 7 & 8) from cell phone 2;
- Cell phone 1 made three (3) phone calls (see numbers call type 1, 4 & 5) to cell phone 2;
- Cell phone 1 sends one (1) SMS (see number call type 6) to cell phone 2;
- Cell phone 1 used two (2) different handset devices to communicate with cell phone 2 (see numbers IMEI 1-8);
- Cell phone 1 travelled from the vicinity of the Newton, the New Orleans and Huguenot cell towers was activated, and lastly, the Amstelhof, Paarl cell tower (see cell name 1-8); and
- Between 10:25:58 and 19:00:29 cell phone 1 registered on eight (8) occasions between Wellington and Paarl (see cell name 1-8).

4.5.2 Cell Phone Record Two (2)

The researcher presents the analyses of cell phone record two (2), which is one of the cell phone records presented in Table 4.3 above. The analysed information contained in the hypothetical cell phone record two (2) and the following evidence were generated from the cell phone record two (2):

- Cell phone 2 received three (3) phone calls as illustrated (see numbers call type 1, 4 & 5) from cell phone 1;
- Cell phone 2 made four (4) phone calls (see numbers call type 2, 3, 7 & 8) to cell phone 1;
- Cell phone 2 receive one (1) SMS (see number call type 6) from cell phone 1;
- Cell phone 2 used one (1) handset device to communicate with cell phone 2 (see numbers IMEI 1-8);

- Cell phone 2 travelled from the vicinity of the Newton, the Northern Paarl and Lemoenkloof cell towers was activated and lastly, the Amstelhof, Paarl cell tower (see cell name 1-8); and
- Between 10:25:58 and 19:00:29 cell phone 1 registered on eight (8) occasions between Wellington and Paarl (see cell name 1-8).

In conclusion, the analysed information presented in the Table 4.3 above provides evidence that cell phone one (1) and cell phone two (2) were both present in the vicinity of Newton. Moreover, evidence clearly indicates that cell phone one (1) and cell phone two (2) travelled in different directions based on their locational information from the different cell towers and meet up again in the vicinity of Paarl. Cell phone one (1) and cell phone two (2) had continuous communication throughout the day, and no other calls nor SMS's were made to other cell numbers. In practice, the locational data will be accurately captured and stored by the Global Positioning System (GPS) instrument of the device. The researcher provides an illustration of the locational information of cell phone record one (1) and cell phone record two (2) in Figure 4.1 below. The geographical positioning/ location of cell phone one (1) and cell phone two (2) is illustrated and discussed in greater detail hereafter.

4.5.3 Determining the geographical positioning/location

A GPS receiver requires three or more satellites to establish its position. The GPS uses information of the satellite and the time the signal takes to establish its position on the earth's surface (Schmitz & Cooper, 2016:335). The GPS receivers are used to establish the geographical location of the target cell towers, crime scene or scenes, places and points of interest (Schmitz & Cooper, 2016:335). In addition, the GPS feature of the cell phone coupled with the cell tower records, the past mobility of the cell phone can be tracked to provide invaluable information that may corroborate or refute the witnesses' or suspects' accounts (Shavers, 2013:24). In that regard, a GPS device records comprises of a "goldmine" of information that creates a timeline of movement (Shavers, 2013:24). According to Lochner and Zinn (2014:161), two sets of electronic cell phone records can be used in the investigation and place the cell phone in the crime scene location. Firstly, the cell phone records in the form of phone calls made or received, SMS's generated or

received from the cell phone. Secondly, the electronic records generated by the mechanical (automatic) and continuous communication (registration) between the cell phone and the cell tower without communications made from the cell phone can be used to map the location of the target cell phone in the location of the crime scene. Lochner and Zinn (2014:161) is of view that both electronic records and data can be utilised respectively to produce a geographical mapping to determine the location of the target cell phone.

The utilisation of this kind of data to map and determine the locations of cell phones in criminal investigation serves as the basis for application of the Lochner Principle. Lochner and Zinn (2014:171) acknowledge that the data obtained from the cell phone record printouts can now be converted into a graphic display by means of mapping. Schmitz and Cooper (2016:327) also acknowledge that cell phone records and telephone landline records can be utilised to establish the communication activity of the suspect when the crime was committed. Landline records can be used, since every landline is registered at a specific address that can be traced.

The analysis of the cell phone records can be mapped and outlined, which can be utilised as evidence in Court for prosecution purposes (Schmitz & Cooper, 2016:327). Meanwhile, Hoy (2015:2) and Schmitz and Cooper (2016:340) believe that cell phone record evidence can be mapped and used to refute alibis of the suspect, place the suspect in the close vicinity of the crime scene or areas of interest, corroborate the evidence provided by state witnesses, and demonstrate the travel route of the suspect to and from the crime scene. The investigator can utilise cell phone records to determine whether the suspect had any cellular activity near the location or time when the crime was committed (Hoy, 2015:1).

Shih, Chen, Cheng and Kaod (2019:1902) advice that using Google Maps services can assist the investigator to illustrate the perpetrators or co-accused's path in a criminal investigation and helps law enforcement agencies to identify, track and arrest the perpetrator or co-accused. Moreover, this will allow the investigating officer to illustrate the route used by the perpetrator or co-accused when leaving the crime scene. The investigating officer can illustrate possible stops in the journey and its identified locations, which helps in presenting evidence and showing the Court a full picture of the cell phone records evidence.

Kumar et al. (2016:50), believes that graph visualisation provides an easy way of searching and understanding the links between people or suspects. Hunter (2020:20) states that communication data may also be utilised to map out the operations of a criminal network. Geldenhuys (2017a:17) and Geldenhuys (2017b:28) suggest that some of the advantages of cell phone record analysis and mapping allow Prosecutors to visually illustrate the crime scene to the in Court, helping the Court to understand the evidence and placing the perpetrator at the scene of the crime.

Lochner and Zinn (2015:172) and Schmitz and Cooper (2016:330) assert further that the process of cell phone record analysis enables the identification of a particular cell phone which featured at all of the crime scenes in the event that there were a series of related crimes committed in an area. The important factor is to identify possible suspects that were in a locational area and vicinity of the crime scene when the crime was committed. Similar to identifying perpetrators, cell phone evidence can also be used to identify possible witnesses who might have been in the vicinity of the crime scene when the crime was committed (Lochner & Zinn, 2015:172). The cell tower information can be utilised by investigating officers to assist in mapping the movement of the target cell phone under investigation (Lochner & Zinn, 2014:169). The investigator will be able to identify the location of the targeted cell phone by means of establishing the specific Cell ID of the cell towers in the area of interest.

Sammons (2015:152) maintains that cell phones can be located by different methods, such as triangulation - which allows the investigating officer to establish the cell phone's approximate location by using its distance from the three cell towers. The distance is calculated by establishing the signal delay for the cell phone to the three cell towers. Lochner and Zinn (2014:161) state further that the data transactions are automatically documented on the cell phone's location and also utilised to map the target cell phone's location. The connections are then documented as traces which can be gathered and used as evidence. The location of the target cell phone can be determined and also those of other people involved in the crime at a given point in time.

Hoy (2015:2) confirms that cell phone records provide information which can prove that a specific cell tower was used by the targeted cell phone within a specific geographical area of interest. In addition, Hoy (2015:255) states that the investigating officer's establishment of the location of the cell tower used and its positioning enables the possibility of inferences to be made on the potential location of the cell phone user. Therefore, establishing the geographical coverage of specific cells and combined with call detail records, might deliver crucial data to establish plausible geographical locations with some degree of certainty for the specified times involved (Hoy, 2015:255).

The use of cell phone records with cell site tower information obtained from the cellular network service provider helps to interpret and translate cell identifiers into geographical locations in relation to the cell towers used; as well as the general location from where the calls in question were made (Schmitz & Cooper, 2016:332). Ayers et al. (2014:54), on the other hand, assert that the plotting of call record locations and information onto a map is valuable. However, such plotting does not automatically offer a comprehensive and accurate picture.

For participant in Sample E, the following question was posed: "In your opinion, how can the geographical positioning of the caller or receiver be identified?"

The participants were free to answer this open-ended question in their own words, and according to their thoughts and ideas. No options were provided to the participants from which to select a possible answer.

The response provided by the Sample E participant is reflected as follows:

> "It cannot be identified, only in terms of Section 8 of the RICA (Act No. 70 of 2002) where there is a matter of life and death. Communications must be made via SMS to the "NASCOM" (meaning National Commissioner) standby cell phone who will in turn communicate with the relevant cellular network service provider. The cellular network service provider will communicate back via SMS, providing the location of the respective cell phone under investigation. Cell C cannot provide an exact location, but only the nearest base station. With a cell phone record, the base stations can narrow down the geographic position of the user".

When comparing the responses of the participant in Sample E, it becomes clear that these views are in agreement with those found in literature, as indicated by authors, Hoy (2015:1, 2) and Schmitz and Cooper (2016:332, 340). The response of the research participant and the reviewed literature, it is evident that the precise location of the cell phone cannot be mapped. However, the cell tower location can provide a general geographical location to the investigating officers, which is crucial information to place the suspect within the vicinity of the crime scene and other locations of interest. Therefore, the cell tower locations allow the investigating officer to narrow down the geographic position of the subscriber at the given time when communications were made. The researcher used the cell phone records shown in Table 4.3 to illustrate the hypothetical geographical locations of cell phone (C1) and cell phone (C2) which is mapped in the geographical map in Figure 4.1 below.

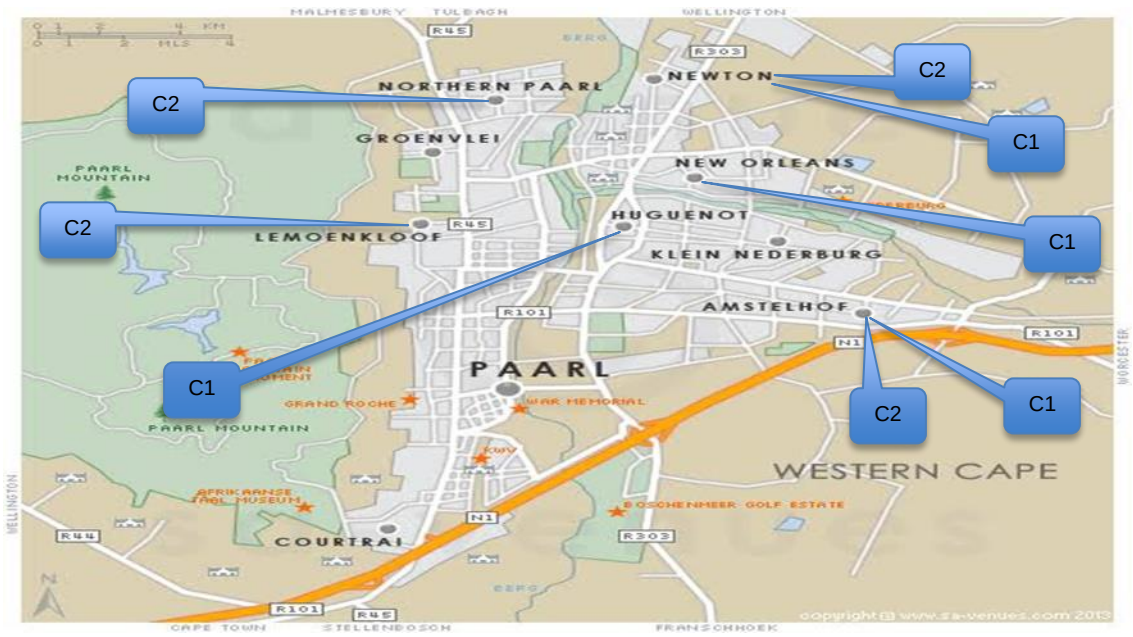

Figure 4.1: Geographical map of cell phone (1) and cell phone (2)

(Source: Adapted by the researcher from SA-Vanues.com, 2021:1)

The researcher analysed and mapped the information pertinent to cell phone record analysis as illustrated in Figure 4.1. Evidence indicates that cell phone one (C1) connected to cell towers in Newton, New Orleans, Huguenot and Amstelhof. In addition, cell phone two (C2) connected to cell towers in Newton, Northern Paarl, Lemoenkloof, and Amstelhof. The researcher provided an illustration of the locational information of cell phone record one (1) and cell phone record two (2) in Figure 4.1. Based on the analysed information in Figure 4.1, the researcher

determined the travelling routes of cell phone one (1) and cell phone two (2), which is discussed in greater detail hereafter.

4.5.4 Determining the travelling route (movement) of the cell phones

Cell phone records always include the starting cell tower location that was activated when a call was initiated, and in some instances (not always), includes the final cell tower at which the call was terminated. In some instances, cell phone records capture information about the intermediate cell towers activated during the call, as a result of which the cell tower registers a location update each time the cell phone activates the cell tower and is situated at a new location (Janecek, Hummel, Valerio, Ricciato & Hlavacs, 2012:3, 5). Hayes (2015:10) maintains that cell towers keep records of cell phone activities, and the movement of a suspect can be tracked according to the cell phone activity from one cell tower to another.

Accordingly, the investigating officer will be able to establish the direction and speed travelled by the perpetrator, and whether such speed could be reached by vehicle or other means, based on the different time spaces of the cellular activity when activated (Schmitz & Cooper, 2016:330). The analysed information presented in Figure 4.1 above provides evidence that both cell phone one (C1) and cell phone two (C2) were present in the vicinity of Newtown, and travelled in separate directions. This could be determined by mapping the particular cell towers that were activated along the way. In practice, the mapping of the cell tower locations would be determined by measurements of a GPS instrument.

The evidence gathered is reflected below:

- Cell phone one (C1) had to travel along Jan Van Riebeeck Road (R303) to activate the New Orleans and Huguenot cell towers and reaching Amstelhof;
- Cell phone two (C2) had to travel via the back road (R45) from Wellington to Paarl, in order to activate the Northern Paarl and Lemoenkloof cell towers and reaching Amstelhof;
- Cell phone one (C1) and two (C2) travelled on separate routes until they meet at Amstelhof again; and

- By establishing the times of the cell towers' activation and the distance between the cell towers, investigating officers are enabled to establish the possible speed travelled, and whether a vehicle was used or not.

In *S v Sibisi and Another* 2019 ZAGPJHC 3, the analysed cell phone records provided by Vodacom and MTN for both 'Accused No. 1' and 'Accused No. 2' indicated that their cell phones utilised the same reception towers in the same vicinity around the same times. On that basis, the researcher concludes that the hypothetical cell phone records shown in Table 4.3, proves that both cell phone one (C1) and cell phone two (C2) were activated by the cell tower in Newton at the same time. This indicated that both cell phone one (1) and cell phone two (2) were in the same vicinity near the crime scene.

Based on the views of the respective authors, the researcher concludes that it is evident that the possible route can be determined based on cell tower locations. This allows the investigating officer to establish the direction of movement based on the different timelines and cell tower locations. The precise location cannot be determined, but it reduces the geographical area of interest. From a cell phone investigation viewpoint, cell phone record analysis is relevant and possess great evidential value in the investigation of serious and violent crime. The researcher discusses the evidential value of cell phone records in greater detail hereafter.

4.6 THE EVIDENTIAL VALUE OF CELL PHONE RECORDS

Sultan et al. (2018:41728), state that cell phone technologies and cellular networks have grown massively over the past few decades, such as the development of smart phones and tablets. Cell phones and tablets subscribers have increased explosively during this period. Geldenhuys (2017a:16) ascertains that when the cell phones of suspects or victims become part of criminal investigations, they can become valuable and important sources of evidence and information. Investigating officers will be able to access voluminous information about the subscriber/user of the device. In many instances, the evidence found on a cell phone can provide more detail than a fingerprint. Guigourés et al. (2015:1) and Schmitz and Cooper (2016:370), uphold that the value of cell phone records analysis has drawn significant recognition and serious consideration in recent years because it provides

valuable information on the human behaviour and patterns of the subscriber, amongst others. Furthermore, Afonin and Katalov (2016:11) acknowledge that the relevance and importance of cell phone record analysis cannot be underestimated, especially in the investigation of serious and violent crime. Geldenhuys (2017a:17) and Schmitz and Cooper (2016:327) illuminate further that telephone landline records are equally important and useful, since they are registered to a physical address which is unique and specific to an address and subscriber. The use of telephone landline records and cell phone records has been previously utilised by law enforcement agencies to prosecute offenders successfully in South African Courts and internationally (Geldenhuys, 2017a:16; 2017a:17; 2018:13; Schmitz & Cooper, 2016:327).

Cell phone records analysis has illustrated its high value in many domains such as criminal investigation (Guigourés et al., 2015:1). Colonel Sales and Lt. Colonel Moller (as quoted in Geldenhuys, 2017a:19) believe that cell phone record analysis cannot solely prove a case, however, this must be done in collaboration with other evidence in the case. From a cell phone investigation viewpoint, the use of cell phone records and data in the investigation of serious and violent crime is of great value. Cell phone records are circumstantial evidence, and should be used in conjunction with other forms of evidence to prove a case beyond reasonable doubt. Fick (2020:15) maintains that investigating officers must advance their investigative methods, and recommends the use of cell phone record analysis as evidence to assist in the investigation and prosecution of crime. Cell phone record analysis is a positive development towards effective and expeditious resolution of crime in our contemporary era (Fick, 2020:15).

In *S v Miller and Another* 2015 ZAWCHC 118 at paragraph 21, the Court held that in the pre-Constitutional era, Section 205 of the CPA (Act No. 51 of 1977) was used extensively for the examination of individuals (often members of the media) in order to obtain information regarding their informants, or commonly to gather information about the commission of an offence. The Court held further that the leading cases dealing with Section 205 of the CPA (Act No. 51 of 1977) emanating from the pre-Constitutional era include *Haysom v Additional Magistrate, Cape Town and another* 1979 (3) SA 155 (C) and *S v Matisonn* 1981(3) SA 302 (A). The Court held further

and confirmed in *Nel v Le Roux NO and Others* 1996(3) SA 562 (CC) that Section 205 of the CPA (Act No. 51 of 1977) is constitutional in the post-1994 democratic era. Moreover, in deciding the case, the Court was fully conscious of the invasions of the various protected rights prescribed in the Bill of Rights. The Court also found that if properly applied, Section 205 of the CPA (Act No. 51 of 1977) is an important evidence gathering mechanism in the preparation of criminal prosecutions.

For participants in Sample B, the following question were posed: “In your opinion, what evidential value does cell phone records have in the prosecution of serious and violent crime?”

The participants were free to answer the afore-cited open-ended question in their own words, and according to their thoughts and understanding. No other options were provided to the participants from which to select a possible answer. Some of the participants submitted multiple responses.

The responses for Sample B are reflected as follows:

- One (1) participant stated that it (evidential value of cell phone records) is limitless “Infinite”; and
- One (1) participant mentioned that it has a lot of evidential weight because it is a corroborator and ‘silent witness’.

According to the researcher, the participants in Sample B has a relatively good understanding of the evidential value of cell phone records in the investigation and prosecution of serious and violent crime. These responses are supported in literature by Colonel Sales and Lt. Colonel Moller (as quoted in Geldenhuys, 2017a:19). Based on the views of the respective authors and the views expressed by the participants, the researcher concludes that the IMEI usage (handset) profile gives the investigating officer an indication of all SIM cards inserted into that specific cell phone during specific times.

Similar information can be requested in terms of the SIM card profile in order to determine the IMEI numbers registered to that specific SIM card number and to establish the identity of the subscriber. In this regard, it is evident that the SIM card

profile adds evidential value to the investigation of crime and cannot be underestimated because it produces a plethora of evidence.

4.7 SUMMARY

In this chapter, the researcher examined the cellular network concept in order to understand the functioning of a cellular network service provider, the important role of each cell tower within the cellular network, and the key components of the cellular network. The cell phone record and nature of information displayed on a cell phone record is discussed, as well as the utilitarian value of cell phone in the investigation of serious and violent crime. The abbreviations and terminology appearing on a cell phone record was listed and described. The legal framework and process of obtaining cell phone records from the cellular service provider was also discussed in this chapter.

In addition, the chapter encapsulated the researcher's developed investigation framework illustrating the four-step operational procedures for obtaining data from a cell phone or SIM card. In this regard, an illustration was provided of two (2) hypothetical cell phone records and cell phone record analysis. The researcher illustrated the effect of establishing the geographical positioning of the suspected cell phones insofar as determining the travelling routes of the two (2) hypothetical cell phones.

The next chapter focuses on cell phone (mobile) forensics and SIM card analysis, the process of obtaining digital evidence, the cell phone (mobile) forensic process and the data recovery process. The valuable information stored on cell phones SIM cards and evidential value of digital evidence is discussed.

CHAPTER 5: CELL PHONE (MOBILE) FORENSICS AND SIM CARD ANALYSIS

5.1 INTRODUCTION

The use of mobile cell phone devices has changed the way individuals interact with each other. In this regard, mobile devices, particularly cell phones have become an important part of contemporary everyday life. Furthermore, cell phones could be of great importance in a criminal case, considering their popularity and multiple functionality advantages or benefits. Theodorou and Yongo (2018:12) report that 95% of Africa's population uses prepaid network services. The majority of Subscriber Identity Module or Subscriber Identification Module (SIM cards) usage is based on a pay-as-you-go prepaid subscription service. This is common amongst subscribers who are unable to engage in monthly subscription fees and meet the credit requirement for such contracts. It is easy for subscribers to change cellular network service providers based on their needs. Theodorou and Yongo (2018:4) maintain further that in 147 countries globally, governments require mandatory SIM card registration with cellular network service providers in order to capture, validate and store the subscriber's identification credentials before activating their SIM cards.

Mandatory SIM card registration is usually part of complying with specific laws or their license conditions (Theodorou & Yongo, 2018:27). South Africa is amongst those countries whose governments require mandatory registration in terms of the RICA (Act No. 70 of 2002). Accordingly, all South Africans are required to register their SIM cards with their respective cellular network service provider, as required by the RICA (Act No. 70 of 2002) for law enforcement agencies to track the activities of suspected criminals or victims if needed (Right2Know, 2016:11, 12). However, the analysis of SIM cards is relatively new and AlShehri (2018:151) is of view that despite previous research efforts, SIM card forensics are still in its early stages due to the extensive in-depth knowledge and expertise required.

The Department of Communications asserts that registration of SIM cards is applicable to both prepaid and contract services (South African Government News Agency, 2011:1). Prior to the RICA (Act No. 70 of 2002) legislation, registration of

SIM cards was not an obligation, and unregistered SIM cards posed great risk for investigation because no proper record keeping measures were in place. Therefore, the RICA (Act No. 70 of 2002) has provided law enforcement agencies with a valuable investigation tool that will assist in preventing criminal organisations from using illegal cell phone activity in committing crime. The Department of Communications requires that subscribers should provide their proof of residence and proper identification when registering their SIM cards with their respective cellular network service provider (South African Government News Agency, 2011:1). Furthermore, the cellular network service providers must capture and store their subscribers' information as a requirement under the law (Fick, 2020:14; South African Government News Agency, 2011:1).

The information gathered in terms of the RICA (Act No. 70 of 2002) assist investigators in identifying the subscriber to whom the specific SIM card is registered. Although the cellular network service providers have placed various measures and means in place to ensure the correctness of the subscribers' information, criminals have discovered ways to overcome these measures, which renders some of the subscribers' information untrustworthy (Fick, 2020:14). According to the Department of Communications, the RICA (Act No. 70 of 2002) was designed and implemented to curb crimes committed with the use of cell phones, and to limit of the growing trend of cell phone theft (South African Government News Agency, 2011:1). Amongst other causal factors, cell phone theft is increased by the capacity and functionality of these devices to hold large quantities of personal and sensitive information of the user (Tamma & Tindall, 2015:3; Tamma, Skulkin, Mahalik & Bommisetty, 2018:6; 2020:6).

Hayes (2015:10) acknowledges that the field of cell phone (mobile) forensic investigations is growing significantly as a result of the growing capabilities of cell phone devices. The large volumes of information stored on cell phones has resulted in the prominence of in the field of cell phone (mobile) forensic investigations specialising in the extraction and retrieval of data from cell phone devices and SIM cards (Tamma & Tindall, 2015:1; Tamma et al., 2018:6; 2020:6). Bair (2018:4) and Ali et al. (2017:1), describe cell phone (mobile) forensics as a process in terms of which cellular-related data are recovered in a forensically sound manner by means

of detailed cell phone investigations. Given the significance of cell phone (mobile) forensics and SIM card analysis, this study explores the investigative value of cell phone and SIM card analysis in modern-day investigation of serious and violent crimes, particularly in the Winelands District, WCP. This chapter then, explores and provides a descriptive analysis of the process of conducting the analysis of cell phones and SIM cards, the valuable information that can be obtained from SIM card and cell phone analysis, and the evidential value of the analysis of SIM cards and cell phones.

Such an orientation or trajectory of the chapter is informed by the researcher's intention to address the research objective as stated in Section 1.5 of the study, namely:

- To explore and describe the valuable information that cell phones or SIM cards hold in the investigation of crime.

From a cell phone investigation viewpoint, cell phone (mobile) forensics and SIM card analysis are instrumental in serious and violent crime investigations. On that basis, the researcher maintains that is important to adhere to strict protocols and procedures in such investigations. The researcher explores and discusses the legal framework and process of obtaining cell phone and SIM card evidence in greater detail hereafter.

5.2 THE PROCESS OF OBTAINING DIGITAL EVIDENCE

People have become information based and dependent cell phones and other digital devices in their daily lives (Jordaan, 2016:362, 363). Digital evidence is fundamentally associated with electronically obtained forms of evidence in the investigation and subsequent prosecution of range of crimes, including fraud, child pornography, credit card fraud, and other sophisticated unlawful deeds (Jordaan, 2016:362). In modern times, all forms of crime are investigated and prosecuted by using digital evidence. The Internet and other gadgets/devices such as personal computers, laptops, tablets, and cell phones have transformed people's way of life and the manner in which they interact with one another (Jordaan, 2016:362).

Similarly, criminals have also adapted to the changes in technology, which exacerbates the crime problem facing South Africa. It is in this regard that cell phones and other digital devices have become tools to commit crime (Jordaan, 2016:363). However, it should be borne in mind that digital evidence could also be derived from cellular network service providers and cloud or cyber based services and networks to provide the scope of digital evidence (Sammons, 2015:2). According to Lee and Pagliaro (2013:3) the latest developments in electronics and cyber technology have necessitated that concomitant steps be taken to thwart digitally committed crimes.

According to Idris, Alhassan, Waziri and Majigi (2016:75) there are at least four main instances where a cell phone could be linked to crime:

- The cell phone could possibly be used as a means of communication during the process of the crime;
- The cell phone could possibly contain and store data that forms part of the required evidence to a crime;
- The cell phone could possibly contain the victim's information; and
- The cell phone could possibly be the definite means of committing the crime.

The Criminal Justice System addresses crime through a criminal investigation process, and ultimately brings the alleged offender before Court in order to prosecute him/her (Jordaan, 2016:362; Sammons, 2015:3). An important requirement for proving a case is to present admissible evidence before Court in order to prove a case, and the absence of such evidence in Court will weaken the possibility of convicting the offender (Jordaan, 2016:362). Therefore, cell phones and other mobile devices can assist in rendering a criminal case convictable (Sammons, 2015:145). There is an obligation on digital forensic investigators/analysts to present forensically sound evidence regarding their findings insofar as such evidence assisted the Court in establishing precedents and ultimately accepting digital evidence as an admissible record of the Court (Boddington, 2016:6). Evidence is regarded as admissible information that the Courts utilises to make an independent and informed decision on matters before the Court (Jordaan, 2016:370).

Jordaan (2016:378) states that prior to the inception of the ECTA (Act No. 25 of 2002), the question of admissibility of digital evidence in South Africa was a 'grey area' and presented a difficult task for the admission of digital evidence in South African Courts. In this regard, the ECTA (Act No. 25 of 2002) dealt with the issues of admissibility of digital evidence in the South African legal system, and allows for admission of digital evidence in legal proceedings. Jordaan (2016:378) further maintains that a key prerequisite for admitting digital evidence in Court is the reliability of the evidence insofar as its integrity is concerned. Section 3.6.1.3 of this research study provided more details regarding Section 1 of the ECTA (Act No. 25 of 2002) that defines a data message and Section 15 (1) and Section 15 (3) that controls the evaluation and admission of data messages.

The CCA (Act No. 19 of 2020) which took effect from 1 December 2021, has repealed certain sections of the ECTA (Act No. 25 of 2002). Section 1 of the CCA (Act No. 19 of 2020) that define a data message is also described in 3.6.1.3 of this research. It is worth noting that all offences committed before 01 December 2021 are still prosecuted under the ECTA (Act No. 25 of 2002). Investigating officers should fully embrace the new approach of equipping themselves with knowledge and skills about the nature and value of digital evidence because of the increased potential of digital evidence of matters under investigation (Jordaan, 2016:370).

Basdeo, Montesh and Lekubu (2014:49) and Jordaan (2016:363) inform that the harvesting of evidence from cyber environments by investigation officers should be informed by the primary goal of obtaining evidence that is deemed to be admissible in a Court of law, and preserving the integrity of such evidence. Searching for computer-generated and other related evidence is normally more time consuming and complex than the old-fashioned way of searching for physical evidence (Basdeo et al., 2014:49). Additionally, the modern-day search and seizure of electronically generated evidence differs from the traditional search and seizures of physical evidence on crime scenes.

According to Basdeo et al. (2014:49, 50), it is more preferable for the investigating officer to perform non-traditional ways of seizing electronic evidence. Such a viewpoint premises on the fact that the cell phone and SIM card are the lawful property of the owner/subscriber and for law enforcement agencies to randomly

search such property will be an infringement of the persons Constitutional rights (Graves, 2014:323). Therefore, whenever law enforcement agencies conduct search and seizures, considerations of the Constitutional rights of the person under investigation come into prominent focus (Graves, 2014:322). Afonin and Katalov (2016:15) caution that before any search and seizure process, the investigator should obtain proper legal authorisation in accordance with Section 21 of the CPA (Act No. 51 of 1977), or written consent by the duly authorized person/s.

From the researcher's viewpoint, it is important to clearly stipulate the specific storage device or devices that will be seized. In *Oosthuizen 2021 (1) SACR 278 (WCC), Magistrate for the District of Hermanus and Others*, a search warrant was authorised for "all electronic equipment which includes cell phones, desktop computers, laptops and iPads". The Court ruled further that this category of articles was rather broad and vague. Prior to the operation of the CCA (Act No. 19 of 2020) on 1 December 2021, law enforcement agencies relied on the CPA (Act No. 51 of 1977) for the seizure of electronic devices. In Table 4.1 (overleaf) the researcher illustrates the different investigative approaches to obtain digital evidence in terms of the CPA (Act No. 51 of 1977) and the CCA (Act No. 19 of 2020).

Table 5.1: Different investigative approaches to obtaining digital evidence in terms of the CPA (Act No. 51 of 1977) and the CCA (Act No. 19 of 2020)

No.	CPA (Act No. 51 of 1977)	The CCA (Act No. 19 of 2020)
1.	Section 20 of the CPA (Act No. 51 of 1977) sets out the items or articles the State may seize, which includes (a) where reasonable grounds exist that an offence or suspected offence has been committed in the Republic (of South Africa) or elsewhere; (b) which may afford evidence that an offence or suspected offence has been committed in the Republic (of South Africa) or elsewhere; (c) which is anticipated to be used or where reasonable grounds exist that it may be used in the commission of an offence.	Section 1 of the CCA (Act No. 19 of 2020) defines an ''article'' that may be seized as the following: *(a)* data; *(b)* computer programme; *(c)* computer data storage medium; or *(d)* computer system, which (i) is concerned with, connected with or is, on reasonable grounds, believed to be concerned with or connected with the commission or suspected commission; (ii) may afford evidence of the commission or suspected commission; or (iii) is intended to be used or is, on reasonable grounds, believed to be intended to be used in the commission or intended commission. Section 25 of the CCA (Act No. 19 of 2020) stipulates that **''**seize**''** includes to: *(a)* remove a computer data storage

No.	CPA (Act No. 51 of 1977)	The CCA (Act No. 19 of 2020)
		medium or any part of a computer system; *(b)* render inaccessible, data, a computer programme , a computer data storage medium or any part of a computer system in order to preserve evidence; *(c)* make and retain a copy of data or a computer programme ; or *(d)* make and retain a printout of the output of data or a computer programme .
2.	Section 21 of the CPA (Act No. 51 of 1977) provides for articles to be seized under search warrant and Section 21 (2) of the CPA (Act No. 51 of 1977) stipulates that a search warrant issued by a Magistrate, Justice, Judge or Judicial officer will necessitate for Police to seize the article in question, and the Police will be authorised to search any person identified in the warrant, or to enter and search any premises identified in the search warrant and to search any person found on or at such premises.	Section 29 (1) of the CCA (Act No. 19 of 2020) stipulates that an article can only be searched for, accessed or seized by virtue of a search warrant issued by a Magistrate or Judge of the High Court, when a written application was made and if there are reasonable grounds for believing that an article (as described by Section 1 of the CCA (Act No. 19 of 2020) is within their area of jurisdiction. It must have been used or is involved in the commission of an offence within their area of jurisdiction within the Republic (of South Africa) and it appears to such Magistrate or Judge that an article is required in evidence at such proceedings.
3.	Section 22 of the CPA (Act No. 51 of 1977) provides that a Police official may seize items listed in Section 20 without a search warrant, if the person concerned provides consent to such search and seizure. Section 22 of the CPA (Act No. 51 of 1977) provides further that there must be reasonable grounds to believe that a search warrant will be issued in terms of Section 21 (1) (a), if the Police officer had applied and delaying obtaining the search warrant would have defeated the object of the search.	Section 31 (1) of the CCA (Act No. 19 of 2020) stipulates that any Police official may, without a search warrant may execute the powers of search and seizure if the person who has the lawful authority to consent to the search. The consent should be in writing for the search and seizure of the article, and also the access of the article in question. Section 32 (1) of the CCA (Act No. 19 of 2020) provides that a Police official may without a search warrant, there must be reasonable grounds to believe that a search warrant will be issued to them under Section 29 (1) *(a),* if they applied for such warrant and that the delay in obtaining such warrant would defeat the object of the search and seizure.
4.	In terms of Section 23 (1) of the CPA (Act No. 51 of 1977), upon the arrest of any individual, the person effecting the arrest may (a) if he/she is a peace officer, search the arrested person and seize any article referred to in Section 20, that is found in the possession of or	Section 33 (1) of the CCA (Act No. 19 of 2020) stipulates that a Police official may without a warrant, as contemplated in Section 40 of the CPA (Act No. 51 of 1977), arrest any person who commits any offence.

No.	CPA (Act No. 51 of 1977)	The CCA (Act No. 19 of 2020)
	in the custody, or under the control of the arrested person, and where such peace officer is not a Police official, he/she shall immediately deliver any such article to the Police.	Section 33 (2) of the CCA (Act No. 19 of 2020) provides that on the arrest of a person a Police official may search for and perform the powers referred to in paragraphs *(a)* and *(b)* of the definition of ‘‘seize’’ in respect of a computer data storage medium or any part of a computer system referred to in paragraph *(c)* or *(d)* of the definition of ‘‘article’’, which is found in the possession of or in the custody or under the control of the person. In terms of Section 33 (3) of the CCA (Act No. 19 of 2020), a Police official may only access or perform the powers referred to in paragraph *(c)* or *(d)* of the definition of ‘‘seize’’, in respect of a computer data storage medium or a computer system by means of a search warrant for the purpose of accessing the article.

(Source: Adapted by the researcher from the CPA (Act No. 51 of 1977) and CCA (Act No. 19 of 2020)

The CCA (Act No. 19 of 2020) directs investigating officers on how to seize and access electronic devices. The CPA (Act No. 51 of 1977) still applies to the search and seizure of articles or items as prescribed in Section 20. Basdeo et al. (2014:57), believes that Section 20 of the CPA (Act No. 51 of 1977) is not clear with regard to electronic devices, but that the term, “anything” allows for the search for and seizure of electronic devices and information. Section 1 of the CCA (Act No. 19 of 2020) provides a clear and detailed description regarding electronic devices that may be seized. In *S v Miller* 2015 JDR 1808 (WCC), arguments were made that the Police may seize a cell phone which is in the person’s possession, and the cell phone is deemed as an extension of the person.

In the case of *BK and Another v Minister of Police and Others* 2019 ZAWCHC 91, the Court cited Section 23 (1) (a) of the CPA (Act No. 51 of 1977) which permits a peace officer to search a person and seize any article upon the arrest of such a person. Graves (2014:322) advises that when conducting search and seizures, investigators should be mindful of issues such as the legal basis of the search; the integrity and validity of the evidence extracted; as well as the relevance of such evidence. Captain Coetzee (as quoted in Kempen, 2017:23) cautions that when a

search and seizure is conducted and items are found that fall outside the scope of the search warrant, such items must not be seized. When reasonable grounds exist that such seizure could render the search and seizure illegal, such search and seizure should be stopped forthwith. Jordaan (2016:380) cautions that the most common mistake any investigating officer could make, is to obtain evidence in an unlawful manner or to alter the evidence after its collection. To ensure that evidence is admissible in Court, one should adhere to the legal requirements of the law.

In terms of Section 35 (5) of the Constitution (Act No.108 of 1996), any evidence obtained in a manner that violates any right in the Bill of Rights, must be excluded as evidence. Jordaan (2016:380) supports the view that evidence deemed inadmissible in legal proceedings will not be considered as evidence and must be excluded from the trial. From a cell phone investigation viewpoint, the investigating officer must obtain a search warrant to search a person, his/her property and to seize the items listed in the search warrant in terms of Section 29 (1) of the CCA (Act No. 19 of 2020). The CCA (Act No. 19 of 2020) allows for search and seizure of items in circumstances where no search warrant could have been obtained, and upon the arrest of the perpetrator, the cell phone and SIM card may be seized without a search warrant, if it is under the possession of the arrested person.

Basdeo et al. (2014:50), maintain that the search and seizure of electronic evidence does not simply involve transferring electronic hardware or cell phones from a crime scene to the evidence store for safekeeping. Equally important is the safeguarding of the data in an electronic format, which is not merely handing over of mobile devices or computer hardware. Sammons (2015:152) states that when investigating officers are dealing with cell phones and other mobile devices, their primary duty should be to isolate the identified cell phone from the network. Isolation of the cell phone is essential for preserving the stored evidence in its original position or condition and possible danger of remote wiping of the data. Therefore, cell phones must under no circumstances, be connected to the cellular network service provider, local Wi-Fi or Bluetooth devices (Boddington, 2016:57).

Afonin and Katalov (2016:10), Fick (2020:13) and Tahiri (2016:17) advise that digital forensic investigator/analyst must be mindful that a large number of suspects frequently utilise cloud services such as Google Drive, OneDrive, Apple iCloud, and

others to store information such as emails, photos, videos, files and notes. Additionally, individuals, organisation and government agencies also use cloud services to store online communications and large volumes of data, most of which is private and confidential (Boddington, 2016:29). However, the investigating officer can obtain a Court order to subpoena the cloud service providers for access to the information stored on the cloud provided that there are convincing grounds for such a course of action (Afonin & Katalov, 2016:10). From a technical perspective, the use of cloud services has created an enormous challenge for investigating officers because the information is not necessarily stored on the cell phone itself, but normally in an international server outside of South Africa (Boddington, 2016:29; Fick, 2020:13).

Fick (2020:13) maintains that South African law enforcement agencies and Courts do not have jurisdiction of these servers which are based in other countries. Therefore, a local subpoena would not be sufficient to obtain the information that is required. In addition, Afonin and Katalov (2016:10) and Fick (2020:13) advise the investigating officer to acquire written consent from the suspect in order to search the cloud server and obtain the necessary information required for the investigation. The cloud username, email address and passwords must be requested from the person under investigation, and this should form part of the written consent so that the digital forensic investigator/ analyst can analyse the cell phone and duly access the data. Fick (2020:13) cautions further that the absence of the necessary legal consent implies that the investigating officer will be subjected to a tiresome process of mutual legal assistance (MLA) in order to obtain access to the relevant information.

In a South African context, accessing of data legally is crucial as a result of Section 86 (1) of the ECTA (Act No. 25 of 2002). Section 86 (1) of the ECTA (Act No. 25 of 2002) stipulates further that any person who intentionally accesses or intercepts any data without the legal authorisation, shall be guilty of an offence. Section 37 (1) of the CCA (Act No. 19 of 2020) provides that a Police official or an investigator (referred to as private person assisting the Police) who unlawfully and intentionally searches for, accesses or seizes data, a computer programme, a computer data storage medium or any part of a computer system without the relevant legal

authorisation or consent is guilty of an offence. It is against such a backdrop that Jordaan (2016:381) cautions against the mistake that an investigating officer could make by collecting evidence without the proper legal authorisation. Section 37 (2) of the CCA (Act No. 19 of 2020) stipulates that an investigator or Police official shall be found guilty of an offence if he/ she acquires or uses any instrument, device, equipment, password, decryption key, data or other information to gain access to or use data, a computer programme, a computer data storage medium or any part of a computer system in the manner and for the purposes specified in the search warrant concerned.

Section 37 (3) of the CCA (Act No. 19 of 2020) stipulates further that a Police official or an investigator who transgresses or fails to adhere to Subsection (1) or (2), is liable on conviction, to a fine or imprisonment for a period not exceeding two (2) years, or both a fine and such imprisonment. The legal obligation rests upon the digital forensic investigator/ analyst to ensure that they have the necessary legal authorisation to access the data in order to acquire, examine and analyse such data. The necessary legal authorisation to access the data will be either in terms of the relevant search warrant, by Court order, or consent from the owner or custodian of the cell phone (Jordaan, 2016:381).

For participants in Samples A, C, D and E, the question was posed: “In your experience, when a cell phone and sim card is seized, what is the procedure to obtain data from a SIM card?”

This was an open-ended question allowing participants to freely respond according to their own experience and understanding. No optional answers were provided to the participants from which to select a possible answer. Some of the participants submitted multiple responses.

The responses for Samples A, C, D and E are reflected as follows:

- Six (6) participants explained that the cell phone and the SIM card should be submitted to the Command Centre or DPCI by means of a formal letter specifying the particular request for downloading;

- Three (3) participants mentioned that the exhibits should be booked in the SAPS13 register as part of exhibit management;
- Three (3) participants stated that the cell phone and SIM card are analysed/ downloaded separately;
- Three (3) participants mentioned that the exhibits should be packaged and sealed in a forensic seal bag;
- Two (2) participants stated that the investigating officer must seize the cell phone and SIM card;
- Two (2) participants explained that the cell phone should be switched off and the SIM card removed;
- One (1) participant noted that the identified cell phone should be isolated from the cellular network;
- One (1) participant responded: “Dit word gedownload”, meaning it is downloaded;
- One (1) participant mentioned: “Die sim kaart word in ‘n device geplaas”, meaning that the SIM card is placed in a device;
- One (1) participant stated that the 212 Statement is sent back to the investigating officer with the downloaded information;
- One (1) participant explained that it is important to keep the cell phone switched on, and not to remove the SIM card;
- One (1) participant mentioned that the investigation officer should obtain the PIN number of the cell phone or pattern which must be written down and placed in forensic evidence seal bag;
- One (1) participant mentioned the importance of taking a photo in the event that something like a message showed on the front of the cell phone;
- One (1) participant mentioned that the investigating officer must send the cell phones to the TSU unit in Bishop Lavis, with some of the cell phones taken to at the Forensic Labs. So, they never handle the cell phone at the Police Stations; and
- One (1) participant noted that a statement must be completed, with a receipt form issued when delivering the exhibits.

Additionally, one (1) participant explained that it is important to remove the SIM card immediately in order to restrict the communication to the cellular network. The

investigating officers should either make use of the 'Faraday bags', but a challenge remains that only digital forensic investigators/ analyst is issued with these bags. The participant advised that the use of normal household foil or rice will suffice in restricting communication. The participant further advised on the importance of investigating officers' sealing of each exhibit separately and correctly, with one cell phone and SIM card in a forensic evidence seal bag. It is crucial for the cell phone to reach the digital forensic laboratory expeditiously in order to secure the information faster. The SIM card and cell phone are always analysed separately and not as a package.

When comparing the responses of the participants with the literature from authors such as Fick (2020:13) and (Jordaan, 2016:381), it is evident that the majority of the participants do not have a common understanding of the procedure to obtain data from a cell phone or SIM card. Evidently, the above extracts indicate the participants' informed understanding of the procedure for a cell phone and SIM card seizure, and obtaining data thereof. Each has his/her own version of the concept.

From a cell phone investigation viewpoint, it is crucial for the Police to follow strict protocols within the boundaries of the law and obtaining legal authorisation to perform such investigations. Based on the literature review and the responses of the participants in both Samples A, C, D and E, the researcher developed the following investigation framework, illustrating the operational steps of the procedure to obtain data from a cell phone or SIM card, as presented in Table 5.2 below.

Table 5.2: Operational steps of the procedure to obtain data from a cell phone or SIM card

Operational steps	Procedure to obtain data
Step 1: **Search and seizure**	• The investigating officer has to apply to a Magistrate or Judge for a search warrant, no Commissioned Officer may authorise a search warrant in respect of the CCA (Act No. 19 of 2020). • There should be reasonable grounds for requesting a search warrant. This must be submitted in an affidavit under oath or affirmation, and the articles requested to be seized must be described clearly. • It is important to obtain a search warrant that allows the investigating officer to legally seize a cell phone and or SIM card in terms of Section 29 (1) of the CCA (Act No. 19 of 2020). • Section 33 (1) of the CCA (Act No. 19 of 2020) allows for the search and seizure of an article described in

Operational steps	Procedure to obtain data
	Section 1 of the CCA (Act No. 19 of 2020) where consent is provided by a person with lawful authority to do so. The consent should be in writing for the search and seizure of the article, and also the access of the article in question.
Step 2: **Collection phase**	• A copy of the search warrant and affidavit used to obtain the search warrant should be handed over to the person whose property is being searched and seized. • After the search and seizure, the evidence should be properly documented by means of photography and a detailed scene report. • Immediately thereafter, the cell phone should be isolated from the cellular network to prevent its use in any further communications. • The cell phone should be placed on flight mode and placed in a Faraday bag (where possible) or even use normal household foil or rice. • Faraday bags are specifically designed for the storage of cell phones and blockage of wireless connectivity to the cellular network service provider on a temporary basis. • Obtain the PIN number or pattern used by the owner when unlocking the cell phone. This should be written on a piece of paper. • Place the exhibit with the PIN number or pattern in a forensic evidence bag and seal in front of the owner where possible. Each exhibit (each cell phone) should be sealed separately. • Important to note, no action should be taken by any Police official that will change the original form of the data on the data storage device.
Step 3: **Chain of custody**	• It is crucial for the investigating officer to institute a chain of custody for every exhibit collected or seized. The chain of custody is essential to uphold the integrity of the exhibits collected on the crime scene. • It is crucial for investigating officers to follow due processes when evidence is collected, until the evidence is presented in Court and proper documentation should be kept of who handle the exhibits and for what reasons. • Therefore, the investigating officer should book the exhibits in the SAPS13 register (SAPS stations) immediately after collection for safeguarding and exhibit management.
Step 4: **Apply for a secondary search warrant to obtain the data from the article (exhibits)**	• In terms of Section 33 (3) of the CCA (Act No. 19 of 2020), a Police official may only access or perform the powers referred to in paragraph (c) or (d) of the definition of ‘‘seize’’, in respect of a computer data storage medium or a computer system by means of a search warrant for the purpose of accessing the article. • The investigating officer should apply for a secondary search warrant in order to search the exhibits and copying of the data. The acquisition of data without the

Operational steps	Procedure to obtain data
	necessary legal authorisation constitutes an offence in terms of Section 37 (1) of the CCA (Act No. 19 of 2020).
Step 5: Deliver the article (exhibits) for acquisition	• The exhibits should be booked out of the SAPS13 register for further investigations, a copy of the search warrant permitting for the search of the exhibits and collection of data, as well as a detailed request letter should accompany the exhibits. • The exhibits should be booked in at the respective digital forensic laboratory, whether the Command Centre or DPCI for acquisition as soon as possible.

(Source: Concept developed by researcher)

The operational steps of the procedure to obtain data from a cell phone or SIM card above cover the search and seizure, collection phase, chain of custody, application for a secondary search warrant to obtain the data from the article (exhibits) and delivering the article (exhibits) for acquisition. The next section discusses the chain of custody of cell phones and SIM cards in greater detail.

5.3 CHAIN OF CUSTODY OF CELL PHONES AND SIM CARDS

Tamma and Tindall (2015:3) maintain that one of the key areas of forensic soundness premises on the importance of proper documentation of exhibits, especially from the start of the collection phase. Accordingly, Swanepoel et al. (2014:260) and Sammons (2015:7), describe chain of custody as the systematic processes that accounts for each piece of evidence, starting from the evidence collection until it is presented in Court. In that regard, the chain of custody is a record of movement to illustrate the route of the exhibit from the time of collection until the self-same exhibit is presented in Court (Dutelle, 2022:402; Houck & Siegel, 2015:31; Houck et al., 2018:16; Siegel & Mirakovits, 2016:36; Tamma & Tindall, 2015:3; Turvey & Crowder, 2017:9).

The chain of custody is a physical log for a specific exhibit tracking the movement and accounting for the custodianship of the exhibit, and the reason/s for such custody (Houck et al., 2018:16). The chain of custody is kept via exhibit registers, reports, evidence receipts, notes and statements (Sammons, 2015:7). According to Houck et al. (2018:16), every meaningful exhibit will eventually reach the Court and presented as evidence during the prosecution. Such a process emanates from the importance of the exhibit to the prosecution's case, and it is required of law

enforcement to correctly collect, mark, handle and transport the exhibit properly to establish the route of the exhibit. Houck and Siegel (2015:31) and Houck et al. (2018:16), believe that the chain of custody is arguably the single most important piece of paper generated on the crime scene. Therefore, a well-documented and maintained chain of custody is of utmost importance to guarantee the integrity of the evidence collected (Sammons, 2015:7).

It is advisable to designate one person to serve as the custodian of the evidence. In that regard, Dutelle (2022:96), Jordaan (2016:388), Kempen (2017:23, 24), Sammons (2015:152) and Zinn and Dintwe (2016:388) provide guidelines for seizing a cell phone and SIM card in order to ensure that the integrity of the evidence is kept. As such:

- The cell phone must be handled and preserved the same way as any other physical evidence;
- If the cell phone is password protected, the investigator should request the password from the owner where possible and write it a piece of paper;
- The code can be tested immediately in the presence of the perpetrator to determine whether the code is correct and valid;
- The cell phone must be placed on airplane/flight mode immediately to block cellular connection and the investigator must not access the cell phone at any stage, since the evidence may be altered or changed. Remove the SIM card immediately and placed in a separate evidence bag, this should be a set as a rule when seizing and handling cell phones evidence (Fick, 2020:13);
- If the cell phone is switched off, it should not be switched on, and if the cell phone is switched on, it must be placed in either a Faraday bag or wrapped with several layers of aluminium kitchen foil to isolate and insulate the cell phone from the cellular network service provider and extent battery life;
- Faraday bags are designed to store cell phones and temporary block wireless connectivity to the cellular network service provider (Afonin & Katalov, 2016:17; Tamma et al., 2018:9, 16; 2020:8);
- Cell phone chargers and connectors should also be seized and sealed in an adequate evidence sealing bag; and

- The seized cell phone must be placed in a secure area during transportation thereof, and the investigating officer must avoid placing the cell phone close to places with high magnetic fields, such as speakers. The cell phone must be handed in at the digital forensic laboratory as soon as possible for analysis purposes.

Fick (2020:13) explains that ideally, and where possible, the battery should be removed in order to avoid remote wiping of the cell phone data. Remote wiping is a function that allows for data and files to be accessed remotely and wiping all data and files stored on the cell phone (Boddington, 2016:62; Fick, 2020:13). Fick (2020:13) cautions investigating officers that in instances of arrest and a cell phone is seized, the perpetrators and their co-accused could wipe their data remotely. Fick (2020:13) further advises investigating officers to place the cell phone on airplane/flight mode or powering off the device, which prevents any attempts of remote wiping.

Fennelly and Perry (2018:29) and Ayers et al. (2014:33), recommend further that when the cell phone and SIM card are seized, the investigator/s should properly mark, pack and seal each exhibit in the correct and proper container or evidence sealing bag. The marking should be done in terms of the proper recognised Standard Operating Procedures (SOP) of the SAPS. Cell phones should be identified by means of their make, model, serial number and service provider if known (Ayers et al., 2014:37). Fick (2020:13) proffers that each item (cell phone, SIM card, memory card) should be collected and packaged separately as individual items. Each individual item contains different information that could be key to the investigation.

Turvey and Crowder (2017:27) maintains that each item or article seized or collected as evidence will be submitted at Court. Thereafter, a detailed chain of custody must be kept. Each person handling such exhibits and or taking custody thereof for analysis must note the date and time of receipt, and the reason for receipt must be stipulated in the chain of custody. Fick (2020:12) asserts that investigating officers should book the cell phone as evidence, and not as personal property when arresting a suspect and follow the correct procedures when booking it out for further investigation.

From a cell phone investigation viewpoint, the cell phone and SIM card is booked in the SAPS13 register (SAPS stations) immediately after collection. The SAPS13 register have different columns that make provision for date and time of handing in, relevant case and exhibit reference numbers, circumstances under which exhibit was collected, signature of the responsible person handing in the exhibit and the responsible person receiving such exhibit. The exhibit is then stored in the exhibit room for safekeeping. The SAPS13 register has a column that makes provision for date and time of booking out the exhibit, signature of the responsible person handing over the exhibit and the responsible person receiving such exhibit, and circumstances or reasons for booking out such exhibit. An additional occurrence book (OB) entry is made for each transaction. The exhibit should be booked out as soon as possible and submitted to the relevant office for downloading of the information.

In *Matshaba v S* 2016 ZANWHC 36 at paragraph 14, the Court held that the importance of proving the chain of custody is to prove that no alteration or substitution of the exhibits took place. The Court held further that when no admission is made by the defence team of the accused, the onus to prove the chain of evidence rests on the State. Furthermore, the Court held that failure from the State to prove the chain of evidence may affect the integrity of the presented evidence and rendering it inadmissible in Court. In another case *Botha v S* 2017 ZAECGHC 29 at paragraph 20, the Court held that the utmost important rationale to prove the chain of evidence, is to ensure that accused is not convicted on the foundation of possibly contaminated, altered or unreliable evidence.

Based on the critical analysis of the literature and case law, the researcher believes that it is evident that the chain of custody plays an integral role in ensuring that the integrity of the evidence is maintained. The onus rests on the State to prove that the evidence is not tampered with, and failure to do so could influence the State's case immensely. In supporting this view, Dutelle (2022:402) and Houck and Siegel (2015:19, 31) assert that when the chain of custody is not properly followed, the evidence may be rendered inadmissible in Court. From a cell phone investigation viewpoint, the cell phone can be analysed by extracting information from the device that is pertinent to the investigation. The SIM card can also be analysed to extract

relevant and essential evidence that could assist the investigating officer to determine ownership via RICA details. The next section discusses the process of cell phone and SIM card analysis in greater detail.

5.4 THE CELL PHONE (MOBILE) FORENSIC PROCESS

Cell phones have evolved into very important instruments for personal communication, but have also created a difficult situation for investigating officers to answer these pertinent investigative questions: who, what, where, when and how (Idris et al., 2016:75). Cell phones in our pockets are emblematic of a true technological marvel (Sammons, 2015:145). Most people are dependent on cell phones, which is enormously significant for forensic investigators to extract valuable data from these cell phones (Idris et al., 2016:75). Given the increasing levels of sophistication in cell phone technology, investigating officers are now compelled to gather and process evidence in non-traditional ways by thinking 'out of the box', rather than only adhering to the old 'tried and tested' methods of criminal investigation (Kader & Minnaar, 2015:67; Tahiri, 2016:4).

Therefore, investigating officers must seriously consider and understand the evidential value of cell phones in the investigation of crime, since a lot of crimes are linked to these cell phones. Cell phone (mobile) forensics is considered a relatively novel field, compared to other fields of digital forensics, such as computer and database forensics (Ali, Abd Razak, Othman & Mohammed, 2015:364; Tahiri, 2016:1). Cell phone (mobile) forensics is a process according to which cell phone devices are analysed in order to identify and collect evidence relating to a crime. Such analysis mainly focuses on the processing of the cell phone's external and internal memory and SIM card (Sai et al., 2015:4848; Tamma & Tindall, 2015:3; Tahiri, 2016:1).

From a cell phone investigation viewpoint, cell phone (mobile) forensics has a lot of potential and adds value to the investigation of crime. A lot of information can be obtained from a cell phone. Therefore, investigating officers should be highly knowledgeable and skilled in the processing of cell phones in a legally and forensically sound manner (Fick, 2020:15). Jordaan (2016:363) acknowledges that the cell phone (mobile) forensic process starts during the preliminary investigation

phase when the potential cell phone is identified and seized on the crime scene. Thereafter, the cell phone (mobile) forensic process continues with the further investigation phase during which the cell phone devices could be identified and seized as potential evidence.

Jordaan (2016:384) states that the pre-examination phase follows after the search and seizure phase, and consists of five particular phases that need to be adhered before any digital evidence can be investigated by a digital forensic investigator/analyst. These stages entail the following aspects:

- legal authorisation or mandate must be obtained for the investigation of the cell phone or other digital devices;
- the identification of all the legal elements and all allegations that need to be investigated in accordance with the legal authorisation obtained;
- the identification of all the possible cell phone or other digital devices that may comprise of the applicable digital evidence based on the legal authorisation;
- the seizure and transportation of the cell phone or other digital devices;
- the forensic acquisition of the digital evidence from the recognised cell phone or other digital devices; and
- forensic authentication of the digital evidence is acquired.

From the researcher’s viewpoint, the investigating officer is viewed as the gatekeeper in the process of obtaining digital evidence from cell phones. The process begins with the investigating officer who applies to the Court for obtaining legal authorisation by means of a warrant, subpoena or Court order to seize the relevant device/s and collect evidence from such devices. This is to ensure that the evidence is seized and collected legally within the boundaries of the law. A secondary search warrant should be obtained from the Court to allow for the search and acquisition of data from the cell phone in terms of Section 33 (3) of the CCA (Act No. 19 of 2020). Jordaan (2016:384, 391) and Sai et al. (2015:4848, 4849), confirm that it is essential for digital forensic investigator/analyst to know and understand the four phases in the cell phone (mobile) forensic process, namely: seizure; acquisition; analysis and reporting. Seizure of a cell phone he's discussed in greater detail hereafter.

5.4.1 Seizure

Basdeo et al. (2014:49), state that when an investigating officer collects evidence from computer-generated environments or mobile devices, the principal objective remains obtaining evidence in a legally and forensically sound manner. This serves the purpose of ensuring that the evidence is still admissible in a Court of law and in its preserved state for evidential integrity (Basdeo et al., 2014:49). Sai et al. (2015:4849), also allude that, there needs to be a seizure of the digital media before any analysis can take place. In many instances, a specialist digital forensic investigator/analyst will accompany the investigating officer with the task of correctly identifying, persevering and collecting the digital evidence (Sai et al., 2015:4849).

Section 1 of the CCA (Act No. 19 of 2020) addresses articles that can be seized as evidence to the Police and other law enforcement agencies – as discussed in more detail in table 5.1 of this research study. Section 31 (1) and Section 32 (1) of the CCA (Act No. 19 of 2020) provide that a Police official may seize items listed in Section 1 of the CCA (Act No. 19 of 2020) without a search warrant. Sai et al. (2015:4849), maintains that the cell phone seizure implies that all wireless networks should be blocked to prevent compromising of the evidence being sought and the various phases of investigation. It should be borne in mind that the primary objective of seizure is to preserve all evidence which can be useful in the investigation of crime.

From a cell phone investigation viewpoint, the seizure of the cell phone is primarily the task of the investigating officer in the case. However, the help of a digital forensic investigator/analyst can also be requested in the event that the investigating officer is unsure on the actual processes of seizure, isolation of the device and transportation thereof. The cell phone should be handed in at the digital forensic laboratory for examination and analysis as soon as possible. Jordaan (2016:384), Sammons (2015:7) and Tamma, et al. (2018:14), mention that the primary focus is to ensure that the digital forensic investigator/analyst has the proper and correct legal authorisation to forensically acquire any digital evidence, consequently investigating and analysing such evidence. Traditionally, this is performed by the investigating officer of the case, either by obtaining a search warrant to seize such digital devices, or by means of a subpoena or Court order, or even obtaining consent

from the lawful owner of the digital device in question. Jordaan (2016:389) cautions digital forensic investigators/analyst to make sure that all the fundamentals are observed, and that legal authorisation or consent has been granted because it is possible that the digital forensic investigator/analyst was not present during the seizure of the cell phone and SIM card. Jordaan (2016:389) further emphasizes that conforming to the legal issues is important, which was also referred to, in greater detail in paragraph 5.2 of this research. The second phase premises on acquisition, which is performed after the cell phone is legally seized and the preservation of digital evidence on the cell phone has been conducted (Sai et al., 2015:4849). The acquisition of digital evidence is discussed in more detail in the ensuing section.

5.4.2 Acquisition

Tahiri (2016:5) maintains that the acquisition of data must be performed in a manner that is acceptable, and with the necessary legal authority from the Court concerned. When the mobile device is admitted by the digital forensic laboratory, the investigating officer must submit the necessary documentation including the particular request for the evidence to be extracted from the device and its SIM card (Tamma & Tindall, 2015:3; Tamma et al., 2018:13; 2020:12). The details of the owner and the cell phone, where possible should be included in the documentation submitted to the digital forensic laboratory as part of the chain of custody (Tamma & Tindall, 2015:3; Tamma et al., 2018:13; 2020:12). In this regard, trained and qualified forensic experts should be examining and analysing cell phones to ensure the admissibility and reliability of the digital evidence contained on therein (Fick, 2020:13; Jordaan, 2016:380).

The cell phone in question is received at the digital forensic laboratory, after which the acquisition phase takes place with the digital forensic investigator/analyst identifying the cell phone type and model, as well as the selection of the correct methodology and method for the analysis phase (Sai et al., 2015:4849). Forensic imaging should be performed by proper trained and qualified digital forensic investigator/analyst who received training in forensic imaging of digital evidence and possess the proper tools and software to perform such an enormous task (Jordaan, 2016:388). Once the digital device is received, the digital forensic investigator/analyst develops a forensic image of the device, usually through a write

blocking device, a process referred to as imaging or acquisition (Boddington, 2016:57; Jordaan, 2016:388; Sai et al., 2015: 4849). Data acquisition/preservation relates to the process of taking an image or cloning the data from the cell phone (Alamin & Mustafa, 2015:16). Forensic imaging, on the other hand, is an exact duplication of all the data found on the cell phone or other digital devices (Jordaan, 2016:388). Boddington (2016:57) upholds that the imaging process is intended to copy all the relevant data from the particular suspected cell phone to the digital forensic investigator's/analyst's targeted device or workstation. Regardless of the massive advantages digital evidence provides to investigations, digital forensic investigators/analyst must be mindful that a small margin of tools is available which can help them in their assigned tasks (AlShehri, 2018:150).

In *S v Brown* 2015 ZAWCHC 128, evidence was presented that the Command Centre (War Room) is a newly created technical division of the SAPS that is responsible for downloading video surveillance material and data from cell phones. In addition, the DPCI also has a similar office that assists in digital forensic investigations. Lieutenant Colonel Linnen (employed at the Command Centre) presented evidence to the effect that the Command Centre uses a standardised form for cell phone analysis. Lieutenant Colonel Linnen (as quoted in *S v Brown* 2015 ZAWCHC 128) described the process of cell phone analysis as fairly simple. That is, the investigating officer completes the form and writes his/her request with regard to the cell phone analysis and data that is required.

The digital forensic investigator/analyst will then determine the extent of the investigation in relation to the request made by the investigating officer (Tamma et al., 2018:14). From a cell phone investigation viewpoint, these data include the cell phone's contact list, photographic and video images, as well as messages sent or received through the phone using various messaging formats. In *S v Brown* 2015 ZAWCHC 128 further evidence was presented to the effect that cell phone analysis was performed by means of a globally used Swedish computer software programme available to the SAPS since 2008. The software programme in question do not allow for any tampering of data on a phone, purposefully or accidentally. Lieutenant Colonel Linnen (as quoted in *S v Brown* 2015 ZAWCHC 128) testified that the cell phone is simply connected to a laptop containing the software programme, and it

proceeds to read all the data on the cell phone and downloads it into a file by applying the same Bluetooth principle. Boddington (2016:62) and Sai et al. (2015:4849), explain that the computer software programme simply connects the digital forensic investigator's analyst's workstation to the suspected cell phone, which allows for the retrieval/extraction of the required data through a sequence of commands and small adjustments in the settings. The forensic image is then created using a hard-drive duplicator or software imaging tools such as DCFLdd, IXimager, Guymager, TrueBack, or EnCase.

According to Boddington (2016:62), the leading software applications used to retrieve cell phone data is Cellibrite and Microsystemation's XRY. In a South African context, Lieutenant Colonel Linnen (as quoted in Schmitz and Cooper, 2016:327) maintains that the SAPS uses XRY and Analyst Notebook computer software programmes. The XRY is utilised to extract information from the seized cell phone and SIM card, while the Analyst Notebook is utilised to conduct link analysis between various cell phone and landline records (Schmitz & Cooper, 2016:327). Analyst Notebook was discussed in more detail in Section 4.5 in this research.

Jordaan (2016:390) maintains that it is essential for the investigating officer and the digital forensic investigator/analyst to work in conjunction with one another to ensure that they both understand the objectives of the investigation; as well as the kind of evidence required for the matter under investigation. From the researcher's viewpoint, the investigating officer should possess relevant technological knowledge and skills concerning the case under investigation, thus, placing the investigating officer in a position to lead the digital forensic investigation with a clear view of the exact nature of the evidence required and what purpose it will serve in the investigation insofar as supporting or contradicting the hypothesis of the investigating officer. The ensuing section discusses the next phase, namely, the analysis phase in more detail.

5.4.3 Analysis

According to Sai et al. (2015:4849), the contents of the forensic image files are analysed to identify evidence that either corroborates or contradicts the hypothesis of the investigation, or for signs of tampering and deleted evidence. In addition,

Alamin and Mustafa (2015:16) and Sammons (2015:7) state that the original data should under no circumstances be analysed because the original evidence can easily be modified or even be destroyed. Instead, a forensic image should always be used for analysis of the digital pieces inside the recovered data. Furthermore, Sammons (2015:8) illuminates that the type of analysis will depend on the facts and circumstances of the case under investigation. Some analyses can be time consuming and complicated, whereas others are less time consuming. Jordaan (2016:390) maintains that when potential and relevant evidence has been identified during the acquisition phase, the potential and relevant evidence will be examined and analysed by the digital forensic investigator/analyst in conjunction with the investigating officer to determine the relevance thereof to the matter under investigation.

Alamin and Mustafa (2015:15) and Jordaan (2016:391) state further that the analysis phase answers questions such as: what happened, why it happened, when it happened, where it happened, who is responsible, and how did it happen? The examiner usually recovers evidential material by employing various methodologies and tools to assist the identification and recovery process, often beginning with recovery of deleted material. During the analysis phase, evidence can be discovered from websites and search engines, timelines of particular events, any files opened, deleted or downloaded, as well as applications installed or uninstalled (Sai et al., 2015:4849; Sammons, 2015:8). The type of data recovered varies, depending on the investigation chat logs of the SMS conversations. Once the examiner recovers evidence, the information is then analysed to reconstruct events or activities in order to reach plausible or definitive conclusions.

During the critical stages of the analysis phase, every step of the process is documented again and verified through hashing techniques in order to keep track of the integrity of the evidence to ensure that it remains unchanged from its original state (Sai et al., 2015:4849; Tahiri, 2016:10; Tamma et al., 2018:17). Given the amount of data to be recovered, identifying relevant evidence is crucial in ensuring that the Court is not overwhelmed with irrelevant evidence (Jordaan, 2016:390, 391).

From a cell phone investigation viewpoint, the digital forensic investigator/analyst and the investigating officer should eliminate all unnecessary and irrelevant data that bears no relevance or contributes insignificant evidential value to the case under investigation. This will ensure that the Court is not unduly overworked due to evidence that has no impact or value, and does not assist the Court in its informed or independent decision-making. All the information that is relevant to a case must be drafted in the form of an affidavit or report, and submitted to the investigating officer for filing in the case docket.

The task of the digital forensic investigator/analysts is not only limited to acquisition and analysis, but also reporting and presentation of evidence in Court (Boddington, 2016:14). It is also the duty of the digital forensic investigator/analysts to interpret the findings to the investigating officer, the prosecution and the Court. From a cell phone investigation viewpoint, the digital forensic investigator/ analyst's interpretation of the findings will provide possible leads for further follow-up and collection of more evidence. This will ensure that the investigating officer has a prima facie case to present for prosecution. The aspect of reporting is discussed in more detail hereafter.

5.4.4 Reporting

According to Sammons (2015:9), whenever the cell phone (mobile) forensic process is performed, a report ought to be produced and provide adequate details of the process itself and the outcomes thereof. Jordaan (2016:391), meanwhile mentions that there are particular steps that needs to be completed before the digital forensic investigators/analyst presents his/her evidence in Court. The first step is that there must be a peer review of the digital forensic examination process to confirm accuracy and quality control of the processes followed until the reporting of the results (Jordaan, 2016:391; Tamma et al., 2018:17).

The digital forensic investigators/analysts must document each step or phase of the entire digital forensic examination process in the form of an affidavit or report (Jordaan, 2016:391; Sammons, 2015:153; Tamma & Tindall, 2015:9; Tamma et al., 2018:17). Sai et al. (2015:4849) and Tamma et al. (2018:17), maintains that the reporting phase illustrate the results from the analysis phase and the data gets

presented to assist the investigating officer. Once the examiner has completed the investigation, the information is drafted in a report which may include audit information and other meta-documentation. Jordaan (2016:391) adds that the digital forensic investigators/analyst affidavit or report must be reviewed as part of quality control measures and thereafter, the final affidavit or report is submitted to the investigating officer who is in charge of the case. The final reports are usually sent to the investigating officer to serve as evidence in Court (Sai et al., 2015:4849). The report will contain the written expert findings of the evidence as well as the evidence itself (Sai et al., 2015:4849; Tamma et al., 2018:18).

Particularly in criminal investigation, the digital forensic investigators/analysts should ensure that conclusions are based upon the recovered data and their own expert knowledge (Boddington, 2016:15; Sai et al., 2015:4849). Furthermore, the forensic expert must be able to produce a report on the findings of the cell phone analysis and will have to testify in Court on these findings as the authentic reflection of the digital forensic investigators'/analysts' analysis of the investigation in question (Boddington, 2016:15). A statement and findings in this regard should be drafted and produced in terms of Section 212 or 213 of the CPA (Act No. 51 of 1977).

From a cell phone investigation viewpoint, the statement received from the digital forensic investigators/analysts will contain attachments such as photographs, text, emails, and voice notes that can be used as evidence in the investigation. This might provide valuable leads that the investigating officer can pursued. The last step, ultimately, premises on the digital forensic investigator's/analyst's presentation of evidence in Court (Jordaan, 2016:391; Sammons, 2015:9). It is common cause that, in a criminal case, the Court will require the digital forensic investigators/analysts to present written expert conclusions by means of an affidavit, as well as the evidence itself (Sai et al., 2015:4849). Evidence cannot speak by itself, but requires the collector to interpret its factual and legal importance or relevance to the case (Boddington, 2016:14).

Alamin and Mustafa (2015:16) describe presentation of evidence as the reporting of evidence found during the analysis phase. On the other hand, Swanepoel et al. (2014:261), remarks that expert evidence is the case-related information which is presented in Court by a professionally trained, qualified, knowledgeable, skilled and

experienced person in their respective fields of specialisation and be regarded as an expert in that specific field. The extraction of data from cell phones is a complex process due to the inherent security functions and operating system of each device (Tamma & Tindall, 2015:8). As such, factors such as the operating system, the make and model of the cell phone, as well as the methods used to acquire data from the cell phone or SIM card in question will be chosen. Based on the arguments raised by Tamma and Tindall (2015:8), this research explores and describes the data recovery process in order to address and achieve the research aim, research objectives and questions of this study. Accordingly, the data recovery process and acquisition methods are discussed in greater detail hereafter.

5.5 THE DATA RECOVERY PROCESS

The data recovery process premises on the extraction/restoration/reconstruction of the actual data that has been hidden or even deleted from the image file of the cell phone or other mobile devices (Alamin & Mustafa, 2015:16; Tamma & Tindall, 2015:8, 9; Tamma et al., 2018:22; 2020:21, 22). It is virtually impossible to destroy digital evidence, and simply deleting the data files does not imply its complete removal. When criminals (think they) destroy digital evidence, traces and copies of the data files remain in places unknown to them, and can be recovered with the utilisation of specific forensic procedures and processes (Jordaan, 2016:372).

Due to advances in computer technology, the removed or deleted data can be recovered from accessible disk space, deleted (unallocated) space or from within operating system cache files. Therefore, the ultimate goal of cell phone (mobile) forensic investigations is to uncover and recover data stored on the device by applying well tested and forensically efficient techniques (Tamma et al., 2018:26; 2020:26). The type of data recovered will differ, depending on factors such as the nature of the investigation, the type of data; as well as pictures, emails, internet history, documents or chat application logs such as WhatsApp, Twitter, or Facebook. Different methods are utilised to recover and uncover evidence, which usually involves some form of search according to keywords from the recovered image file to either identify relevant matches of phrases or breaking down the recognisable file types (Sai et al., 2015:4849).

Some files are characterised by specific categories of bytes (such as graphic images) which identify the start and end of a file, from which a deleted file can be reconstructed if identified (Sai et al., 2015:4849). It is for such reasons that the digital forensic investigators/analysts should familiarise themselves with the different ways in which data can be retrieved from a cell phone (Fick, 2020:13). Boddington (2016:62) and Tamma and Tindall (2015:8, 9) acknowledge that cell phones are not imaged in the same manner as desktops and laptops. As such, the data recovery process is categorised into three categories, namely: manual, logical and physical acquisition - all of which are discussed in more detail below.

5.5.1 Manual acquisition

According to Tamma and Tindall (2015:8), manual acquisition is the simplest of the acquisition methods. For instance, no special software is required to perform this task. However, this method of acquisition's efficacy is limited because of the particular focus and emphasis on visible data extraction. In the manual acquisition mode of extraction, the investigator takes the actual cell phone device and manually scrolls through all the visible information therein; such as contacts, photos and records of calls generated or received (Tamma & Tindall, 2015:8; Tamma et al., 2018:22). This form of acquisition is quick and easy to apply on almost any cell phone. The evidence that has been recovered/discovered/uncovered is photographically documented in order to obviate the fallibility of human error, especially in the event of the digital forensic investigator/analyst being unfamiliar with the interface of the cell phone (Sammons, 2015:153; Tamma et al., 2018:22).

An unread message could display a "read" message because the digital forensic investigator/analyst opened the SMS to view the content of the communication therein (Tamma et al., 2018:22). Fick (2020:13) and Jordaan (2016:379) caution investigators not to pursue such action, as this could affect the evidence's admissibility in Court. The defence could also capitalize on such admissibility to cast aspersions on the integrity of such evidence placed before the Court. For instance, it could be alleged that the cell phone was tampered with in order to alter its contents, or that evidence was planted (meaning, the alleged perpetrator is being 'framed' for whatever nefarious purposes). It is possible for the contamination of evidence to take place, because accessing of the device will register the last

transaction and not the last date when the perpetrator accessed such device (Fick, 2020:13; Jordaan, 2016:379). The next acquisition method (i.e., logical acquisition) is discussed in more detail below.

5.5.2 Logical acquisition

Boddington (2016:62), Mikhaylov (2017:38) and Tamma and Tindall (2015:8, 9) describe logical acquisition or extraction as a process that allows for the extraction of certain logical data, such as phone books/contact lists, call log details, SMS and MMS messages received and sent, internet browser history, GPS location data, external and internal image data, internal and external video data, music, list of applications installed; as well as social media applications such as Facebook, and WhatsApp. Logical acquisition enables the investigator to access and retrieve the data which has not been deleted from the cell phone (Tamma et al., 2018:22).

Additionally, the logical acquisition technique is a quick and easy method normally used to describe the extraction or retrieval of data by connecting the cell phone to the forensic workstation via a normal USB or RJ-45 cable, infrared or Bluetooth (Tamma & Tindall, 2015:99). Once the cell phone is connected to the forensic workstation, a command is then sent to the cell phone's processor for delivery of the requested data. Through this acquisition process, a forensic image is created using a hard-drive duplicator or software imaging tools to avoid contamination or tampering, and the original drive is stored in secure storage to prevent any tampering or contamination (Sai et al., 2015:4848, 4849).

Sai et al. (2015:4848), caution digital forensic investigators/analyst to be mindful of acquiring data from memory extensions (such as SD Cards) as these devices may possess valuable data for investigation purposes. In this regard, almost no additional security for SIM cards exist and it can be easily bypassed by means of SIM cloning, which is a process whereby the digital forensic investigators/analyst copy the original content of the SIM card of the perpetrator to another sterile SIM card by using a computer programme (Al-Fayoumi & Shilbayeh, 2013:261; Tamma & Tindall, 2015:141). Anwar, Riadi and Luthfi (2016:75) and Singh, Chauhan and Khan (2015:26) mention that investigators can access SIM card by mounting the card in a standard smart-card reader to enable the SIM card's logical access by

software programmes. The data contents of the SIM card are then stored in a variety of files and in the form of binary data, which is extracted in a forensically proper manner and then analysed by a trained forensic analyst. A cloned SIM card does not have a PIN number, and cannot connect to the cellular network service provider. Therefore, the original SIM card is still inaccessible and protected by that PIN number (Tamma & Tindall, 2015:141). Physical acquisition is discussed in greater detail in the following section.

5.5.3 Physical acquisition

According to Tamma and Tindall (2015:9, 145) and Tamma et al. (2020:23), physical acquisition entails the creation of a bit-by-bit copy of the complete flash memory of the cell phone. The data extracted from the cell phone is in raw form and a forensic image is created, since all analysis are conducted on this forensic image which will ensure that the original data stays in the original form. According to Boddington (2016:57), a bit-by-bit copy acquisition mode is always preferred in the data recovery process.

However, according to Boddington (2016:62) and Tamma et al. (2020:23), physical acquisition, despite its time-consuming aspect, possesses the capacity to enable the digital forensic investigators/analyst acquisition of some deleted information on the cell phone. This form of acquisition is achieved by means of connecting the device to a forensic workstation (computer) and instructing the computer programme to extract information and ‘dump’ the memory of the device to the forensic workstation (computer). A physical dump relates to the process of creating a full copy of the entire device’s memory, and contains information relating to service data, application’s data and user’s data (Mikhaylov, 2017:38).

Basically, any text-based evidence can be extracted from the cell phone, such as emails, address books, instant messages, browsing history and many more (Tamma & Tindall, 2015:146; Tamma et al., 2020:23; Tahiri, 2016:39). Boddington (2016:58) and Sai et al. (2015: 4849), mention that the cell phone can either be returned to a secure storage to prevent tampering and damages, or handed back to the lawful owner after the digital forensic investigators/analyst has created the by bit copy of the complete flash memory of the cell phone in order to reduce the risk

of contamination or even hard drive failures. From the researcher's viewpoint, the investigating officer can book out the cell phone from the digital forensic laboratory and book it back to the relevant SAPS13 store (register) at the Police station. This will ensure the proper chain of custody and safekeeping of the cell phone until it is presented in Court. Given the potential valuable information that can be retrieved from a cell phone, the researcher finds it necessary to explore and describe the valuable information that cell phones hold in the investigation of crime in greater detail in the next section. Such an orientation also fulfils the purpose of addressing the research aim, research objectives and research questions entailed in this study.

5.6 VALUABLE INFORMATION THAT CELL PHONES HOLD IN THE INVESTIGATION OF CRIME

The evidence extracted from cell phones play a significant role in forensic investigation (Ali et al., 2015:365). Therefore, digital forensic investigators/analyst are advised to exercise extreme caution when dealing with cell phone devices such as smartphones, because three locations are used to store data: the SIM card essentially used to store contact particulars and texts; the device's memory where the user created data such as MMS, text messages, the operating system and settings are stored; and the device memory where portable application software and appropriate logs are stored.

When a cell phone is imaged (direct copy of the information on the cell phone), it has the potential and capacity to provide the investigating officer with the content of SMS's and MMS's, WhatsApp communication and other chat applications that offer essential evidence in the investigation (Fick, 2020:13). Furthermore, when digital evidence is mirrored, the copy can be examined without altering the original information because text messages are stored on the cell phone device rather than the SIM card (AlShehri, 2018:150; Jordaan, 2016:371). The implication is that the subscriber can place the SIM card in another cell phone device, but will not be able to view the existing text messages received or sent from that specific number, unless the subscriber manually relocates them to the particular SIM card (AlShehri, 2018:150).

According to Jordaan (2016:371), Sammons (2015:151, 154), Tamma and Tindall (2015:3), Tamma et al. (2018:25 & 26) and Tamma et al. (2020:25), evidence can be located on the device's memory, the SIM card and external storage card, commonly known as the memory or SD card. The following evidence can be extracted from the mobile device:

- Contact list: the names, numbers or even email addresses of contacts;
- Call history: the calls made, missed or received, and their duration;
- SMS: the texted contents of the received or sent messages;
- MMS: the media files such as videos and photographs sent or received;
- Email: the sent, received and drafted email communications;
- Web browser history: the history of websites visited;
- Photos: the images captured with the device's camera, downloaded from the internet, images sent via communication applications such as WhatsApp, telegram, and images transferred from one device to another;
- Videos: the videos captured using the device's camera, downloaded from the internet, images sent via communication applications such as WhatsApp, telegram, and images transferred from one device to another;
- Music: the music files downloaded from the internet, voice notes sent via communication applications such as WhatsApp, telegram, or transferred from one device to another;
- Documents: the files created using applications on the device, transferred from one device to another or even downloaded from the internet;
- Calendar: the appointments and calendar entries of the user;
- Network communication: the GPS location information;
- Maps: the places visited by the user, searching and downloading maps, and the direction searches;
- Social networking data: the information stored by social media platforms such as WhatsApp, Facebook, Twitter, and Telegram;
- Deleted data: the information that was erased or removed by the user; and
- Voicemail: the information pertaining to persons who called the subscriber and left a voice recorded message.

Based on the critical analysis of the literature, the researcher concludes that it is axiomatic that cell phones hold crucial information that is useful in the investigation of serious and violent crimes. Voluminous evidence is made available to the investigating officer's disposal in order to assist the process of proving the case under investigation. It is in this particular regard that digital or electronic techniques and strategies fulfil an important part of evidence collection in criminal investigations and prosecution thereof. In support, Lee and Pagliaro (2013:3) maintain unequivocally that cell phones can provide valuable leads and evidence that can be used to identify perpetrators of crime.

In addition, Afonin and Katalov (2016:10) add that there is also the internet footprint with browser logs, hidden geolocation data, videos and photographs taken with the internal cell phone camera, password of cloud services and social networks, and even stored payment details and shopping websites that may add valuable information or evidence to the investigation. Meanwhile, Graves (2014:314) contend that the functionality of a cell phone is rendered ineffective without a SIM card, other than making emergency calls only, given that SIM cards are absolutely essential for making or receiving phone calls, sending or receiving SMS's and browsing the internet. On this account, the ensuing section explores, describes and discusses the valuable information that SIM cards hold in the investigation of crime.

5.7 VALUABLE INFORMATION THAT SIM CARDS HOLD IN THE INVESTIGATION OF CRIME

Srivastava and Vatsal (2016:2) assert that SIM card forensics constitutes an important part of cell phone (mobile) forensic investigations. According to Shavers and Bair (2016:43, 44) and Singh et al. (2015:24), the Subscriber Identity Module or Subscriber Identification Module are commonly known as a SIM card, or a moveable memory chip that safely stores the subscriber's account-related information that is required for authentication of the service and details of the user. The SIM card is also referred to as the Integrated Circuit Card (ICC). Ibrahim, Al Naqbi, Iqbal and AlFandi (2016:219) provides a clearer description of the SIM card is a smart card which is utilised in cell phones for storage of the cellular network service provider's information required for communication functions.

The SIM card as a smart card with a non-volatile memory and contains a processor (Anwar et al., 2016:75). The SIM card is needed for cell phones to communicate and connect digitally (Srivastava & Vatsal, 2016:2). Accordingly, the SIM card is a major identity module whose functions include keeping record of names, phone numbers and network settings, and allows for the portability between phones (Sai et al., 2015:4848). Most importantly, the SIM card enables the separation of stored personal information from the actual cell phone device itself. Therefore, based on its capacity to store processed and reusable data of the subscriber, the SIM card is of great use and significance to the Police and crime investigators in their investigation of serious crime whose commission entailed the cell phone as a pivotal common denominator (Anwar et al., 2016:75; Singh et al., 2015:24).

As such, the handling and analysis of the data in the SIM card's memory is essential as evidence and should be handled in a forensically appropriate manner. Notwithstanding its nascent status as a developing area of forensic investigations, the SIM card is of immense value insofar as producing masses of evidentiary data to the investigators, given that they possess right knowledge and equipment to extract forensically-sound evidence (Ibrahim et al., 2016:231). For AlShehri (2018:150), the value of SIM card analysis derives from its clear, non-contradictory and impartial confirmation of a plethora of digital evidence for investigators.

From the researcher's point of view, the following eclectically derived attributes of the SIM card are relevant for purposes of forensic investigations (Afonin & Katalov, 2016:24; Anwar et al., 2016:71; Graves, 2014:314; Ibrahim et al., 2016:221; Idris et al., 2016:76; Singh et al., 2015:24-28; Srivastava & Vatsal, 2016:2, 4).

- SIM cards can hold important information such as the cell phone numbers, passwords to personal information of the subscriber, such as PIN (Personal Identification Number) and PUK (Personal Unblocking Code);
- SIM cards can hold personal information and professional messages, important contacts and call logs, as well as the cellular network service provider's details and Network Code;
- SIM cards contains crucial forensic evidence such as location data and a list of all cell towers to which it has recently connected;

- IMSI (International Mobile Subscriber Identity): a unique fifteen-digit number provided to the subscriber. The first three digits of the IMSI identify the Mobile Country Code, the following two or three digits identify the Mobile Network code (MNC) and the rest of the digit identifies the Mobile Subscriber Identification Number (MSIN);
- ICCID (International Circuit Card Identifier);
- Mobile Country Code (MCC) and Mobile Network Code (MNC);
- Mobile Station International Subscriber Directory Number (MSISDN): a unique number identifying a subscriber or cell phone number of the user;
- Abbreviated Dialling Number (ADN): any number and name dialled by the subscriber that is saved by the ADN;
- Last Dialled Number (LDN) and Short Message Services (SMS): the last sent or received messages;
- Language Preference (LP) and Card Holder Verification CHV1 & CHV2);
- Fixed Dialled Number (FDN): with this function, the subscriber does not have to dial a number by pressing any number of the phone pad. However, no SIM card has any detail about FDN;
- Local Area Identity or Location Area Information (LAI) and Own Dialling Number. The LAI is a unique identification number stored in the SIM card, and represents specific locations, by receiving service from the nearby mobile phone tower. Whenever the cell phone changes from one location to another, a new location and signal are activated;
- Temporary Mobile Subscriber Identity (TMSI) and Routing Area Identifier (RAI);
- Messages which were deleted can also be recovered from SIM cards;
- The stored data found in SIM cards are not destroyed by heat or flames, dust or soil, moisture, stains or magnetic fields. Environmental circumstances have no deleterious bearing on the stored data in SIM cards;
- Once the SIM card has been physically examined for physical damages, only then can a SIM card be rendered unreadable. However, scratches and striations do not render the SIM card unreadable;
- SIM cards can become unreadable when compression marks are created on the metallic circuit if damaged by stone, a hammer or bitten by teeth;

- Although a SIM card has become unreadable, it can become readable when the EEPROM chip are replaced into a new SIM card or by connecting it to proper probes;
- When a SIM card is discarded, it should be cut into pieces to avoid strangers from re-suing it and stealing private data through a SIM card reader; and
- In instances of suicide or accidental drowning, mass disasters or road accidents where the cell phone of the unknown victim was broken or turned off due to battery removal, the SIM card can be placed in a SIM card reader to extracted personal details of the victim;

The SIM card stores information relating to the cellular network service provider that is utilised for authentication and subscriber identification. Therefore, investigators should act quickly in the event that email server logs the content of email servers such as undelivered email, content of SMS and MMS message servers, or other IP address authentication logs are needed as evidence, because cellular network service providers only keep data for a limited period of time (Anwar et al., 2016:71; Ayers et al., 2014:52).

In a South African context, the cellular network service providers are obliged to preserve the data for a period of not less than three years. The data can still be used to identify communications between the people of interest which are linked to each other. The location area information is stored in the SIM card and receives cellular service from the nearest cell tower. Therefore, it is worth noting that when the cell phone changes locations, the location area information changes to a new location. The previous location area information visited by the cell phone is stored and kept.

Srivastava and Vatsal (2016:2) believes that it is a real advantageous point for digital forensic investigators/analysts because when a SIM card is examined, digital forensic investigators/analysts could form a general idea of the SIM card’s previous geographical location. In turn, such information allows digital forensic investigators/analysts to establish the movement of the cell phone, which can be relayed back to where the subscriber of the cell phone has been.

From a cell phone investigation viewpoint, the cell tower and sector locational information can only be obtained from the cellular network service provider in order to determine information about geographical movement of the subscriber or suspect. In *S v Brown* 2015 ZAWCHC 128, evidence was presented that ownership or subscriber details, cell phone and SIM card registration could only be obtained from the relevant cellular network service provider, and not through the software programme utilised by the SAPS. In terms of the RICA, it is important for investigators to establish which cellular network service providers is the specific number registered to the person/s of interest in the investigation (Shavers & Bair, 2016:39).

It is that regard that the investigating officer needs to complete the application for a Section 205 subpoena in terms of the CPA (Act No. 51 of 1977) to be issued by the Court requesting or instructing the cellular network service providers to formally avail the ownership details of the person who registered the SIM card with the particular cellular network service providers. Consequently, the cellular network service providers will be in a position to provide crucial and relevant information to the law enforcement agencies which is applicable to the investigation.

The following question was posed to participants in Samples A, B, C, D and E: “In your understanding, what information is stored on a sim card?”

This was an open-ended question which allowed the participants to freely respond according to their own experience and understanding. No optional answers were provided to the participants from which to select a possible answer. Some of the participants submitted multiple responses.

The responses of the participants in Samples A, C, D and E are reflected as follows:

- Seven (7) participants mentioned that the address book/contact list/phone numbers are stored on the SIM card;
- Six (6) participants explained that the SMS transactions and the content thereof is stored on the SIM card;
- Three (3) participants stated the cell phone number of the user is stored on the SIM card;

- Two (2) participants mentioned that the call logs are stored on the SIM card;
- Two (2) participants retorted that the last dialled numbers are stored on the SIM card;
- Two (2) participants stated the RICA details are stored on the SIM card (linked to a specific person if it is a contract);
- Two (2) participants mentioned the IMSI number and ICCID number are stored on the SIM card, and that it is the cell phone number and a SIM card number;
- One (1) participant noted the cellular network service provider's details are stored on the SIM card;
- One (1) participant noted that it shows the last used cell phone device – SIM profile;
- One (1) participant remarked: "normaalweg selfoon nommers", meaning that usually, cell phone numbers were stored, and "in verlede was daar meer inligting op" in the past there was more information stored;
- One (1) participant stated that photographs were stored;
- One (1) participant stated that emails were stored;
- One (1) participant mentioned that locational data was stored;
- One (1) participant alluded that not much information is stored in the SIM card, except the serial number;
- One (1) participant stated that the serial number of SIM card is linked to specific cell phone number;
- One (1) participant explains that the situation has changed over the years. Previously, the cell phone or SIM card was used to store messages and cell phone numbers and that was the purpose for a SIM card; and
- One (1) participant noted that with the improvement of smartphones, less information is stored on the SIM card.

The responses for the Sample B participants are reflected as follows:

- Two (2) participants mentioned that the address book/contact list/phone numbers were stored in the SIM card;
- One (1) participant explained that the SMS transactions and content thereof are stored on the SIM card;

- One (1) participant explained that smart phones store everything, and the SIM card stores nothing;
- One (1) participant mentioned personal information; and
- One (1) participant stated that the RICA details (linked to a specific person if it is a contract) were stored on the SIM card.

When comparing the responses of the participants for Samples A, C, D and E, it becomes clear that they (responses) were in consonance with literature as indicated by authors, Afonin and Katalov (2016:24), Anwar et al. (2016:71), Graves (2014:314), Idris et al. (2016:76), Ibrahim et al. (2016:221), Singh et al. (2015:24, 28) and Srivastava and Vatsal (2016:2, 4). On that basis, the researcher concludes that the majority of the participants have a good understanding of the nature of information stored on a SIM card. The responses of the participants are further supported by Srivastava and Vatsal (2016:2), who assert that data extracted from a SIM card could provide the digital forensic investigators/analysts with decisive evidence that is pertinent to an investigation. SIM cards provide a plethora of data which indicates the perpetrator's cellular history over a period of time. In many instances, some of this data could help an investigating officer to obtain information about the phone numbers of calls made or received, contacts, SMS details (i.e., time/date, recipient) and SMS text (the message itself).

When comparing the responses of the participants in Sample B, it becomes clear that the participants agree with the literature perspectives proffered by authors such as Shavers and Bair (2016:49), who mention that certain cell phones save contacts on their memory by default. With the ever-changing expansion and development of cell phones, more information is now stored directly on the cell phone itself. From the researcher's point of view, the participants in Sample B have a good understanding of the nature of the information stored on a SIM card. Based on the overall analysis of the literature, the researcher's own experience and the responses of the research participants in Samples A, B, C, D and E, the researcher agrees that the ever-increasing improvements in cell phone technology have induced a situation of less storage of information on SIM cards. The researcher also agrees that a SIM card is required for a cell phone to operate and communicate with the outside world.

From a cell phone investigation viewpoint, SIM cards still possess valuable evidence in the form of a cell phone number, which constitutes the foundational premises for requesting the cell phone records from a cellular network service provider. This information will form part of the Section 205 application, in terms of the CPA (Act No. 51 of 1977). In conclusion, SIM cards are still required to operate a cell phone, notwithstanding the rapid developments in the world of cell phone technology. The SIM card still possess crucial information that can add value to the investigation of serious and violent crime. In order to address and achieve the research aim, research objectives and questions of this study, the researcher discusses the evidential value of digital evidence in greater detail hereafter.

5.8 THE EVIDENTIAL VALUE OF DIGITAL EVIDENCE

In a Court of law, all adjudicated criminal and civil cases are dependent on admissible and relevant evidence which allows the presiding officer to make an independent and informed ruling (Schmitt & Jordaan, 2013:41). In legal proceedings, evidence is used to prove or refute matters of a case in dispute. In contemporary society and its 'mod cons', forensically obtained evidence has become an indispensable instrument in the Courts' prosecution of criminal and civil litigation (Boddington, 2016:56; Schmitt & Jordaan, 2013:40). Such prosecutions are enabled by the fact that digital evidence is relatively easily locate and processed, and that data obtained from the acquisition phase of investigation could provide essential information to prove a crime successfully (Boddington, 2016:66).

Jordaan (2016:373) maintains that the use of digital evidence collected on a cell phone and SIM card can answer important questions relating to matters under investigation, such as: what happened, when it happened, who interacted with whom, where the digital evidence originates from, and who is the responsible person that created the digital evidence? Furthermore, digital evidence can assist the investigating officer and the prosecution to develop a working hypothesis supported by the evidence, and can be used to develop links between the crime and the perpetrator; as well as the victim and the perpetrator (Boddington, 2016:56). Additionally, digital evidence could assume many forms, depending on the case under investigation and the device from which the evidence was retrieved (Boddington, 2016:57).

For example, in a case of fraud, the investigating officer could use the recovered emails to prove that the perpetrator sent those fraudulent emails from a particular cell phone. Emails contain valuable information, such as the date and time when it was sent to the victim in the matter being investigated. Jordaan (2016:370) contends further that digital evidence has become a central part of several criminal investigations, such as SMS messages sent and received between two offenders when planning a crime, captured cell phone video footage of crime being committed and emails that possess specific information concerning a crime. The files recovered from the cell phone contain useful background information in the form of file content and data, the date and time of creation, modification and last access (Boddington, 2016:62). Such information could be useful for the investigating officer to reconstruct the relevant details of the investigation and presented as digital evidence in legal proceedings through link analysis.

According to Boddington (2016:62) and Fick (2020:13), link analysis is the practice of systematically extracting information from cell phone records, the contact list and applicable communication applications such as WhatsApp and Telegram in order to comprehend the complex relations between different parties. Furthermore, link analysis will provide the investigating officer with a graphic illustration of the cell phone information and the relations between the data. Fick (2020:13) further states that a link analysis could be visually illustrated by combining the data in a graphical representation of the cell phone records obtained from the cellular network service provider and evidence obtained through the analysis of the cell phone. The investigating officer could produce a clearer picture of the communication patterns that transpired during the period under investigation. Such a picture accrues from the calls made and received between specific cell phone numbers and to other numbers; as well as the number of calls and owner details such as personal details and addresses based on the RICA data.

From a cell phone investigation viewpoint, link analysis is crucial to combine the evidence obtained from the cell phone and SIM card analysis and those of cell phone records obtained from the cellular network service provider. This allows the prosecution to present a clearer picture to Court concerning the interconnectedness of the evidence. Schmitt and Jordaan (2013:41) state that a key factor that the

Courts consider relates to the reliability of the digital evidence and the maintenance of the integrity of the digital evidence. Schmitt and Jordaan (2013:40) maintain that a critical element for cell phone (mobile) forensics and other forms of digital forensics is to ensure that the digital evidence remains unchanged from the moment of its acquisition, until its presentation in Court. This will ensure that the integrity of the evidence is kept at all times.

From a cell phone investigation viewpoint, digital evidence is the most common evidence produced during criminal prosecution or civil litigation, whether in the form of images and videos captured on the cell phone's internal camera or received via social media, phone books logs and emails. In essence, then, digital evidence could assist the investigating officer to expedite his/her investigation tasks (e.g., identification of perpetrators or victims) on account of its valuable information relating to the particular crime under investigation.

5.9 SUMMARY

In this chapter, the researcher explored the process and specific procedures that an investigating officer has to follow in order to obtain digital evidence from a cell phone and its SIM card. The researcher further proposed/ recommended an investigation framework in that regard. Additionally, the researcher outlined and discussed the applicable legislation previously utilised when dealing with digital evidence, the CCA (Act No. 19 of 2020) which took effect from 01 December 2021.

Also discussed in detail was the chain of custody of cell phones and SIM cards, as well as the importance of such custody, including other pertinent aspects such as the cell phone (mobile) forensic process, and its attendant data recovery process. The chapter further discussed the valuable information that cell phones and SIM cards hold in the investigation of crime as aspects of the evidential value of digital evidence in criminal investigation and proceedings. The next chapter focuses on the research findings, recommendations and the researcher's own concluding remarks on some specific aspect of the study and its findings.

CHAPTER 6: FINDINGS, RECOMMENDATIONS AND CONCLUSION

6.1 INTRODUCTION

This chapter concludes the study by focusing largely on the findings derived from the interview-based interactions with the sampled participants and the reviewed literature. The review of literature improved, broadened and strengthened the researcher's knowledge base in the field of study and enabled the development of his own recommendations and conclusions derived from the findings. The purpose of this research was to develop knowledge based on sound scientific findings. A subpoena obtained in terms of Section 205 of the CPA (Act No. 51 of 1977) instructs a person who possess or have control over relevant and critical information to provide such information to the relevant requester (i.e., investigating officer).

Based on the researcher's own personal and professional experience, it has been observed that most of the challenges presented by the participants concerning cell phone records analysis and the process thereof, are the outcome of the lack of training. Therefore, the researcher undertook this study in order to enhance knowledge on the process of obtaining and analysing cell phone records as prescribed in Section 205 of the CPA (Act No. 51 of 1977). In that regard, the current research further explored the investigative value of cell phone record analysis in the investigation of serious and violent crimes in the Winelands District, WCP.

The below-listed research questions were developed as the fundamental framework to achieve the aim of the study:

- What is the nature of crime investigation in South Africa?
- What is the meaning of cell phone records analysis?
- How are cell phone records analysed?
- What is the value of analysed cell phone records in the investigation of crime?
- What is the valuable information that cell phones and SIM card hold in the investigation of crime?
- What practical guidelines, procedures and recommendations can be offered to the SAPS to successfully use in analysing cell phone records in the investigation of serious and violent crimes?

Based on the above-mentioned questions, this chapter also entails the main findings accruing from the interviews with the participants. It is worth stating that the recommendations made by the researcher are not peripheral to the information obtained from the findings (Habib et al., 2014:11). Furthermore, the recommendations are also a reflection and product of the diverse range of data collection approaches embraced in this study: i.e., the literature review, document-based sources, semi-structured interviews; as well as the personal and professional experiences of the researcher.

As such, these recommendations pertain to the various stakeholders in the Winelands District, WCP. These are: serious and violent crime investigators; the NPA Prosecutors who prosecute serious and violent crime; Detective branch commanders who manage the investigating officers; Forensic investigators of the DPCI (Western Cape) who investigate cell phone related matters; as well as a cell phone analysis expert who performs cell phone record analysis.

6.2 MAIN FINDINGS

The main findings are categorised into the primary and secondary findings. The former (primary findings) address the research questions as articulated in Section 1.6 of this study. Meanwhile, the secondary findings are thematically premised on three critical aspects in criminal investigations, namely: The Lochner Principle, the process of obtaining cell phone records from the cellular network service provider; as well as the evidential value of cell phone records.

6.2.1 Primary findings

6.2.1.1 Research Question 1: What is the nature of crime investigation in South Africa?

From the various literature-based perspectives, the researcher objectively determined that crime is existent in every society and is part of the human nature and it is not unique to South Africa, but it is a globally issue. Crime is principally concerned with people's behaviour and all criminal activity is also concerned with people because crime can only be committed by people. Before any crime can be committed, there must be applicable government laws and rules in place, governed by the state (Eterno, 2012:4; Lochner, 2014:1).

Emanating from the consulted literature, the various responses from the research participants, it has been established that criminal investigation in South Africa predominantly focusses on the physical evidence collection. Physical evidence collection premise on the Locard Exchange Principle that premise on the notion that when two objects come into contact, the contact factor will cause a criminal to either leave his/her traces at the crime scene, or carry such traces away from the crime scene with him/her. Based on the views proffered by Lochner and Zinn (2014:161) of physical contact in cyberspace, the researcher found that new opportunities and possibilities for criminal investigation and crime scene processing have emerged, and that new possibilities become available because technology is improving rapidly.

From the researcher's perspective, the Lochner Principle is relatively new to the participants and that the majority of the investigating officers did not have an understanding of the Lochner Principle's properties, including its functionality and purposes. The SAPS members are trained with the focus on the physical evidence collection, instead of cell phone records – which are characteristically electronic and/ or digital. Accordingly, the researcher concludes that the majority of the participants did not receive any training regarding cell phone record analysis. In that regard, Cell phone analysis is a very grey area to them, as mentioned by one of the participants. On that basis, the researcher concludes that both the Locard Exchange Principle and the Lochner Principle are valid and relevant in criminal investigation.

6.2.1.2 Research Question 2: What is the meaning of cell phone records analysis?

From the various literature-based perspectives, the researcher objectively determined that, although the subscriber's detailed cellular activity is initially captured and stored for billing purposes, these details could also serve as evidence for criminal investigations. The information obtained from the cell phone records is useful evidence and can provide facts of the subscriber's location relating to cellular activity (Guigourés et al., 2015:1; Saravanan et al., 2013:125). In addition, Letouzé, Vinck and Kammourieh (2015:5) acknowledge that the investigating officer will be able to determine how the perpetrator communicated, and to which cell phone number communications were made. The identity of the receiving caller can also be

established, as well as identifying whether the caller was also in the same vicinity when the crime was committed. With regard to the participants' understanding, it was found that cell phone records constitute an important source of information pertaining to the activities and movements of the individuals who handled the cell phone; or whether the cell phone was moving (travelling). As such, the investigating officer will be in a position to narrow down the geographical location of the suspect when communications took place and place him/her in the geographical area close to the crime scene.

The researcher concludes that the participants had a reasonable understanding of the nature and the functioning of cell phone records. A cell phone record depicts the electronic history of the specific communication linked to specific cell phone number. The information obtained is stored with the cellular network service providers. Most of the participants used the term 'itemised billing' or 'detailed billing', although the dominant parlance in various literature sources refer to 'Call Detail Records (CDR)'. However, it still remains a document with detailed communications of the subscriber, irrespective of the terminological references used. In addition, the researcher concludes that a cell phone record is a document that indicates communication transactions registered with the cellular network service providers, and it shows detailed transactions that is more for billing purposes.

It is worth noting that the cellular network service providers record all cell phone activities and monetary transactions involved (where it is necessary). The data is generated every time the subscriber utilises the cellular network service provider to generate or to terminate communications. The cell phone record displays the following information: the cell phone number of the subscriber, IMSI/SIM card number, IMEI number, date and time of calls, call type (incoming or outgoing calls), the duration of calls made or received, the other party connecting or terminating the communication, date and time of SMS/MMS messages, the cell ID of the base station used during the communication, names of base stations and GPRS streaming. Overall, the participants in this study were general conversant with what a cell phone record entails, and the kind of information displayed on such a device.

6.2.1.3 Research Question 3: How are cell phone records analysed?

Emanating from the consulted literature, it has been established that cell phone records analysis can help investigators to determine the origin and nature of the committed crime; as well as the perpetrator's movements (Geldenhuys, 2018:13). Letouzé et al. (2015:5), describe the information available to the investigating officer from the cell phone record, the unique record identifier, the caller's phone number (unique to each caller), the receiver's phone (unique to each receiver), the starting date and time of the call, the duration of the call, caller cell tower locations and receiver cell tower locations and the call type activity (voice call, SMS, GPRS, and so on).

In tandem with the participants' understanding, it was found that cell phone records should be scrutinised to establish the links in communication, identify and highlight the cell phone numbers that are relevant to the investigation, and check the duration of calls or conversations. In addition, the investigating officer can view the locational data in order to narrow down the geographical location and movements of the subscriber/suspect. The date and time frames of the communication can be compared with the time when the crime was committed. The IMEI/handset profiling allows the investigating officer to determine which SIM cards were placed in the cell phone, and the detailed communication between the various parties (i.e., the number of calls made or received, SMS sent or received). On that basis, the researcher then concludes that the participants had a fair understanding of what cell phone records entails.

From the literature-based perspectives, it was found that when cell phone records are properly analysed, an interesting picture emerges, including an understanding of the various abbreviations and terminology used on the cell phone record. With regard to the researcher perspectives, each cell phone record received by the investigator from the cellular network service provider will include a list of the abbreviations and terminology, which is important for the investigating officers to understand in order to interpret the unfolding story in full. From the participant's perspectives, it was found that cell phone record analysis should be kept as uncomplicated as possible in order to allow the Court to understand the information better as well.

From the researcher's perspectives, the communication amongst of individual's can be colour coded to provide an easy distinction between the communicating parties. For example, suspect one (1) should be colour coded as red, and suspect two (2) as yellow, which will make it easy to distinguish the communication transactions between each of the two suspects. Accordingly, the researcher concludes that the majority of the participants did not receive any training regarding cell phone record analysis. In that regard, Cell phone analysis is a very grey area to them, as mentioned by one of the participants. The researcher then concludes that, although the participants had an idea of how to analyse cell phone records, the majority's understanding is based on self-taught or erudite knowledge and experience because there is no proper training programme/course within the SAPS.

6.2.1.4 Research Question 4: What is the value of analysed cell phone records in the investigation of crime?

From the literature-based perspectives, it has been established that cell phone record analysis is a valuable instrument in any investigation, whether in the form of cell phone records analysis or digital evidence contained on the device itself (Fick, 2020:15). From the participant's viewpoint, the analysis of a cell phone record entails evidential value in the investigation of serious and violent crime. Therefore, and what is irrefutably, the researcher concludes that cell phone record analysis is an invaluable crime investigation tool that can help solve the preponderance of serious and violent crimes in any criminal investigation. When cell phone records are properly analysed, it presents the investigating officer with voluminous evidence.

It was found that the following could be established through cell phone record analysis:

- Determining ownership of the cell phone based on the RICA information;
- Support the investigator's theory and suspicions;
- Leading the investigation and refuting or corroborating the version of a suspect, witness or victim;
- Establishing communication between suspects, witnesses or others;
- Linking the suspect to the crime scene;

- Establishing the geographical location/area of the suspect (subscriber) in respect of the cell tower and sector locations;
- Narrowing down the geographical location of the suspect's where about in respect of the cell tower locations;
- Establishing the possible travelling route of the suspect (subscriber) as directed by the cell tower and sector location information;
- Determining the possible speed travelled, based on the activation of cell phone towers;
- Establishing the duration of calls between suspects or witnesses to determine whether the conversation was short or long;
- Determining the frequency of communication between suspects as informed by the calls received and made, and SMS messages received or sent;
- Drawing of a time around the crime to determine whether there was planning and/or confirmed conspiracy; and
- Handset profiling to establish what SIM cards were inserted into the cell phone.

From the literature-based perspectives, it was established that the criminal justice system could benefit from a proper understanding of the value of mapping cell phone records and presentation of such evidence as physical evidence in Court. The researcher then concludes that analysing cell phone records is synonymous with the "DNA" of a cell phone. Similar to the DNA, analysed cell phone records are unique to a particular subscriber. Analysed cell phone records present the investigating officer with invaluable evidence that can help solve serious and violent crimes committed. The researcher compares the IMEI number of a cell phone and SIM card (IMSI number) to those of a unique and unduplicated fingerprint. The unique IMSI number provided to the subscriber has fifteen digits. On that account, the researcher concludes that the majority of the participants understands the importance of cell phone record analysis in the investigation of serious and violent crime.

6.2.1.5 Research Question 5: What is the valuable information that cell phones and SIM cards hold in the investigation of crime?

From a literature-based perspective, it was established that the cell phone's internal and external memory modules and SIM cards play an instrumental role as evidence

because an extensive volume of information is stored at those locations. Data extracted and collected from cell phone call records, e-mail messages recovered from a suspect's computer hard drive or cell phone, can provide crucial investigative leads for investigation (AlShehri, 2018:150). Furthermore, copious mounds of evidence can be found on the cell phone, as listed and described in Section 5.6 of this research by authors, Jordaan (2016:371), Sammons (2015:151, 154), Tamma and Tindall (2015:3), Tamma et al. (2018:25-26) and Tamma et al. (2020:25). A lot of valuable data about service providers and subscribers are stored on the SIM card, as listed and described in Section 5.7 of this research by authors such as Anwar et al. (2016:71), Afonin and Katalov (2016:24), Graves (2014:314), Idris et al. (2016:76), Ibrahim et al. (2016:221), Singh et al. (2015:24-28) and Srivastava and Vatsal (2016:2, 4).

Not all SIM cards have the relevant and necessary evidential data that can be useful during an investigation (Shavers & Bair, 2016:49). This is due to the technological advancements of cell phones, and the data usually stored on SIM cards are now kept in the cell phone's memory. Regarding the participants understanding of data stored in the SIM card, the participants listed the following: address book/contact list/ phone numbers; the subscriber's cell phone number; the SIM card's serial number; the cellular network service provider's details; call logs; SMS transactions; last dialled numbers and RICA details. In addition, various participants believe that in the past, more information was stored in the SIM card, but that has changed over the years with the smart phones storing more than the SIM card.

The researcher concludes that cell phones and SIM cards possess invaluable information that can is crucial in the investigation of crime. Based on the researcher's own experience, the ever changing and expansion of cell phone technology has introduced the storage of less and less information on the SIM card, with almost everything stored on the cell phone's memory. Although less information is stored on SIM cards, it still has a unique SIM card number and cell phone number specifically issued to that SIM card. It was also found that the value of cell phone and SIM card analysis cannot be underestimate, given the plethora of evidence linked to these devices.

From a literature-based perspective, it was found that the primary step for a digital forensic investigator/analyst is to ensure that the proper and correct legal authorisation for acquisition of forensic or digital evidence is obtained and followed to the spirit of the law. Traditionally, this is usually conducted by the investigating officer of a particular case, either by obtaining a search warrant to seize such digital devices, or by means of a subpoena or Court order; or even obtaining consent from the lawful owner of the digital device in question. Digital forensic investigators/analysts should ensure that all the legal parameters are adhered to, and that legal authorisation or consent has been granted, since it might be that the digital forensic investigators/analysts are present during the seizure of the cell phone and SIM card in question. The researcher concludes that it is crucial for the digital forensic investigator/analyst and investigating officers to work collaboratively, which will ensure that the digital forensic investigator/ analyst understands the objectives of the investigation and the kind of evidence required for the matter under investigation.

From a literature-based perspective, it was found that manual acquisition is the simplest form of acquisition methods available, and that no special software or methods is required to perform this method of data acquisition. The latter method is prone to human error, especially in the event that the digital forensic investigators/analysts are unfamiliar with the interface of the cell phone. Human error could also result in the alteration of the evidence. An unread message will show ‘read’ because the digital forensic investigators/analysts opened the SMS to view the contents of the communication. Consequently, contamination of evidence could take place because accessing the device will register the last transaction, and not the last date when the perpetrator accessed the device.

It was found further that, when the Courts consider the data messages’ evidential value, the following aspects are considered: reliability of the stored and communicated evidence gathering method; reliability of the integrity of the maintenance of data messages; as well as the manner of identifying the originator of these messages. It was found further that in a criminal case, the Court will usually require the digital forensic investigator/analyst to present written expert conclusion in the form of an affidavit of the evidence, as well as the evidence itself.

Given that evidence does not speak on its own, but requires human agency in the form of the collector explaining the importance and implications of such evidence to the case. The researcher concludes that investigating officers should equip themselves with the required knowledge and applicable skills, given the increased potential of digital evidence on matters under investigation. Therefore, it is of utmost importance for investigating officers to follow strict protocols and stay within the law when collecting evidence. In this regard, the SAPS should provide training and conduct workshops to equip its members and personnel on the processes of the search and seizure, collection and handling of digital evidence and maintenance of a proper chain of custody. In addition, it was found that a need exists for more experts in the field of forensic cell phone record analysis and digital forensic investigation and analysis.

6.2.1.6 Research Question 6: What practical guidelines, procedures and recommendations can be offered to the SAPS to successfully use in analysing cell phone records in the investigation of serious and violent crimes?

All fourteen (14) participants were provided an opportunity to make recommendations or suggestions that could be offered to the SAPS for the successful analysis of cell phone records in the investigation of serious and violent crimes. All of the participants mentioned once again that the SAPS should provide training in the field of cell phone record analysis. When asked whether they ever received any training regarding cell phone SIM card analysis, all the participants responded in the negative (i.e., “no”). Based on their Police experience, most of the participants found it necessary to be erudite (self-taught) in the rudimentary aspects of cell phone record analysis.

From the researcher’s perspectives, the SAPS should consider adopting the empirical findings of this study and theoretical/ abstract literature perspectives to draft a SOP or National Instruction dealing with cell phone record analysis and cell phone (mobile) forensics. The SOP or National Instruction should be implemented nationally to ensure a uniform or standard approach to conducting forensic cell phone and SIM card record analysis within the SAPS. In addition, the SAPS should provide training and conduct workshops to members with the deliberate intention of

equipping investigating officers with the required skills and knowledge to successfully conduct cell phone record analysis. Investigating officers should also be trained in Analyst Notebook where possible, since this is the fastest and easiest way to analyse digital information. Proper training should also be conducted on the processes and procedures of applying the Section 205 subpoena in terms of the CPA (Act No. 51 of 1977). The researcher then concludes that the investigating officer can follow the investigation framework containing the operational steps to obtain cell phone records, as developed and presented in Table 4.2 of this research. The researcher provided an illustration of cell phone record analysis in Section 4.5 of this research study.

In addition, the researcher has proposed an investigation framework to illustrate the operational steps for the procedure to obtain data from a cell phone or SIM card that can be adopted by investigating officers, shown in Table 5.2 of this research study. From the researcher's perspectives, the NPA should consider drafting their own SOP, directive or policy concerning the presentation of the cell phone record evidence in criminal trials. This will equip prosecutors with relevant knowledge, skills, and experience to understand cell phone record analysis and its value clearly. Furthermore, the SOP directive or policy will serve as a guide to Prosecutors when dealing with cell phone record analysis in trials.

6.2.2 Secondary findings

6.2.2.1 The Lochner Principle

From a literature-based perspective, it was established that criminal investigation is based on two (2) prominent and foundational principles, namely: the Locard Exchange Principle and the Lochner Principle. The Lochner Principle basically deals with the utilization of technological and scientific techniques to expose or reveal the invisible signal or traces left at a crime scene by mapping such signals through telecommunication techniques to render such traces visible. From the participants' perspective, it was found that the presence of a cell phone signal at the crime scene, is neither visible to the human eye, nor palpable or physically collectible when investigating the crime scene. From the researcher's perspectives, the cell phone record/activity are not left behind at the crime scene. However, the cell phone record/activity is captured and stored with the cellular network service

provider at an offsite location, which is not part of the crime scene and may even be many kilometres away. The researcher concludes that the majority of the investigating officers did not have an understanding of the Lochner Principle's properties, including its functionality and purposes. It is somewhat novel to the participants. From the researcher perspective and own experience, the SAPS members are trained with main focus on the physical evidence collection, with insufficient concentration on forensic cell phone records analysis. Accordingly, the SAPS should consider integrating the Lochner Principle within their training manuals and SOPs.

6.2.2.2 The Process of obtaining cell phone records from the cellular service provider

From the viewpoint of the participants, it was found that investigating officers should question the suspect on whether he/she possesses a cell phone. The next question should be directed at the cell phone number of the suspect. A follow-up question should then aim at finding out or determining whether there is any other person using the cell phone in question except the suspect. The questions and responses of the suspect should be captured and recorded in the suspect's warning statement, which in itself eliminates questions concerning the manner in which the cell phone number was obtained by the investigating officer.

Furthermore, it is the view of the researcher that it is important for the suspect to sign next to the entry, and the warning statement of the suspect can be used as evidence in Court to prove that the suspect in question gave the cell phone number, after which he/she signed next to it voluntarily and confirmed the correctness of the number provided. Such an orientation or approach will obviate the chance of a 'trial within a trial', to determine how the cell phone number was obtained by the investigating officer when applying for cell phone records from the cellular phone network provider.

From both the literature-based and the participants' perspectives, it was established and found that the cellular network service providers will only extract and supply cell phone records once the request has been duly pursued by means of the mandatory

legal protocols and procedures, and that prior approval and authorisation of the Section 205 subpoena in terms of the CPA (Act No. 51 of 1977) was obtained. Based on the participant's perspective, it was found that it is indispensable for the Section 205 application and statement of the investigating officer to be filed in the case docket as evidence. Based on the latter assertion, the researcher concurs that it is proof of the process followed by the investigating officer in obtaining the sought-after cell phone records from the cellular network service providers. This also strengthened the chain of custody.

From a literature-based perspective and the researcher's personal experience, it was established that the chain of custody is arguably the single most important piece of paper generated on the crime scene, and that a well-documented and maintained chain of custody is of utmost importance to guarantee the integrity of the evidence collected. From a case law perspective, it was found that the State will have to prove the chain of custody and the utmost important rationale to prove the chain of custody, which is to ensure that the person being accused is not convicted unfairly on the basis of possible falsification, contamination, or alteration - any, or all of which could compromise the evidential value of the investigation officer's exhibits presented before Court. Proving the chain of custody may affect the integrity of the presented evidence and render it inadmissible in Court. Accordingly, the researcher concurs that the chain of custody plays an integral role in ensuring that the integrity of the evidence is maintained.

From a literature-based perspective, it was found that the use of cloud services has created an enormous technical challenge for investigating officers because the information is not stored on the cell phone itself. Obtaining such information can only be retrieved from an international server outside of South Africa beyond the territorial jurisdiction of both South African law enforcement agencies and South African Courts. As such, the sought after information then becomes ultra vires in the South Africa legal context. Therefore, a local subpoena would not be sufficient to obtain the information that is required. It is then advisable for the investigating officer to acquire written consent from the suspect to search the cloud server and obtain the necessary information required for the investigation. In conclusion, the researcher proposed an investigation framework illustrating the operational steps

for the procedures to be followed by investigating officers when obtaining data from a cell phone or SIM card. The framework appears in Table 5.2 of this research study.

6.2.2.3 The Evidential Value of Cell Phone Records

From a literature-based perspective, it has been established that cell phone evidence (which is stored within the cellular network service providers' servers) is an instrumental tool in any criminal investigation. Such evidence is extracted from a cell phone, and analysed and interpreted as part of the preparations to submit the evidence to Court. In most cases, investigating officers request, collect and analyse cell phone records of a specific suspect(s) in a specific case, but this is not done against unsolved cases which may have the same modus operandi. From the researcher's perspective, it is evident that cell phone records analysis can help investigating officers to solve the current cases under investigation, and also unsolved cases which may provide critical information to identify and link other suspects to the crime or suspect.

The investigating officer can produce a clear picture of the communication that transpired during the period under investigation; the calls made and received between specific cell phone numbers and to other numbers; as well as the number of calls and owner details, such as personal details and addresses based on the RICA data. The researcher concludes that link analysis is essential in order to combine the evidence obtained from the cell phone and SIM card analysis and those of cell phone records obtained from the cellular network service provider. Link analysis allows the prosecution to present a clearer picture to Court in relation to the interconnectedness of evidence. Therefore, cell phone records analysis could not be underestimated, since it adds evidential value to the investigation of serious and violent crime.

The following section presents the researcher's recommendations. It should be mentioned that the recommendations themselves are not peripheral to the study, but are reflective of a concerted logical and thematically cohesive outcome of both the literature and empirical evidence of the study and also measure the extent to which this study has made a contribution to the field of study concerning the

phenomenon of criminal investigation (Alderson & Morrow, 2020:13; Fick, 2020:18; Bishnu & Bhattacherjee, 2018:268, 269; Creswell, 2015:19; Greenfield, 2016:47).

6.3 RECOMMENDATIONS

As outlined in Chapter 1 of this study, the aim of this research was to explore the investigative value of cell phone record analysis in the investigation of serious and violent crimes in the Winelands District, WCP. Based on the findings as explicated in the preceding section of this chapter, it could then be declared unequivocally that cell phone record analysis provides invaluable evidence when analysed properly, and that there is a compelling need for the training of SAPS members and personnel in this regard. With the ever-changing and transformation occurring in the technological realm, the training of investigating officers should also adapt to these inevitable advances in technology.

Given the evidential value of cell phone record analysis, the following recommendations are made, with particular emphasis on the SAPS and criminal investigators/analysts:

- The SAPS should consider developing and drafting a SOP or National Instruction with the view to improving cell phone record analysis and cell phone (mobile) forensics in the organisation. The SOP or National Instruction should be implemented nationally to ensure a uniform standard of conducting cell phone record analysis within the SAPS.
- The SAPS should consider adopting and implement the list of abbreviations and terminology used on the cell phone record, because no cell phone records can be properly analysed without such understanding. In this regard, the list of abbreviations and terminology as shown in Table 4.1 should be implemented in the SOP or National Instruction. It is important for investigating officers to know how to interpret the cell phone records that have been obtained.
- The SAPS should consider including a subject in cell phone record analysis within the detective training manuals and programmes, because cell phone record analysis is an invaluable crime investigation tool that can help solve the preponderance of serious and violent crimes, and any other criminal investigation.

- In addition, it is recommended that further training should be provided on the process of the Section 205 application procedure. This will ensure that investigating officers are properly equipped and trained to address crime, especially, serious and violent crime. The SAPS should integrate the Lochner Principle within their training manuals, SOPs and the National Instruction.
- The SAPS should train more investigating officers in the use of Analyst Notebook computer programme where possible, since this is the quickest and easiest way to analyse information.
- The SAPS should consider training more experts in the field of cell phone record analysis and digital forensic investigators/analyst to deal with the cell phone (mobile) forensics aspect. Moreover, the DPCI's digital forensic laboratory should be strengthened in terms of human resources (manpower) to deal with the volume of cell phone devices sent to the digital forensic laboratory.
- The investigating officers should be knowledgeable about the nature and value of digital evidence because of the increased potential of digital evidence in matters under investigation.
- The investigating officers and digital forensic investigators/analysts should not pursue the manual acquisition method of retrieving data from a cell phone, as such action could affect the admissibility of the evidence in Court. The defence could argue that the data on the cell phone was tampered with, altered or even fabricated. The investigating officers should adopt and implement a standardised process of operational steps to obtain cell phone records, which includes obtaining a cell phone number or IMEI number, completing the Section 205 application and drafting the investigating officer's statement, as well as the application process at Court and subpoenaing the cellular network service providers. In this regard, the researcher developed an investigative framework, as shown in Table 4.2, that outlines the operational processes that investigating officers should take to obtain cell phone records and should be evaluated for adoption and implementation. It is crucial for investigating officers to follow due processes when evidence is collected, until the evidence is presented in Court. Accordingly, proper documentation should be kept of who handled the exhibits, and for what reasons.
- Investigating officers should equip themselves on the processes of Section 205 of the CPA (Act No. 51 of 1977) which outline the mandatory legal protocols and

procedures that have to be pursued in order to obtain approval and authorisation for a Section 205 subpoena in terms of the CPA (Act No. 51 of 1977).

- Investigating officers should consider approaching the interviewing of suspects differently and consider asking questions based on whether the suspect possesses a cell phone, the cell phone number of the suspect, and any other user of the cell phone except the suspect. It is further recommended that the questions and responses of the suspect should be captured and recorded in the suspect's warning statement. The suspect should sign next to each entry in the warning statement, which will confirm that the information was given by the suspect himself/herself. This is essential in eliminating unnecessary questions on how the cell phone number was obtained by the investigating officer and the possibility of a trial within a trial to determine how the cell phone number was obtained by the investigating officer when applying for cell phone records.
- Investigating officers should keep a well-documented and maintained chain of custody which will guarantee the integrity of the evidence collected. The chain of custody is arguably the single most important piece of paper generated on the crime scene.
- Investigating officers should adopt and implement a standardised process of cell phone record analysis as illustrated in Section 4.5 of this research.
- Investigating officers should adopt and implement a standardised process of operational steps to obtain data from a cell phone or SIM card, which includes the search and seizure, collection phase, chain of custody, application for a secondary search warrant to obtain data from the article (exhibits), and delivery of the article (exhibits) for acquisition, as it is critical for the Police to follow strict protocols within the boundaries of the law.
- Investigating officers should consider analysing cell phone records against unsolved cases which may have the same modus operandi, and not only for one particular case under investigation. Cell phone records analysis can help investigating officers to solve current cases under investigation and unsolved cases which may provide critical information to identify and link other suspects to the crime or suspect.
- Investigating officers should consider keeping cell phone record analysis as simple and easy as possible which will allow the Court to understand the information better. The communications of individuals should be colour coded to

provide an easy distinction between the communications of various parties of interest.

- The NPA should consider drafting their own SOP directive or policy on the presentation of cell phone record evidence in criminal trials.
- This will equip prosecutors with understanding of cell phone record analysis better and the value thereof. The SOP, directive or policy will serve as a guide to Prosecutors when addressing issues of cell phone record analysis in trials.

6.4 CONCLUSION

This study was conducted with the aim of exploring the investigative value of cell phone record analysis in the investigation of serious and violent crimes in the Winelands District, WCP. The researcher reviewed both international and local South African scholarship for more insightful knowledge and understanding of the subject under investigation; that is, an exploration of the investigative value of cell phone record analysis in the investigation of serious and violent crimes in the Winelands District, WCP. The qualitative research approach permitted the involvement of human participants who provided the actual lived experiences as they are actively involved in the investigating serious and violent crimes (see Sample A, C and D). In addition, other data was gathered from the Sample B participants, who are prosecutors of serious and violent crime and present evidence on behalf of the State in a criminal trial. Other participants included a cell phone record analyst (Sample E).

The researcher established that there is great need for training within the field of cell phone record analysis and cell phone (mobile) forensics. The research aim was accomplished by responding to the research questions as clearly articulated in both Section 1.6 and 6.1 of this research study. The researcher is of the view that this study provides an important opportunity for all the relevant stakeholders in the justice system (the SAPS and NPA in particular) to develop a strategy for eliminating sophisticated criminal activities where cell phone record analysis is central in proving cases in Court. If adopted, the findings and recommendations in this study offer an important contribution to the SAPS and NPA in eradicating crime in South Africa. As a whole, the study also poignantly provided a crucial opportunity for the

researcher to consider further studies in the investigated field through doctoral research.

LIST OF REFERENCES

Abba, E., Aibinu, A.M. & Alhassan, J.K. 2019. Development of multiple mobile networks call detailed records and its forensic analysis. *Science Direct: Digital communications and networks,* 5:256–265.

Afonin, O. & Katalov, V. 2016. *Mobile forensics: Advance investigative strategies*. Birmingham, UK; Packt.

Africa Criminal Justice Reform. 2019a. The independence and structure of the prosecuting authority: Prosecutorial power and independence from political interference. Africa: ACJR Factsheet.

Africa Criminal Justice Reform. 2019b. Arrest without a warrant. Africa: ACJR Factsheet.

Alderson, P. & Morrow, V. 2020. *The ethics of research with children and young people: A practical handbook*. 2nd ed. London: Sage.

Ali, A., Abd Razak, S., Othman, S.H. & Mohammed, A. 2015. Towards adapting metamodeling approach for the mobile forensics investigation domain. Paper presented to the 1st ICRIL-International Conference on Innovation in Science and Technology (IICIST 2015): UniversitiTeknologi Malaysia, Kuala Lumpur, Malaysia, April 20th, 2015.

Ali, A., Abd Razak, S., Othman, S.H., Mohammed, A. & Saeed, F. 2017. *A metamodel for mobile forensics investigation domain*. Plos One.

Alvi, M.H. 2016. *A manual for selecting sampling techniques in research*. University of Karachi, Iqra University.

Al-Fayoumi, M.A. & Shilbayeh, N.F. 2013. *Cloning SIM Cards Usability Reduction in Mobile Networks*. New York: Springer.

Alhassan, J.K., Oguntoye, R.T., Misra, S., Adewumi, A., Maskeliūnas, R. & Damaševičius, R. 2018. *Comparative evaluation of mobile forensic tools* (Pp. 106-114). Rocha, Á & Guarda, T. (Eds) Advances in Intelligent Systems and Computing 721. Research Gate: Proceedings of the International Conference on Information Technology & Systems (ICITS 2018). Research Gate.

Al-Hadadi, M. & AlShidhani, A. 2013. Smartphone forensics analysis: A case study. *International Journal of Computer and Electrical Engineering*, 32(5):576-580.

AlShehri. M.A.R. 2018. A review of mobile and SIM forensics tools. JCSNS *International Journal of Computer Science and Network Security*, 32(18):150-154.

Alamin, A.A.M. & Mustafa, A.B.A. 2015. A survey on mobile forensic for android smartphones. *IOSR Journal of Computer Engineering*, 32 (17):15-19.

Anwar, N., Riadi, I. & Luthfi, A. 2016. *Forensic SIM Card Cloning Using Authentication Algorithm*. 32(4):71-81.

Ary, D., Cheser Jacobs, L., Sorensen Irvine, C.K. & Walker, D.A. 2019. *Introduction to research in education*. 10th ed. Boston: Cangage.

Aurini, J.D., Heath, M. & Howells, S. 2016. *The how to of qualitative research*. London: Sage.

Alshammari, H.Z. & Alghathbar, K.S. 2017. CLogVis: *Crime data analysis and visualization tool*. Paper presented to the AWICT '17: Association for Computing Machinery. Paris, France, November 13–14, 2017.

Anderson, J. & Poole, M. 2014. *Assignment & thesis writing*. South African edition. Cape Town: Juta.

Asiamah, N., Mensah, H.K. & Oteng-Abayie, E.F. 2017. *General, target, and accessible population: Demystifying the concepts for effective sampling*. 32(1):1607-1621.

Astalin, P.K. 2013. *Qualitative research designs: A conceptual framework*. 32(22):118-124.

Ayers, R., Brothers, S. & Jansen, W. 2014. *Guidelines on Mobile Device Forensics. USA*: National Institute of Standards and Technology.

Badenhorst, C. 2014. *Research writing. Breaking the barriers*. Pretoria: Van Schaik.

Babbie, E. 2014. *The basics of social research*. 6th ed. Belmont, CA: Wadsworth, Cengage Learning.

Babbie, E. 2017. *The basics of social research*. 7th ed. Boston, MA: Cengage Learning.

Bair, J. 2018. *Seeking the truth from mobile evidence: Basic fundamentals, intermediate and advanced overview of current mobile forensic investigations*. London: Academic Press.

Bak, N. 2013. *Completing your thesis: A practical guide*. Pretoria: Van Schaik.

Bard, J. 2019. *Tech troubleshooters: What is data mining?* New York: PowerKids Press.

Basdeo, V.M., Montesh, M. & Lekubu, B.K. 2014. *Search for and seizure of evidence in cyber environments: A law-enforcement dilemma in South African Criminal Procedure*. Pretoria: Unisa Press.

Bazeley, P. 2013. *Qualitative data analysis: Practical strategies*. London: Sage.

Baxter JR, E. 2015. *Complete crime scene investigation handbook*. Boca Raton: CRC Press.

Bell, J. & Waters, S. 2014. *A guide for first-time researchers*. 6th ed. Berkshire: Open University Press.

Belshaw, S.H. 2019. Next generation of evidence collecting: The need for digital forensics in criminal justice education. *Journal of Cybersecurity Education, Research and Practice,* 32 (2019) 1:1-20.

Bishnu, P. & Bhattacherjee, V. 2018. *Data analysis: Using statistics and probability with R language*. PHI Learning.

Bhattacherjee, A. 2012. *Social science research: Principles, methods, and practices*. 2nd ed. University of South Florida: Scholar Commons.

Bleck, J. 2015. *Education and empowered citizenship in Mali*. Baltimore: John Hopkins University.

Boddington, R. 2016. *Practical digital forensics: Get started with the art and science of digital forensics with this practical, hands-on guide!* Birmingham, UK; Packt.

Brown, R.M. & Davenport, J.S. 2016. *Forensic science: Advanced investigations*. Boston, MA: Cengage Learning.

Bruce, P.C. 2015. *Introductory statistics and analytics: A sampling perspective*. New Jersey: Wiley.

Bryman, A., Bell, E., Hirschsohn, P., Dos Santos, A., Du Toit, J., Masenge, A., Van Aardt, I. & Wagner, C. 2014. *Research methodology: Business and management contexts*. Cape Town: Oxford University Press.

Bryman, A. & Bell, E. 2015. *Business research methods*. 4th ed. United Kingdom: Oxford University Press.

Burchell, J. 2013. *Principles of criminal investigation*. 4th ed. Cape Town: Juta.

Case, S., Johnson, P., Manlow, D., Smith, R. & Williams, K. 2017. *Criminology*. United Kingdom: Oxford University Press.

Cassell, C. 2015. *Conducting research interviews for business and management students*. London: Sage.

Chambers, D. 2019. # CrimeStats/ Cops have lost the war, says Western Cape premier. Timeslive, 12 September 2019.

Chauvet, G. 2020. Introduction to sampling techniques (Pp. 1-22). In Ros, F. & Guillaume, S. 2020. *Sampling techniques for supervised or unsupervised task*. Switzerland: Springer.

Cho, J. 2018. *Evaluating qualitative research: Understanding methods qualitative research*. New York: Oxford University Press.

Clark, M.W. 2007. Cell phones as tracking devices. Valparaiso University: *Valpo Scolar*, 32(11):1413-1480.

Clark, T., Foster, L. & Bryman, A. 2019. *How to do your social research project or dissertation*. Oxford, United Kingdom: Oxford University Press.

Centre for Legal Terminology in African Languages. 2015. Legal Terminology: Criminal, Procedure and Evidence. Cape Town: Juta.

Curtis, K., Ramsden, C., Shaban, R.Z., Fry, M. & Considine, J. 2019. *Emergency and trauma care: For nurses and paramedics*. 3rd ed. NSW, Australia: Elsevier.

Corbin, J. & Strauss, A. 2015. *Basics of qualitative research: Techniques and procedures for developing grounded theory*. London: Sage.

Courtney, B. 2012. Introducing criminal investigation (Pp. 17-34). In Birzer, M.L. & Robertson, C. 2012. *Introduction to criminal investigation*. Boca Raton: CRC Press.

Creswell, J.W. 2013. *Qualitative inquiry and research design: Choosing among five approaches*. 3rd ed. London: Sage.

Creswell, J.W. 2014. *Research design: Qualitative, quantitative, and mix methods approaches*. 4th ed. London: Sage.

Creswell, J.W. 2015. *A concise introduction to mixed methods research*. LA, California: Sage.

Daltur, V. & Hajdarević, K. 2014. *Digital forensic investigation, collection and preservation of digital evidence*. Paper presented to the proceedings of the 5th International Symposium on Sustainable Development. Internacional Burch University: Sarajevo, Bosnia and Herzegovina, March 15-28, 2014.

Daniel, J. 2015. The foundation of good research (Pp. 511-552). In Guest, G. & Namey, E.E. 2015. *Public health research methods*. California: Sage.

Daniel, L. 2017. *Cell phone location evidence for legal professionals: Understanding cell phone location evidence from the warrant to the Courtroom*. London: Academic Press.

Daniels, B.K. 2019. What constitutes a good qualitative research study? Fundamental dimensions and indicators of rigour in qualitative research: The TACT framework. Paper presented to the proceedings of the 18th European conference on research methodology for business and management studies. Wits University, Johannesburg, South Africa, June 20–21, 2019.

Davis, F.T. 2019. *American criminal justice: An introduction*. United Kingdom: Cambridge University Press.

Denscombe, M. 2014. *The good research guide: For small-scale social research projects*. 5th ed. England: Open University Press.

Department of Communications. 2011. *RICA your SIM card*. South African Government News Agency, 13 June 2011.

Department of community safety Western Cape Government. 2019. *Western Cape crime report 2018/19*. Cape Town: Western Cape Government.

Dodge, A. 2017. *The digital witness: The role of digital evidence in criminal justice responses to sexual violence*. Canada: Sage.

Del Carmen, R.V. & Hemmens, C. 2017. *Criminal procedure; Law and practice*. 10th ed. Boston, MA: Cengage Learning.

Dutelle, A.W. 2017. *An introduction to crime scene investigation*. 3rd ed. Burlington, MA: Jones and Bartlett Learning.

Dutelle, A.W. & Becker, R.F. 2019. *Criminal investigation*. 5th ed. Burlington, MA: Jones and Bartlett Learning.

Dutelle, A.W. 2022. *An introduction to crime scene investigation*, 4th ed. Burlington, MA: Jones and Bartlett Learning.

Eckhardt, M. 2018. *The bumpy road to universal health coverage: Access to primary and emergency care in rural tropical Ecuador*. Sweden: LiU-Tryck.

Edwards, R. & Holland, J. 2013. *What is qualitative interviewing*? London: Bloomsbury.

Engel, R.S., Worden, R.E., Corsaro, N., McManus, H.D., Reynolds, D., Cochran, H., Isaza, G.T. & Cherkauskas, J.C. 2019. *The power to arrest: Lessons from research*. Switzerland: Springer.

Eterno, J.A. 2012. A brief history of criminal investigation (Pp. 3-16). In Birzer, M.L & Robertson, C. 2012. *Introduction to criminal investigation*. Boca Raton: CRC Press.

Faruque, S. 2019. *Radio frequency cell site engineering made easy*. Switzerland: Springer.

Fay, J.J. 2016. *Key terms and concepts for investigation: A reference for criminal, private, and military investigators*. New York: Routledge.

Ferraro, E.F. 2015. *Investigative interviewing psychology, methods and practice*. Boca Raton: CRC Press.

Fennelly, L.J. & Perry, M.A. 2018. *Investigations: 150 things you should know*. 2nd ed. Oxford: Butterworth-Heinemann.

Federal Bureau of Investigation Laboratory Division. 2019. *2019 Handbook of forensic services*. USA: Federal Bureau of Investigation.

Fick, J. 2020. Understanding evidence the benefits of cellphone (Pp. 12-15). In *Servamis community-based safety and security magazine*, 32(113):12-15. South Africa: Servamis.

Fish, J.T., Miller, L.S., Braswell, M.C. & Wallace Jr. E.W. 2015. *Crime scene investigation*. 3rd ed. New York: Routledge.

Flick, U. 2015. *The Sage handbook of qualitative data analysis*. London: Sage.

Flick, U. 2020. *Introducing research methodology*. 3rd ed. London: Sage.

Forensic Science Regulator. 2020. Forensic science regulator guidance: The control and avoidance of contamination in scene examination involving DNA evidence recovery, issue 2. Birmingham: Crown.

Gardner, R.M. 2012. *Practical crime scene processing and investigation*. 2nd ed. Boca Raton: CRC Press.

Gardner, T.J. & Anderson, T.M. 2016. *Criminal evidence: Principles and cases*. Boston, MA: Cengage Learning.

Gardner, R.M. & Krouskup, D.R. 2019. *Practical crime scene processing and investigation*. 3rd ed. Boca Raton: CRC Press.

Gehl, R. & Plecas, D. 2016. I*ntroduction to Criminal Investigation: Processes, practices and thinking*. New Westminster, BC: Justice Institute of British Columbia.

Geldenhuys, K. 2017a. Cell phone evidence: Digital DNA (Pp. 16-21). In *Servamis community-based safety and security magazine*, 32(110):16-21. South Africa: Servamis.

Geldenhuys, K. 2017b. The digital world's of Sherlock Holmes (Pp. 26-28). In *Servamis community-based safety and security magazine*, 32(110):16-21. South Africa: Servamis.

Geldenhuys, K. 2018. Evidence: It's all about listening to the silent voice of the crime scene (Pp. 10-16). In *Servamis community-based safety and security magazine*, 32(111):10-16. South Africa: Servamis.

Girard, J.E. 2018. *Criminalistics: Forensics, crime scenes, and terrorism*. 4th ed. Burlington, MA: Jones and Bartlett Learning.

Glenn, C. & Gray, L. 2016. *The hodges harbrace*. 19th ed. Boston, MA: Cengage Learning.

Graves, M.W. 2014. *Digital archaeology: The art and science digital forensics*. New Jersey: Pearson Education.

Grove, S.K., Gray, J.R. & Burns, N. 2015. *Understanding nursing research: Building an evidence-based practice*. 6th ed. Missouri: Elsevier.

Gray, J.R. & Grove, S.K. 2021. *Burns and Grove's. The practice of nursing research: Appraisals, synthesis, and generation of evidence*. 9th ed. Missouri: Elsevier.

Grove, S.K. 2021. Objectives, questions, hypothesis, and study variables (Pp. 129-150). In Grove, S.K. & Gray, J.R. 2021. *Burns and Grove's. The practice of nursing research: Appraisals, synthesis, and generation of evidence*. 9th ed. Missouri: Elsevier.

Greenfield, T. 2016. Ethics in research (Pp. 46-51). In Greenfield, T. & Greener, S. 2016. *Research methods for postgraduates*. 3rd ed. United Kingdom: Wiley.

Guigourés, R., Gay, D., Boullé, M., Clérot, F. & Rossi, F. 2015. *Country-scale exploratory analysis of call detail records through the lens of data grid models*. Paper presented to the Joint European Conference on Machine Learning and Knowledge Discovery in Databases 2015: Europe: Springer.

Guillemin, M., Barnard, E., Allen, A., Stewart, P., Walker, H., Rosenthal, D. & Gillam, L. 2018. Do Research Participants Trust Researchers or Their Institution? *Journal of Empirical Research on Human Research Ethics*, 2018, 32(13):285–294.

Habib, M.M., Pathik, B.B. & Maryam, H. 2014. *Research methodology. Contemporary practices: Guidelines for academic researchers*. Newcastle: Cambridge scholars publishing.

Haven, T.L. & Van Grootel, L. 2019. Preregistering qualitative research. *Accountability in research: Policies and quality assurance*, 32(26):229–244.

Hammond, M. & Wellington, J.J. 2013. *Research methods: The key concepts*. New York: Routledge.

Hayes, D.R. 2015. *A practical guide to computer forensics investigations*. New Jersey: Pearson Education, Inc.

Harding, J. 2013. *Qualitative data analysis from start to finish*. London: Sage.

Henning, E., Gravett, S. & Van Rensburg, W. 2013. *Finding your way in academic writing*. 2nd ed. Pretoria: Van Schaik.

Hennink, M., Hutter, I. & Bailey, A. 2020. *Qualitative research methods*. 2nd ed. London: Sage.

Hess, K.M., Orthmann, C.H. & Cho, H.L. 2013. *Police operations: Theory and practice*. 6th ed. New York: Cangage.

Hess, K.M., Orthmann, C.H. & Cho, H. L. 2017. *Criminal investigation*. 11th ed. Boston: Cangage.

Higginson, A., Eggins, E. & Mazerolle, L. 2017a. Investigating serious violent crime: What works, what doesn't and for what crime types. Report to the Criminology Research Advisory Council. *Criminology Research Advisory Council, Australia*, 32(43):1-87.

Higginson, A., Eggins, E. & Mazerolle, L. 2017b. Police techniques for investigating serious violent crime: A systematic review. Australian Institute of Criminology: *Trends & issues in crime and criminal justice*, 32(539):1-12.

Home Office. 2020. *Giving evidence in Court: Version 5.0*. USA: Home Office.

Honders, C. 2018. *Criminal profiling: Searching for suspects*. New York: Lucent Press.

Houck, M.M. & Siegel, J.A. 2015. *Fundamentals of forensic science*. 3rd ed. Oxford: Elsevier.

Houck, M.M., Crispino, F. & McAdam, T. 2018. *The science of crime scenes*. 2nd ed. London: Academic Press.

Hoy, J. 2015. *Forensic radio survey techniques for cell site analysis*. United Kingdom: Wiley.

Hunter, M. 2020. *Cops and call records: Perspectives on privacy, policing and metadata in South Africa*. South Africa: A report for the Media Policy and Democracy Project.

Ibrahim, N., Al Naqbi, N., Iqbal, F. & AlFandi, O. 2016. *Sim card forensics: Digital evidence*. Paper presented to the proceedings of the 16th Annual ADFSL Conference on Digital Forensics, Security and Law. Abu Dhabi: Conferences at Scholarly Commons. May 26th, 2016.

IBM i2 Analyst's Notebook. 2018. IBM i2 analyst's notebook: User help, version 9 release 2.

Idris, I., Alhassan, J.K., Waziri, V.O. & Majigi, M.U. 2016. *SIM Cards Forensic Capability and Evaluation of Extraction Tools*. International Conference on Information and Communication Technology and Its Applications. Nigeria, November 28 – 30, 2016.

Israel, M. 2015. *Research ethics and integrity for social scientists: Beyond regulatory compliance*. 2nd ed. London: Sage.

Janecek, A., Hummel, K.A., Valerio, D., Ricciato, F. & Hlavacs, H. 2012. *Cellular data meet vehicular traffic theory: Location area updates and cell transitions for travel time estimation*. Paper presented to the 2012 ACM Conference on Ubiquitous Computing (UbiComp '12). New York: UbiComp '12.

Jordaan, J. 2016. Digital forensics and cybercrime (Pp. 361-396). In Zinn, R. & Dintwe, S. 2016. *Forensic investigation legislative principles and investigative Practice*. Cape Town: Juta.

Joubert, C. 2015. *Applied law for Police officials*. 4th ed. Cape Town: Juta.

Kader, S. & Minnaar, A. 2015. Cybercrime investigations: Cyber-processes for detecting of cybercriminal activities, cyber-intelligence and evidence gathering. Acta Criminologica: Southern African Journal of Criminology Special Edition No 5/2015: Criminology in democratic South Africa: Coming of age.

Kay, J. & Wainwright, J. 2018. Data collection using qualitative methods (Pp. 135-165). In Carter, C. 2018. *Successful dissertations: The complete guide for education, childhood and early childhood studies students*. 2nd ed. London: Bloomsbury.

Kawthalkar, I., Jadhav, S., Jain, D. & Nimkar, A. 2020. Predictive crime mapping for smart city (Pp. 359-368). In Tripathy, A.K., Sarkar, M., Sahoo, J.P., Li, K. &

Chinara, S. 2020. *Advances in distributed computing and machine learning: Lecture notes in network and systems 127*. Singapore: Springer.

Kempen, A. 2017. Digital forensics: Offering more possibilities to convict criminals (Pp. 22-25). In *Servamis community-based safety and security magazine*, 32(110):16-21. South Africa: Servamis.

Khaldi, K. 2017. Quantitative, qualitative or mixed research: Which research paradigm to use. *Journal of Educational and Social Research*, 7(2):15-24.

Korstjens, I. & Moser, A. 2018. Series: Practical guidance to qualitative research. Part 4: Trustworthiness and publishing. *European journal of general practice*, 2018, 32(24):120–124.

Kingshott, B.F. 2015. Investigation of human trafficking (Pp. 91-118). In Palmiotto, M.J. 2017. *Combatting human trafficking: A multidisciplinary approach*. Baco Raton: CRC Press.

Kruse, C. 2016. *The social life of forensic evidence*. California: University of California Press.

Kumar, R. 2014. *Research methodology: A step by step guide for beginners*. 4th ed. London: Sage.

Kumar, S. 2015. *Wireless communication: The fundamental and advanced concepts*. Denmark: River.

Kumar, M., Hanumanthappa, M. & Suresh Kumar, T.V. 2016. *Crime investigation and criminal network analysis using archive call detail records*. 2016 IEEE Eighth International Conference on Advanced Computing (ICoAC). Chennai, India.

Kumar, R. 2019a. *Research Methodology: A step-by-step guide for beginners*. 5th ed. London: Sage.

Kumar, R. 2019b. *Nursing research & statistics*. 2nd ed. New Delhi: Jaypee.

Lamont, C. & Boduszyński, M.P. 2020. *Research methods in politics & international relations*. London: Sage.

Laws, S., Harper, C., Jones, N. & Marcus, R. 2013. *Research for development: A practical guide*. 2nd ed. London: Sage.

Lawrence, D.S., Gourdet, C., Banks, D., Planty, M.G, Woods, D. & Jackson, B.A. 2019. *Prosecutor Priorities, Challenges, and Solutions*. USA: Rand.

Leavy, P. 2017. *Research design: Quantitative, qualitative, mixed methods, arts-based, and community-based participatory research approaches*. New York: The Guilford Press.

Lee, H.C. & Pagliaro, E.M. 2013. Forensic Evidence and Crime Scene Investigation. *Journal of Forensic Investigation*, 32(1):1-5.

Letouzé, E., Vinck, P. & Kammourieh, L. 2015. *The law, politics and ethics of cell Phone data analytics*. Data-Pop Alliance white paper series. Data-Pop Alliance and the World Bank Group.

Lochner, H.T., Benson, B.C. & Horne, J.S. 2012. Making the invisible visible: The presentation of electronic (cell phone) evidence as real evidence in a Court of law. *Southern African Journal of Criminology. Acta Criminologica*, 32(2):69-82.

Lochner, H.T. & Zinn, R.J. 2014. Detecting invisible traces generated by a cellphone at a crime scene. *Acta Criminologica: Southern African Journal of Criminology*, 27(1):160-175.

Lochner, H.T. 2014. *Taking effective witness statements*. Cape Town: Juta.

Luton, L.S. 2015. *Qualitative research approaches for public administration*. New York: Routledge.

Majid, U. 2018. Research fundamentals: Study design, population, and sample size. *URNCST Journal*, 32(1):1-7.

Martin, V. 2016. Documenting your work (Pp. 34-45). In Greenfield, T. & Greener, S. 2016. *Research methods for postgraduates*. 3rd ed. United Kingdom: Wiley.

Mason, J. 2018. *Qualitative researching*. 3rd ed. London: Sage.

Masweneng, K. 2021. *Crime Stats: Murder and rape increased in past three months*. Timeslive, 19 February 2021.

Manly, B.F.J. 2015. Standard sampling methods and analysis (Pp. 7-32). In Manly, B.F.J. & Alberto, J.A.N. 2015. *Introduction to ecological sampling*. Baco Raton: CRC Press.

Mavodza, J. 2020. The evolving landscape of research methods in library and information science (Pp. 1-17). In Ngulube, P. 2020. *Handbook of research on connecting research methods for information science research*. Hershey, PA.USA: IGI Global.

Maxfield, M.G. & Babbie, E.R. 2018. *Research methods for criminal justice and criminology*. 8th ed. Boston, MA: Cengage Learning.

McDowell, W.H. 2013. *Historical research: A guide*. New York: Routledge.

McMahon, R.J. 2014. *Practical handbook for professional investigators*. 3rd ed. Boca Raton: CRC Press.

Merriam, S.B. & Tisdell, E.J. 2016. *Qualitative research: A guide to design and implementation*. 4th ed. San Francisco: Wiley.

Ministry of Police, Republic of South Africa. 2019. The official release of the annual crime statistics for financial year 2018/19.Cape Town: Ministry of Police, Republic of South Africa.

Mikhaylov, I. 2017. *Mobile forensics cookbook; Data acquisition, extraction, recovery techniques, and investigations using modern forensic tools*. Birmingham, UK; Packt.

Miller, M.T. 2018. *Crime scene investigation laboratory manual*. 2nd ed. London: Academic Print.

Miller, L.S., Hess, K.M. & Orthmann, C.S. 2018. *Community policing; Partnerships for problem solving*. 8th ed. Boston, MA: Cengage Learning.

Millen, P. 2015. Contamination (Pp. 31-35). In Houck, M.M. 2015. *Professional issues in forensic science: Advanced forensic science series*. Oxford: Elsevier.

Mogorosi, L.D. 2018. Ethics in research: Essential factors for consideration in scientific studies (Pp. 69-93). In Shokane, A.L., Makhubele, J.C. & Blitz, L.V. 2018*. Issues around aligning theory, research and practice in social work education. Knowledge pathing: Multi-, inter- and trans-disciplining in social sciences series*, 32(1). Cape Town: Aosis.

Monaghan, N. 2015. *Law of evidence*. United Kingdom: Cambridge University Press.

Monckton-Smith, J., Adams, T., Hart, A.G. & Webb, J. 2013. *Introducing forensic and criminal investigation*. London: Sage.

Niven, P.R. & Lamorte, B. 2016. *Objectives and key results: Driving focus, alignment, and engagement with OKRs*. New Jersey: Wiley.

Nowell, L.S., Norris, J.M., White, D.E. & Moules, N.J. 2017. Thematic analysis: Striving to meet the trustworthiness criteria. *International Journal of Qualitative Methods*, 32(16):1–13.

Osterburg, J.W. & Ward, R.H. 2015. *Criminal investigation: A method for reconstructing the past*, 7th ed. New York: Routledge.

Padgett, D.K. 2012. *Qualitative and mixed methods in public health*. Thousand Oaks, CA: Sage.

Palmiotto, M.J. 2013. *Criminal investigation*. 4th ed. Boca Raton: CRC Press.

Patten, M.L. & Newhart, M. 2018. *Understanding research methods: An overview of the essentials*. 10th ed. New York: Routledge.

Petrova, E., Dewing, J. & Camilleri, M. 2014. *Confidentiality in participatory research: Challenges from one study*. London: Sage.

Petrisor, I.G. 2014. *Environmental forensics fundamentals: A practical guide*. Boca Raton: CRC Press.

Phillips, A., Godfrey, R., Steuart, C. & Brown, C. 2014. *E-discovery; An introduction to digital evidence*. Boston: Cengage Learning.

Poole, F. 2015. Collection and chain of evidence (Pp. 27-30). In Houck, M.M. 2015. *Professional issues in forensic science: Advanced forensic science series*. Oxford: Elsevier.

Putman, W.H. & Albright, J.R. 2018. *Legal research, analysis, and writing*. 4th ed. Boston, MA: Cengage Learning.

Rees, C. 2016. *Rapid research methods for nurses, midwives and health professionals*. United Kingdom: Wiley.

Reilly, D.A. 2019. *Finding the truth with criminal investigation: Suspect, subject, defendant*. London: Rowman & Littlefield.

Resnik, D.B. 2018. *The ethics of research with human subjects: Protecting people, advancing science, promoting trust*. NC, USA: Springer.

Right2Know. 2016. The Surveillance State: Communications surveillance and privacy in South Africa. Media Policy and Democracy Project for the Right2Know campaign.

Robertson, B., Vignaux, G.A. & Berger, C.E.H. 2016. *Interpreting evidence: Evaluating forensic science in the Courtroom*. 2nd ed. United Kingdom: Wiley.

Roelofse, C. & Gumbi, M.G.C. 2018. *Policing in South Africa: Past and present*. Durban: LexisNexis.

Roulston, K. 2014. Analysing interviews (Pp. 297-312). In Flick, U. 2014. *The Sage handbook of qualitative data analysis*. London: Sage.

Rompf, S.A. 2015. *Trust and rationality: An integrative framework for trust research*. Manheim: Springer.

Roncacè, S. & Nicosia, U. 2016. "...*Every contact leaves a trace*...", Locard 1920 (Pp. 1008. Rend. Online Soc. Geol. It., Suppl. n. 1 al 32(40):1008. Società Geologica Italiana, Roma 2016: Research Gate.

Ros, F. & Guillaume, S. 2020. *Sampling techniques for supervised or unsupervised task*. Switzerland: Springer.

Ruel, E.E., Wagner, W.E. & Gillespie, B.J. 2016. *The practice of survey research: Theory and applications*. London: Sage.

SA-Venues.com. 2021. Paarl map. Available at: SA-Venues.com (accessed on: 28 February 2021).

Sai, D.M., Prasad, N.R.G.K. & Dekka, S. 2015. The forensic process analysis of mobile device. *International journal of computer science and information technologies*, 32(6):4847-4850.

Saini, M. & Kapoor, A.K. 2016. Biometrics in forensic identification: Applications and Challenges. *Journal of Forensic Medicine*, 32(1):1–6.

Saravanan, M., Thayyil, R. & Narayanan, S. 2013. *Enabling real time crime Intelligence using mobile GIS and prediction methods*. 2013 European intelligence and security informatics conference. Europe.

Sammons, J. 2012. *The basics of digital forensics: The primer for getting started in digital forensics*. MA, USA: Elsevier.

Sammons, J. 2015. *The basics of digital forensics: The primer for getting started in digital forensics*. 2nd ed. MA, USA: Elsevier.

Santos, R.B. 2017. *Crime analysis with crime mapping*. Radford University: Sage.

SAPS National Instruction Policy 1 of 2006. Research in the Service. 2006.

Schmitz, P.M.U. & Cooper, A.K. 2016. Forensic geography (Pp. 305-360). In Zinn, R. & Dintwe, S. 2016. *Forensic investigation legislative principles and investigative Practice*. Cape Town: Juta.

Schmitt, V. & Jordaan, J. 2013. Establishing the validity of Md5 and Sha-1 hashing in digital forensic practice in light of recent research demonstrating cryptographic weaknesses in these algorithms. *International Journal of Computer Applications*, 32(68):40-43.

Schneider, Z., Whitehead, D., LoBiondo-Wood, G. & Haber, J. 2013. *Nursing and midwife research: Methods and appraisal for evidence-based practice*. 4th ed. NSW: Elsevier.

Schönteich, M. 2014. *Strengthening Prosecutorial accountability in South Africa*. Pretoria: Institute for Security Studies.

Sennewald, C.A. & Tsukayama, J.K. 2015. *The process of investigation: Concepts and strategies for investigators in the private sector*. Oxford: Elsevier.

Shavers, B. 2013. *Placing the suspect behind the keyboard: Using digital forensics and investigative techniques to identify cybercrime suspects*. MA, USA: Elsevier.

Shavers, B. & Bair, J. 2016. *Hiding behind the keyboard: Uncovering covert communication methods with forensic analysis*. MA, USA: Elsevier.

Shih, C., Chen, F., Cheng, S. & Kaod, D. 2019. *Using google maps to track down suspects in a criminal investigation*. 23rd International conference on knowledge-based and intelligent information & engineering systems. Taiwan: Elsevier.

Siegel, J.A. & Mirakovits, K. 2016. *Forensic science: The basics*. 3rd ed. Boca Raton: CRC Press.

Singh, V.N., Chauhan, S. & Khan, G. 2015. Forensic analysis of SIM cards for data acquisition. *Asian Journal of Multidisciplinary Studies*, 32(3):24-28.

Silverman, D. 2014. *Interpreting qualitative data*. 5th ed. London: Sage.

Silverman, D. 2020. *Interpreting qualitative data*. 6th ed. London: Sage.

Skulkin, O., Tindall, D. & Tamma, R. 2018. *Learning android forensics; Analyze android devices with the latest forensic tools and techniques*. 2nd ed. Burminghum, UK; Packt.

South Africa. 1955. General Law Amendment Act 62 of 1955. Pretoria: Government Printers.

South Africa. 1965. Civil Proceedings Evidence Act 25 of 1965. Pretoria: Government Printers.

South Africa. 1996. Constitution of the Republic of South Africa 108 of 1996. Pretoria: Government Printers.

South Africa. 1977. Criminal Procedure Act 51 of 1977. Pretoria: Government Printers.

South Africa. 1998. National Prosecuting Authority Act 32 of 1998. Pretoria: Government Printers.

South Africa. 2002. Regulation of Interception of Communications and Provision of Communication-related Information Act 70 of 2002. Pretoria: Government Printers.

South Africa. 2002. Electronic Communications and Transmissions Act 25 of 2002. Pretoria: Government Printers.

South Africa. National Prosecuting Authority. 2008. Understanding the Criminal Justice System. Pretoria: National Prosecuting Authority.

South Africa. 2009. Second-hand Goods Act 6 of 2009. Pretoria: Government Printers.

South Africa. National Prosecuting Authority. 2013. Prosecution Policy. Pretoria: National Prosecuting Authority.

South African Police Service. 2019. South African Police Service Annual crime report, 2018/2019: Addendum to the SAPS annual report. Pretoria: National Commissioner.

South African Police Service. 2020. Detective Service News Bulletin. Pretoria: South Africa. 32(4):8.

South African Police Service. 2020. Cybercrimes Act 19 of 2020. Pretoria: Government Printers.

Smith, P.G., Morrow, R.H. & Ross, D.A. 2015. *Field trials of health interventions: A toolbox*. 3rd ed. Oxford University Press.

Srivastava, A. & Vatsal, P. 2016. *Forensic importance of SIM cards as a digital evidence*. Institute of Forensic Science and Criminology: Bundelkhand University, Jhansi, UP, India.

Srivastva, V.S. 2017. *Data analysis and interpretation*. New Delhi: S. Chand.

Stelfox, P. 2013. *Criminal investigation: An introduction to principles and practice*. New York: Willan.

Sultan, K., Ali, H. & Zhang, Z. 2018. *Call detail records driven anomaly detection and traffic prediction in mobile cellular networks*, 32(6):41728– 41737.

Sultan, K., Ali, H., Ahmad, A. & Zhang, Z. 2019. Call details record analysis: A spatiotemporal exploration toward mobile traffic classification and optimization. *MDPI journal: Information*.

Swanepoel, J.P., Lötter, S. & Karels, M.G. 2014. *Policing and the law. A practical guide*. Cape Town: Lexis Nexus.

Suboch, G. 2016. *Real-world crime scene investigation: A step-by-step procedure manual*. Boca Raton: CRC Press.

Tahiri, S. 2016. *Mastering mobile forensics: Develop the capacity to dig deeper into mobile device data acquisition*. Burminghum, UK; Packt.

Tarab, S. 2019. Becoming familiar with qualitative research (Pp. 1-24). In Gupta, M., Shaheen, M. & Reddy, K.P. 2019. *Qualitative techniques for workplace data analysis*. USA: IGI Global.

Tardi, S. 2019. Case study: Defining and differentiating among types of case studies (Pp. 1-19). In Baron, A. & McNeal, K. 2019. *Case study methodology in higher education*. USA: IGI Global.

Tamma, R. & Tindall, D. 2015. *Learning android forensics: A hands-on guide to android forensics, form setting up the forensic workstation to analysing key forensic artifacts*. Burminghum, UK; Packt.

Tamma, R., Skulkin, O., Mahalik, H. & Bommisetty, S. 2018. *Practical mobile forensics: A hands-on guide to mastering mobile forensics for the iOS, Android, and Windows Phone platforms*. 3rd ed. Burminghum, UK; Packt.

Tamma, R., Skulkin, O., Mahalik, H. & Bommisetty, S. 2020. *Practical mobile forensics: Forensically investigate and analyze iOS, Android, and Windows 10 devices*. 4th ed. Burminghum, UK; Packt.

Taylor, S.J., Bogdan, R. & DeVault, M.L. 2016. *Introduction to qualitative research methods: A guidebook and resource.* 4th ed. New Jersey: Wiley.

Thiel, S.V. 2014. *Research methods in public administration and public management: An introduction*. New York: Routledge.

Thomas, G. 2017. *How to do your research project: A guide for students*. 3rd ed. London: Sage.

Tight, M. 2017. *Understanding case study research: Small-scale research with meaning.* London: Sage.

Tight, M. 2019. *Documentary research in the social sciences*. London: Sage.

Tilstone, W.J., Hastrup, M.L. & Hald, C. 2013. *Fischer's techniques of crime scene investigation*. 1st international ed. Boca Raton: CRC Press.

Turvey, B.E. & Crowder, S. 2017. *Forensic investigation: An introduction*. London: Academic Press.

Theodorou, Y. & Yongo, E. 2018. *Access to mobile services and proof-of-identity: Global policy trends, dependencies and risks*. GSMA.

University of South Africa. 2016. Unisa policy on research ethics. Pretoria: University of South Africa.

University of South Africa. 2020a. Covid-19 Guidelines: Implication of Alert Levels for Researchers and Postgraduates' Students. Pretoria. University of South Africa.

University of South Africa. 2020b. University of South Africa COVID-19 Position Statement on Research Ethics.

United Nations Office on Drugs and Crime. 2014. The status and role of Prosecutors. A united nations office on drugs and crime and international association of Prosecutors guide. New York: United Nations.

Uzabakiriho, A. 2015. *The role of Forensic science in Criminal investigation in Rwanda*, 32 (3):1-4.

Vallabhaneni, S.R. 2015. Wiley CIAexcel exam review 2015: Part 1 internal audit basics. New Jersey: Wiley.

Vallabhaneni, S.R. 2019. Wiley CIAexcel exam review 2019: Part 3 business knowledge for internal audit. New Jersey: Wiley.

Van Niekerk, A. 2015. *The analysis of a cell phone record as a source of intelligence in the investigation of copper cable theft. MTech dissertation*. University of South Africa, Cape Town.

Van Rooyen, H.J.N. 2012. *The practitioner's guide to forensic investigation in South Africa*. Pretoria: Henmar.

Wall, D.S. 2017. *Understanding transnational organised crime: An academic research synthesis*. Leeds, University of Leeds.

Walliman, N. 2016. *Social research methods*. 2nd ed. London: Sage.

Walnycky, D., Baggili, I., Marrington, A., Moore, J. & Breitinger, F. 2015. *Network and device forensic analysis of android social-messaging applications*. USA: Elsevier.

Walker, R. & Solvason, C. 2014. *Success with your early years' research project*. London: Sage.

Walton, R.H. 2014. *Practical cold case homicide investigations procedural manual*. Boca Raton: CRC Press.

Wasunna, C., Tegli, J. & Ndebele, P. 2014. Informed consent in an African context (Pp. 57-62). In Kruger, M., Ndebele, P. & Horn, L. 2014. *Research ethics in Africa: A resource for research ethics committees*. Stellenbosch: SUN MeDIA.

WeatherSA Portal. 2020. Provincial demarcation. Available at: weathersa.co.za (accessed on: 25 August 2020).

Western Cape Government. 2019. Cape Winelands: At a glance. Western Cape: Cape Winelands District. Retrieved from: https://www.westerncape.gov.za/provincial-treasury/files/atoms/files/DC02%202019%20Socio-economic%20Profile%20-%20Cape%20Winelands%20District%20Municipality.pdf.

Willig, C. 2014. Interpretation and Analysis (Pp. 136-149). In Flick, U. 2014. *The Sage handbook of qualitative data analysis*. London: Sage.

Yin, R.K. 2014. *Case study research: Design and methods*. London: Sage.

Yin, R.K. 2016. *Qualitative research from start to finish*. 2nd ed. New York: Guilford Press.

Zare, H., Olsen, P., Zare, M.J. & Azadi, M. 2019. Comparing cellphones, global positioning systems (GPSs), email and network and cyber-forensics (Pp. 30-36). In Latifi, S. 2019. *Proceedings of the 16th International Conference on Information Technology: New generations (ITNG 2019)*. Switzerland: Springer.

Zinn, R. & Dintwe, S. 2016. *Forensic investigation legislative principles and investigative Practice*. Cape Town: Juta.

CASE LAW

BK and Another v Minister of Police and Others 2019 ZAWCHC 91

Botha v S 2017 ZAECGHC 29

Fisher v S 2018 ZAWCHC 15

Gcaza v S 2017 ZASCA 92

Gosschalk v Rossouw 1966 (2) SA 476 (C) at 490 – 493

Haysom v Additional Magistrate, Cape Town and another 1979 (3) SA 155 (C)

Khanye v S 2017 ZAGPJHC 251

Mahlangu v S 2019 ZAGPPHC 35

Matshaba v S 2016 ZANWHC 36

Mdlongwa 2010 (2) SACR 419 (SCA)

Motsagki v S 2014 ZAGPJHC 260

Naki v S 2018 ZAGPJHC 509

Nel v Le Roux NO and others 1996(3) SA 562 (CC)

Oosthuizen 2021 (1) SACR 278 (WCC) Magistrate for the District of Hermanus and Others

Sebaka v S 2019 ZAGPPHC 196

Seccombe and others v Attorney-General 1919 TPD 270

S v Brown (CC54/2014) 2015 ZAWCHC 128

S v Brown 2015 ZAWCHC 128

S v De Vries and others 2009 (1) SACR 613 (C)

S v De Vries and Others 2008 ZAWCHC 38

S v Dos Santos 2010 (2) SACR 382 (SCA)

S v Mani 2002 (2) SACR 393 (E)

S v Matisonn 1981(3) SA 302 (A)

S v Mayekiso 1996 (2) SACR 298 (C)

S v Miller 2015 JDR 1808 (WCC)

S v Miller and Another 2015 ZAWCHC 118

S v Motloutsi 1996 (1) SA 584 (C)

S V Mthetwa 1972 (3) SA 766 (A)

S v Ntsele 1998 (2) SACR 178 (SCA)

S v Sibisi and Another 2019 ZAGPJHC 3

S v Siebert 1998 (1) SACR 554 (SCA)

ANNEXURES

8.1 ANNEXURE A: UNISA ETHICAL CLEARANCE CERTIFICATE

UNISA university of south africa

UNISA 2021 ETHICS REVIEW COMMITTEE

Date: 2021:02:19

ERC Reference No. : ST14-2021

Name : DA Van Rooyen

Dear Donavin Adam Van Rooyen

Decision: Ethics Approval from 2021:02:19 to 2024:02:19

Researcher: Donavin Adam Van Rooyen

Supervisor: Prof J Horne

An exploration of the investigative value of cell phone record analysis in the investigation of serious and violent crimes in the Winelands District.

Qualification: MA Criminal Justice

Thank you for the application for research ethics clearance by the Unisa 2021 Ethics Review Committee for the above mentioned research. Ethics approval is granted for 3 years.

*The **Low risk application** was **reviewed** by the CLAW Ethics Review Committee on 19 February 2021 in compliance with the Unisa Policy on Research Ethics and the Standard Operating Procedure on Research Ethics Risk Assessment.*

The proposed research may now commence with the provisions that:

1. **The researcher will ensure that the research project adheres to the relevant guidelines set out in the Unisa Covid-19 position statement on research ethics attached. Provisional authorisation is granted.**

University of South Africa
Preller Street, Muckleneuk Ridge, City of Tshwane
PO Box 392 UNISA 0003 South Africa
Telephone: +27 12 429 3111 Facsimile: +27 12 429 4150
www.unisa.ac.za

2. The researcher(s) will ensure that the research project adheres to the values and principles expressed in the UNISA Policy on Research Ethics.
3. Any adverse circumstance arising in the undertaking of the research project that is relevant to the ethicality of the study should be communicated in writing to the CLAW Committee.
4. The researcher(s) will conduct the study according to the methods and procedures set out in the approved application.
5. Any changes that can affect the study-related risks for the research participants, particularly in terms of assurances made with regards to the protection of participants' privacy and the confidentiality of the data, should be reported to the Committee in writing, accompanied by a progress report.
6. The researcher will ensure that the research project adheres to any applicable national legislation, professional codes of conduct, institutional guidelines and scientific standards relevant to the specific field of study. Adherence to the following South African legislation is important, if applicable: Protection of Personal Information Act, no 4 of 2013; Children's act no 38 of 2005 and the National Health Act, no 61 of 2003.
7. Only de-identified research data may be used for secondary research purposes in future on condition that the research objectives are similar to those of the original research. Secondary use of identifiable human research data require additional ethics clearance.
8. No field work activities may continue after the expiry date **2024:02:19**. Submission of a completed research ethics progress report will constitute an application for renewal of Ethics Research Committee approval.

Note:

The reference number ST14-2021 should be clearly indicated on all forms of communication with the intended research participants, as well as with the Committee.

Yours sincerely,

Prof T Budhram
Chair of CLAW ERC
E-mail: budhrt@unisa.ac.za
Tel: (012) 433-9462

Prof M Basdeo
Executive Dean : CLAW
E-mail: MBasdeo@unisa.ac.za
Tel: (012) 429-8603

University of South Africa
Preller Street, Muckleneuk Ridge, City of Tshwane
PO Box 392 UNISA 0003 South Africa
Telephone: +27 12 429 3111 Facsimile: +27 12 429 4150
www.unisa.ac.za

8.2 ANNEXURE B: SAPS APPROVAL TO CONDUCT THE STUDY

SUID-AFRIKAANSE POLISIEDIENS **SOUTH AFRICAN POLICE SERVICE**

Privaatsak/Private Bag X 94

Verwysing/Reference:	3/34/2
Navrae/Enquiries:	Lt Col Joubert AC Thenga
Telefoon/Telephone:	(012) 393 3118
Email Address:	JoubertG@saps.gov.za

THE HEAD: RESEARCH
SOUTH AFRICAN POLICE SERVICE
PRETORIA
0001

A. The National Head
DIRECTORATE FOR PRIORITY CRIME INVESTIGATION

B. The Provincial Commissioner
WESTERN CAPE

PERMISSION TO CONDUCT RESEARCH IN SAPS: AN EXPLORATION OF THE INVESTIGATIVE VALUE OF CELL PHONE RECORD ANALYSIS IN THE INVESTIGATION OF SERIOUS AND VIOLENT CRIMES IN THE WINELANDS DISTRICT: UNIVERSITY OF SOUTH AFRICA: MASTERS DEGREE: RESEARCHER: DA VAN ROOYEN

A-B 1. The above subject matter refers.

2. The researcher, DA Van Rooyen, is conducting a study titled: An Exploration of the investigative value of cell phone record analysis in the investigation of serious and violent crimes in the Winelands District, with the aim ***to explore of the investigative value of cell phone record analysis in the investigation of serious and violent crimes in the Winelands District.***

3. The researcher is requesting to interview twelve (12) police members. The participants will include: six (6) Serious and Violent Crime investigators from Winelands District, two (2) Digital Forensic investigators from the Directorate for Priority Crime Investigation (DPCI) Western Cape, the Branch Commander: Stellenbosch Detectives, the Branch Commander: McGregor Detectives, the Branch Commander: Worcester Detectives and the Cell Phone analyst at Worcester police station.

4. The proposal was perused according to National Instruction 1 of 2006. This office recommends that permission be granted for the research study, subject to the final approval and further arrangements by the offices of the National Head: Directorate for Priority Crime Investigation and the Provincial Commissioner: Western Cape.

PERMISSION TO CONDUCT RESEARCH IN SAPS: AN EXPLORATION OF THE INVESTIGATIVE VALUE OF CELL PHONE RECORD ANALYSIS IN THE INVESTIGATION OF SERIOUS AND VIOLENT CRIMES IN THE WINELANDS DISTRICT: UNIVERSITY OF SOUTH AFRICA: MASTERS DEGREE: RESEARCHER: DA VAN ROOYEN

5. We hereby request the final approval by your office if you concur with our recommendation. Your office is also at liberty to set terms and conditions to the researcher to ensure that compliance standards are adhered to during the research process and that research has impact to the organisation.

6. If approval is granted by your office, this office will obtain a signed undertaking from researcher prior to the commencement of the research which will include your terms and conditions if there are any and the following:

6.1. The research will be conducted at his/her exclusive cost.

6.2 The researcher will conduct the research without the disruption of the duties of members of the Service and where it is necessary for the research goals, research procedures or research instruments to disrupt the duties of a member, prior arrangements must be made with the commander of such member.

6.3 The researcher should bear in mind that participation in the interviews must be on a voluntary basis.

6.4 The information will at all times be treated as strictly confidential.

6.5 The researcher will provide an annotated copy of the research work to the Service.

6.6 The researcher will ensure that research report / publication complies with all conditions for the approval of research.

7. If approval is granted by your office, for smooth coordination of research process between your office and the researcher, the following information is kindly requested to be forwarded to our office:

- **Contact person**: Rank, Initials and Surname.
- **Contact details**: Office telephone number and email address.

8. A copy of the approval (if granted) and signed undertaking as per paragraph 6 supra to be provided to this office within 21 days after receipt of this letter.

PERMISSION TO CONDUCT RESEARCH IN SAPS: AN EXPLORATION OF THE INVESTIGATIVE VALUE OF CELL PHONE RECORD ANALYSIS IN THE INVESTIGATION OF SERIOUS AND VIOLENT CRIMES IN THE WINELANDS DISTRICT: UNIVERSITY OF SOUTH AFRICA: MASTERS DEGREE: RESEARCHER: DA VAN ROOYEN

9. Your cooperation will be highly appreciated.

MAJOR GENERAL
THE HEAD: RESEARCH
DR PR VUMA

DATE: 2021-02-18

South African Police Service

South African Police Service

Private Bag X9004

Fax No: 021 417 7416

Reference: 25/7/2/1(202100037)

Enquiries: AC Gomo

Tel: 021 417 7520

Email: wc.od.research@saps.gov.za

PROVINCIAL COMMISSIONER
SOUTH AFRICAN POLICE SERVICE
WESTERN CAPE
8001

Mr DA Van Rooyen
03 Emerald Street
River Valley
Paarl
7646

PERMISSION TO CONDUCT RESEARCH IN THE SAPS: AN EXPLORATION OF THE INVESTIGATIVE VALUE OF CELL PHONE RECORD ANALYSIS IN THE INVESTIGATION OF SERIOUS AND VIOLENT CRIMES IN THE WINELANDS DISTRICT: RESEARCHER: DA VAN ROOYEN

1. We are pleased to inform you that your research application as stated above has been approved subject to the conditions stipulated on the legal documents attached.

2.1 In order for you to proceed with your research in the province, the following compulsory documents are attached for completion:

- Conditions
- Indemnity
- Undertaking

2.2 The above documents must be signed by yourself, as well as your supervisor and the originals returned to this office.

BRIGADIER
PROVINCIAL HEAD
ORG & STRATEGIC MNGT
PLETTENBERG BAY

BRIGADIER
PROVINCIAL HEAD: ORGANISATIONAL DEVELOPMENT AND STRATEGIC MANAGEMENT
WESTERN CAPE
PL VOSKUIL

Date: 2021/04/07

South African Police Service | Suid-Afrikaanse Polisiediens

Privaatsak Private Bag X94	Pretoria 0001	Faks No. Fax No.	(012) 393 2128

Your reference/U verwysing:

My reference/My verwysing: **3/34/2**

THE HEAD: RESEARCH
SOUTH AFRICAN POLICE SERVICE
PRETORIA
0001

Enquiries/Navrae: **Lt Col Joubert**
AC Thenga
Tel: **(012) 393 3118**
Email: **JoubertG@saps.gov.za**

APPROVED

DA Van Rooyen
UNIVERSITY OF SOUTH AFRICA

RE: PERMISSION TO CONDUCT RESEARCH IN SAPS: AN EXPLORATION OF THE INVESTIGATIVE VALUE OF CELL PHONE RECORD ANALYSIS IN THE INVESTIGATION OF SERIOUS AND VIOLENT CRIMES IN THE WINELANDS DISTRICT: UNIVERSITY OF SOUTH AFRICA: MASTERS DEGREE: RESEARCHER: DA VAN ROOYEN

The above subject matter refers.

You are hereby granted approval for your research study on the above mentioned topic in terms of National Instruction 1 of 2006.

Further arrangements regarding the research study may be made with the following office:

The National Head: Directorate for Priority Crime Investigation:

- **Contact Person:** Brigadier M Mohajane
- **Contact Details:** 084 9522 230 / 060 9976 687
- **Email Address :** MohajaneM@saps.gov.za

The National Head: Directorate for Priority Crime Investigation has stressed that the researcher must provide a copy of the research report to the Directorate for Priority Crime Investigation.

Kindly adhere to paragraph 6 of our attached letter signed on the **2021-02-18** with the same above reference number.

MAJOR GENERAL
THE HEAD: RESEARCH
DR PR VUMA

DATE: 2021-10-21

1

8.3 ANNEXURE C: NPA APPROVAL TO CODUCT THE STUDY

Administration

Enquiry: Mr. Marlua Bester
Email: mjbester@npa.co.za
Phone: 012 845 6274
Date: 23/03/2021

Tel: +27 12 845 6000

Victoria & Griffiths
Mxenge Building
123 Westlake Avenue
Weavind Park
Pretoria

P/Bag X752
Pretoria
0001

Mr. D. Van Rooyen
3 Emerald Street
Stone River Valley
Paarl
7646

RE: Request to Conduct Interviews with Prosecutors at Regional Courts in the Winelands District

Dear Mr. D. Van Rooyen

Thank you for showing interest in conducting research in the NPA. The purpose of this memorandum is to communicate the outcome of your request to conduct research.

The request to conduct interviews with Prosecutors at Regional Courts in the Winelands District is approved.

The NPA appreciates that the topic has been approved by the University of UNISA (Ethics clearance reference no: ST14-2021). Please consider and/or observe (whichever is applicable) the below-mentioned in support of your research:

1. The research request focuses on gathering information through interviews with Prosecutors at Regional Courts in the Winelands District.

Re: Request to Cond Request to Conduct Interviews with Prosecutors at Regional Courts in the Winelands District

2. Permission to conduct research is limited to interviewing selected NPA officials, and is subject to their availability and personal willingness to contribute to your research.
3. Permission is specifically subject to the stated research questions as stated in your research proposal.
4. Interviews with NPA officials should adhere to COVID-19 related Regulations.
5. It is requested that a copy of the report be sent to the NPA for perusal upon completion of the research project.
6. It is also requested that in the event of the author publishing an article on research which contains NPA information, such article should be shared with the NPA.
7. This approval letter is valid for 2 years from the date of approval by the Deputy National Director of Public Prosecutions: Strategy, Operations and Compliance. In case your research exceeds the above-mentioned timeframe, you will be required to re-apply.

In your case, there will be no need to complete "FORM A", which is the request for access to records of a Public Body, in terms of section 18(1) of the Promotion of Access to Information Act, 2000 (Act No. 2 of 2000), since your research study only involves interviews with selected officials.

Kindly keep the NPA informed about further developments on this research and please direct your correspondence to Ms. Kefentse Mojaki-Moremogolo on the following details:

Telephone number: 012 845 6506 / 073 079 8444
E-mail address: kmojaki-moremogolo@npa.gov.za

Yours sincerely

Adv. Anton Du Plessis
Deputy National Director of Public Prosecutions:
Strategy, Operations and Compliance
Date: 6/4/21

Re: Request to Conduct Interviews with Prosecutors at Regional Courts in the Winelands District

8.4 ANNEXURE D: INTERVIEW SCHEDULE FOR INVESTIGATORS

SAMPLE A: WINELAND DISTRICT: SERIOUS AND VIOLENT CRIME INVESTIGATORS
SAMPLE C: DPCI FORESNSIC INVESTIGATORS
SAMPLE D: WINELANDS DISTRICT: DETECTIVE BRANCH COMMANDERS

PARTICIPANT NUMBER: _____

TOPIC: AN EXPLORATION OF THE INVESTIGATIVE VALUE OF CELL PHONE RECORD ANALYSIS IN THE INVESTIGATION OF SERIOUS AND VIOLENT CRIMES IN THE WINELANDS DISTRICT, WESTERN CAPE PROVINCE

I am a post graduate student that is currently busy conducting research for the degree - Masters in Criminal Justice: Forensic Investigation at the University of South Africa. My supervisor is Prof Juanida Horne who can be contacted at the University on 012 433 9415 with regards to any matters pertaining to my research. The aim of this research is to explore the investigative value of cell phone record analysis in the investigation of serious and violent crimes in the Winelands District, Western Cape Province.

The following research questions will be answered in this study:

- Research questions 1: What do analysed cell phone records entail?
- Research questions 2: How are cell phone records analysed?
- Research questions 3: What value can analysed cell phone records add to the investigation of crime?
- Research questions 4: What valuable information do SIM cards hold in the investigation of crime?
- Research questions 5: What practical guidelines, procedures and recommendations can be offered to the SAPS to successfully use analysed cell phone records in the investigation of serious and violent crimes?

My research seeks to explore the investigative value of cell phone record analysis in the investigation of serious and violent crimes in the Winelands District, Western Cape Province. Your participation in this research is of major importance for the successful answering of the research questions. The researcher is bound to his assurances and guarantees by the research ethics code of the University of South Africa. The information you provide will be used in a research project for a Masters in Criminal Justice: Forensic Investigation at the University of South Africa. The analysed and processed data will be published in a research report. The interviewer will personally note your answers on paper and record the interview. Should any question be unclear, please ask the researcher for clarification. Only one answer per question is required. When answering the questions, it is very important to give your own opinion.

All interviews will be treated as strictly confidential

Your participation in this study is voluntary and can be terminated at any time. All responses will be treated with the utmost confidentiality by the researcher and all participants will remain anonymous. The names of the organisations participating in this will not be included. All participants will be allocated a number and completed interview schedules will be captured in an electronic database. All computerised notes will be stored on a secure, password-protected computer. Transcribed interviews will be kept in a secure place for a period of three years as required by the university rules. The transcribed interviews will thereafter be destroyed.

Research agreement between researcher and participant:

I undertake not to disclose your name. All information will be treated confidentially.

When reporting on the findings, no names of individuals or companies will be mentioned. You are free to terminate the questioning at any stage of the interview. The above information has been explained to me and I understand it. My name will not be disclosed, and I will allow my information or responses to be used in a confidential manner that will not harm me or my employer in any way and I am also aware that the thesis might be published in future. If you have any queries about this interview schedule, please contact 083 400 1647/ office 021 929 4995 and via email at Donnievr67@gmail.com .

Thank you for your cooperation.

…….

Masters in Criminal Justice: Forensic Investigation student

UNISA

_____ _____ _____

Signature of participant Place Date

PARTICIPANT

I hereby give permission to be interviewed and that information supplied by me can be used in this research.

YES	NO

SECTION A: BACKGROUND INFORMATION

1. What is your current rank in the SAPS?

_____

2. What is your gender?

A: MALE	**B: FEMALE**

3. How many years of service do you have in the SAPS? [Please mark the most relevant box.]

A: Less than 1 year	**B: 1 – 5 years**	**C: 6 – 10 years**	**D: More than 10 years**

4. What is your current position in the SAPS?

_____

5. How long have you served in this position? [Please mark the most relevant box.]

A	B	C	D
Less than 1 year	**1 – 5 years**	**6 – 10 years**	**More than 10 years**

6. Please specify your role with regards to the investigation of serious and violent crime?

_____

7. Do you have any formal qualifications? If yes, please elaborate.

_____

8. Have you attended any formal courses in your career as a detective? If yes, please elaborate on which courses you have attended.

_____

9. How many years of experience do you have in the investigation of serious and voilent crime? [Please mark the most relevant box.]

A	B	C	D
Less than 1 year	**1 – 5 years**	**6 – 10 years**	**More than 10 years**

10. Have you received any training regarding cell phone record analysis or sim card analysis? If yes, please elaborate.

_____

11. Have you ever testified in Court regarding cell phone record analysis or sim card analysis? If yes, please elaborate.

_____

SECTION B: CRIMINAL INVESTIGATION

12. In your understanding, how would you define criminal investigation?

_____

13. In your understanding, what are the objectives of criminal investigation?

_____

14. In your understanding, how would you define evidence?

_____

15. In your understanding, how would you describe identification?

_____

16. In your understanding, how would you describe individualisation?

_____

17. In your understanding, how would you describe the Locard exchange principle?

_____

18. In your understanding, how would you describe the Lochner Principle?

_____

19. In your understanding, how would you define serious and violent crime?

_____

SECTION C: CELL PHONE RECORD ANALYSIS

20. In your opinion, what is a cell phone record?

_____

21. In your experience, what information is displayed on a cell phone record?

_____

22. In your experience, how can the information displayed on the cell phone record be utilised during the investigation of serious and violent crimes?

_____

23. In your opinion, what type of evidence is cellphone records? Please elaborate.

_____

24. In your opinion, what relevance has cell phone records in the investigation of serious and violent crimes?

_____

25. In your opinion, what are the specific procedures that have to be followed by the investigating officer to obtain cell phone records?

_____

26. In your opinion, what are the responsibilities of an investigating officer with regards to cell phone record evidence?

_____

27. In your experience, what happens to the statement of the investigating officer that is submitted to request cell phone records?

_____

28. In your experience, what information should be contained in an investigating officer's statement when cell phone records are requested?

_____

29. In your opinion, what is the most important information that should be mentioned in an application to obtain cell phone records from a network service provider in terms of Section 205 subpoena of the Criminal Procedure Act 51 of 1977?

_____

30. In your opinion, what purpose does a Section 205 subpoena in terms of the Criminal Procedure Act 51 of 1977 fulfill in the investigation of serious and violent crime?

_____

31. In your opinion, what type of information can be requested from a network service provider in terms of Section 205 subpoena of the Criminal Procedure Act 51 of 1977 which can add value in the investigation of serious and violent crime?

_____

32. In your opinion, how are cell phone records analysed?

_____

33. In your opinion, what value can analysed cell phone records add to the investigation of serious and violent crime?

_____

34. In your experience, what practical guidelines, procedures and recommendations
can you suggest to the SAPS on how to analyse cell phone records?

_____

35. Based on your experience, what practical guidelines can you suggest on how to successfully obtain cell phone records from a network service provider in terms of section 205 of the Criminal Procedure Act 51 of 1977?

_____

36. In your opinion, what are the most important lessons you have learnt regarding the analysis of cell phone records in the investigation of serious and violent crime that you would want to share with others?

_____

37. Do you have any additional comments or suggestions regarding the analysis of cell phone records during the investigation of serious and violent crime have not been discussed?

_____

SECTION D: ANALYSIS OF SIM CARD DATA

38. In your understanding, what is a sim card?

_____

39. In your understanding, what information is stored on a sim card?

_____

40. In your experience, when a cell phone and sim card is seized, what is the procedure to obtain data from a sim card?

_____

41. In your opinion, how are the retrieved sim card data analysed?

_____

42. In your experience, how can sim card data analysis be useful during the investigation of serious and violent crimes?

_____

43. Based on your experience, what practical guidelines can you suggest on how to analyse sim card data in the investigation of serious and violent crimes?

_____

44. In your experience, what practical guidelines, procedures and recommendations can you suggest to the SAPS on how to analyse sim card data that appears on cell phone records?

_____

45. In your opinion, what are the most important lessons you have learnt regarding the analysis of sim card data that appears on cell phone records in the investigation of serious and violent crime that you would want to share with others?

_____

46. Do you have any additional comments or suggestions regarding the analysis of sim card data during the investigation of serious and violent crime have not been discussed?

_____

Thank you for participating in this interview.

8.5 ANNEXURE E: INTERVIEW SCHEDULE FOR NPA PROSECUTORS

SAMPLE B: PROSECUTORS FROM THE NPA

PARTICIPANT NUMBER: _____

TOPIC: AN EXPLORATION OF THE INVESTIGATIVE VALUE OF CELL PHONE RECORD ANALYSIS IN THE INVESTIGATION OF SERIOUS AND VIOLENT CRIMES IN THE WINELANDS DISTRICT, WESTERN CAPE PROVINCE

I am a post graduate student that is currently busy conducting research for the degree - Masters in Criminal Justice: Forensic Investigation at the University of South Africa. My supervisor is Prof Juanida Horne who can be contacted at the University on 012 433 9415 with regards to any matters pertaining to my research. The aim of this research is to explore the investigative value of cell phone record analysis in the investigation of serious and violent crimes in the Winelands District, Western Cape Province.

The following research questions will be answered in this study:

- Research question 1: What do analysed cell phone records entail?
- Research question 2: How are cell phone records analysed?
- Research question 3: What value can analysed cell phone records add to the investigation of crime?
- Research question 4: What valuable information do SIM cards hold in the investigation of crime?
- Research questions 5: What practical guidelines, procedures and recommendations can be offered to the SAPS to successfully use analysed cell phone records in the investigation of serious and violent crimes?

My research seeks to explore the investigative value of cell phone record analysis in the investigation of serious and violent crimes in the Winelands District, Western Cape Province. Your participation in this research is of major importance for the successful answering of the research questions. The researcher is bound to his assurances and guarantees by the research ethics code of the University of South Africa. The information you provide will be used in a research project for a Masters in Criminal Justice: Forensic Investigation at the University of South Africa. The analysed and processed data will be published in a research report. The interviewer will personally note your answers on paper and record the interview. Should any question be unclear, please ask the researcher for clarification. Only one answer per question is required. When answering the questions, it is very important to give your own opinion.

All interviews will be treated as strictly confidential

Your participation in this study is voluntary and can be terminated at any time. All responses will be treated with the utmost confidentiality by the researcher and all participants will remain anonymous. The names of the organisations participating in this will not be included. All participants will be allocated a number and completed interview schedules will be captured in an electronic database. All computerised notes will be stored on a secure, password-protected computer. Transcribed interviews will be kept in a secure place for a period of three years as required by the university rules. The transcribed interviews will thereafter be destroyed.

Research agreement between researcher and participant:

I undertake not to disclose your name. All information will be treated confidentially.
When reporting on the findings, no names of individuals or companies will be mentioned. You are free to terminate the questioning at any stage of the interview. The above information has been explained to me and I understand it. My name will not be disclosed, and I will allow my information or responses to be used in a confidential manner that will not harm me or my employer in any way and I am also aware that the thesis might be published in future. If you have any queries about this interview schedule, please contact 083 400 1647/ office 021 929 4995 and via email at Donnievr67@gmail.com .

Thank you for your cooperation.

Masters in Criminal Justice: Forensic Investigation student
UNISA

_____	_____	_____
Signature of participant	Place	Date

PARTICIPANT

I hereby give permission to be interviewed and that information supplied by me can be used in this research.

YES	NO

SECTION A: BACKGROUND INFORMATION

1. What is your current rank in the NPA (state advocate/senior state advocate/senior public Prosecutor/Prosecutor)?

_____

2. What is your gender?

A **MALE**	**B** **FEMALE**

3. What is your current position in the NPA?

_____

4. How long have you served in this position? [Please mark the most relevant box.]

A	B	C	D
Less than 1 year	**1 – 5 years**	**6 – 10 years**	**More than 10 years**

5. How many years of service do you have as a Prosecutor? [Please mark the most relevant box.]

A	B	C	D
Less than 1 year	**1 – 5 years**	**6 – 10 years**	**More than 10 years**

6. What is your highest formal qualification?

_____

7. How many courses did you attend during your career as a Prosecutor?

_____

8. What is your experience as a Prosecutor with regards to serious and violent crime?

_____

9. Did you receive any training with regards to cell phone record analysis or sim card analysis?

_____

10. Have you prosecuted any criminal cases which involved section 205 subpoena for cell phone records in terms of Criminal Procedure Act 51 of 1977?

YES	NO

11. If you answered 'yes' to question 10, please indicate how many cases have you prosecuted using cell phone records obtained through a section 205 subpoena in terms of CPA 51 of 1977.

TOTAL CASES	MARK WITH X
01 - 05	
06 - 10	
11- 15	
16 - 20	
21 - 30	
31+	

SECTION B: CRIMINAL INVESTIGATION

12. In your understanding, how would you define criminal investigation?

_____

13. In your understanding, what are the objectives of criminal investigation?

_____

14. In your understanding, how would you define evidence?

_____

15. In your understanding, how would you describe identification?

_____

16. In your understanding, how would you describe individualisation?

_____

17. In your understanding, how would you describe the Locard exchange principle?

_____

18. In your understanding, how would you describe the Lochner Principle?

_____

19. In your understanding, how would you define serious and violent crime?

_____

SECTION C: CELL PHONE RECORD ANALYSIS

20. In your opinion, what is a cell phone record?

_____

21. In your opinion, what information is displayed on a cell phone record?

_____

22. In your opinion, what type of evidence is cell phone records? Please elaborate.

_____

23. In your opinion, what are the specific procedures that have to be followed by the investigating officer to obtain cell phone records?

_____

24. In your opinion, what are the responsibilities of an investigating officer with regards to cell phone record evidence?

_____

25. In your experience, what guidelines should an investigating officer take in consideration when collecting cell phone record evidence?

_____

26. In your experience, what happens to the statement of the investigating officer that is submitted to request cell phone records?

_____

27. In your experience, what information should be contained in an investigating officer's statement when cell phone records are requested?

---

28. In your experience, what are the specific procedures that have to be followed by a Prosecutor to obtain cell phone records?

_____

29. In your opinion, what is the most important information that should be mentioned in an application to obtain cell phone records from a network service provider in terms of Section 205 subpoena of the Criminal Procedure Act 51 of 1977?

_____

30. To your knowledge, before signing a 205 application, is the information on which the application is based verified in the case docket? Please elaborate.

_____

31. In your experience, what is the role fulfilled by the Prosecutor in section 205 applications regarding cell phones?

_____

32. In your opinion, what is the purpose of a Section 205 subpoena in terms of the Criminal Procedure Act 51 of 1977?

_____

33. In your opinion, who are all the role players involved in both the requesting and provision of cell phone records through a section 205 subpoena in terms the Criminal Procedure Act 51 of 1977?

_____

34. In your opinion, what type of information can be requested from a network service provider in a Section 205 Subpoena of the Criminal Procedure Act 51 of 1977 which can add value in the investigation and prosecution of serious and violent crime?

_____

35. In your opinion, how can the information obtained in terms of Section 205 subpoena of the Criminal Procedure Act 51 of 1977 be used in the investigation and prosecution of serious and violent crime?

_____

36. In your experience, what challenges have you experienced with (subpoenas) section 205 subpoena in terms the Criminal Procedure Act 51 of 1977?

_____

37. What practical guidelines, procedures and recommendations can be offered to the SAPS to successfully obtain cell phone records from network service providers in terms of section 205 of the Criminal Procedure Act 51 of 1977?

_____

38. In your opinion, what evidential value does cell phone records have in the prosecution of serious and violent crime?

_____

SECTION D: ANALYSIS OF SIM CARD DATA

39. In your understanding, what is a sim card?

_____

40. In your understanding, what information is stored on a sim card?

_____

41. In your experience, how can sim card analysis be useful during the investigation and prosecution of serious and violent crimes?

_____

42. In your opinion, what valuable information do SIM cards hold in the investigation and prosecution of serious and violent crime?

_____

43. In your experience, what practical guidelines, procedures and recommendations can be offered to the SAPS to successfully use analysed cell phone records in the investigation of serious and violent crimes?

_____

44. In your experience, what practical guidelines, procedures and recommendations can be offered to the SAPS to successfully use analysed sim card data that appears on a cell phone record in the investigation of serious and violent crimes?

_____

45. In your opinion, what are the most important lessons you have learnt regarding the analysis of cell phone records in the investigation of serious and violent crime that you would want to share with others?

_____

46. In your opinion, what are the most important lessons you have learnt regarding the analysis of sim card data that appears on cell phone records in the investigation of serious and violent crime that you would want to share with others?

_____

47. Do you have any additional comments or suggestions regarding the analysis of cell phone records or sim cards that have not been discussed?

_____

Thank you for participating in this interview.

8.6 ANNEXURE F: INTERVIEW SCHEDULE FOR THE CELL PHONE ANALYST

SAMPLE E: WINELAND DISTRICT: CELL PHONE ANALYST

PARTICIPANT NUMBER: _____

TOPIC: AN EXPLORATION OF THE INVESTIGATIVE VALUE OF CELL PHONE RECORD ANALYSIS IN THE INVESTIGATION OF SERIOUS AND VIOLENT CRIMES IN THE WINELANDS DISTRICT, WESTERN CAPE PROVINCE

I am a post graduate student that is currently busy conducting research for the degree - Masters in Criminal Justice: Forensic Investigation at the University of South Africa. My supervisor is Prof Juanida Horne who can be contacted at the University on 012 433 9415 with regards to any matters pertaining to my research. The aim of this research is to explore the investigative value of cell phone record analysis in the investigation of serious and violent crimes in the Winelands District, Western Cape Province.

The following research questions will be answered in this study:

- Research questions 1: What do analysed cell phone records entail?
- Research questions 2: How are cell phone records analysed?
- Research questions 3: What value can analysed cell phone records add to the investigation of crime?
- Research questions 4: What valuable information do SIM cards hold in the investigation of crime?
- Research questions 5: What practical guidelines, procedures and recommendations can be offered to the SAPS to successfully use analysed cell phone records in the investigation of serious and violent crimes?

My research seeks to explore the investigative value of cell phone record analysis in the investigation of serious and violent crimes in the Winelands District, Western Cape Province. Your participation in this research is of major importance for the successful answering of the research questions. The researcher is bound to his assurances and guarantees by the research ethics code of the University of South Africa. The information you provide will be used in a research project for a Masters in Criminal Justice: Forensic Investigation at the University of South Africa. The analysed and processed data will be published in a research report. The interviewer will personally note your answers on paper and record the interview. Should any question be unclear, please ask the researcher for clarification. Only one answer per question is required. When answering the questions, it is very important to give your own opinion.

All interviews will be treated as strictly confidential

Your participation in this study is voluntary and can be terminated at any time. All responses will be treated with the utmost confidentiality by the researcher and all participants will remain anonymous. The names of the organisations participating in this will not be included. All participants will be allocated a number and completed interview schedules will be captured in an electronic database. All computerised notes will be stored on a secure, password-protected computer.
Transcribed interviews will be kept in a secure place for a period of three years as required by the university rules. The transcribed interviews will thereafter be destroyed.

Research agreement between researcher and participant:

I undertake not to disclose your name. All information will be treated confidentially.
When reporting on the findings, no names of individuals or companies will be mentioned. You are free to terminate the questioning at any stage of the interview. The above information has been explained to me and I understand it. My name will not be disclosed, and I will allow my information or responses to be used in a confidential manner that will not harm me or my employer in any way and I am also aware that the thesis might be published in future. If you have any queries about this interview schedule, please contact 083 400 1647/ office 021 929 4995 and via email at Donnievr67@gmail.com .

Thank you for your cooperation.

Masters in Criminal Justice: Forensic Investigation student
UNISA

_____ _____ _____

Signature of participant Place Date
PARTICIPANT

I hereby give permission to be interviewed and that information supplied by me can be used in this research.

YES	NO

SECTION A: BACKGROUND INFORMATION

1. What is your current rank in the SAPS?

_____

2. What is your gender?

A	B
MALE	FEMALE

3. How many years of service do you have in the SAPS? [Please mark the most relevant box.]

A	B	C	D
Less than 1 year	1 – 5 years	6 – 10 years	More than 10 years

4. What is your current position in the SAPS?

_____

5. How long have you served in this position? [Please mark the most relevant box.]

A	B	C	D
Less than 1 year	1 – 5 years	6 – 10 years	More than 10 years

6. Please specify your role with regards to the analysis of cell phone records and sim cards?

_____

7. Do you have any formal qualifications? If yes, please elaborate.

_____

8. Did you attended any formal courses in your career as a detective? If yes, please elaborate on which courses you have attended.

_____

9. How many years of experience do you have in the investigation of serious and violent crime? [Please mark the most relevant box.]

A	B	C	D
Less than 1 year	1 – 5 years	6 – 10 years	More than 10 years

10. Have you received any training regarding cell phone record analysis or sim card analysis? If yes, please elaborate.

---

11. Have you ever testified in Court regarding cell phone record analysis or sim card analysis? If yes, please elaborate.

_____

SECTION B: CRIMINAL INVESTIGATION

12. In your understanding, how would you define criminal investigation?

_____

13. In your understanding, what are the objectives of criminal investigation?

_____

14. In your understanding, how would you define evidence?

_____

15. In your understanding, how would you describe identification?

_____

16. In your understanding, how would you describe individualisation?

_____

17. In your understanding, how would you describe the Locard exchange principle?

_____

18. In your understanding, how would you describe the Lochner Principle?

_____

19. In your understanding, how would you define serious and violent crime?

_____

SECTION C: CELL PHONE RECORD ANALYSIS

20. In your understanding, what is a cell phone record?

_____

21. In your opinion, how are cell phone records generated?

_____

22. In your experience, what type of information is displayed on a cell phone record?

_____

23. In your opinion, how can the information displayed on the cell phone record be utilised during the investigation of serious and violent crimes?

_____

24. In your opinion, what type of evidence is a cell phone records? Please elaborate.

_____

25. In your experience, how are cell phone records analysed?

_____

26. In your opinion, what is used to analyse cell phone records?

_____

27. In your opinion, what are the specific procedures that have to be followed by the investigating officer to obtain cell phone records?

_____

28. In your opinion, what are the responsibilities of an investigating officer with regards to cell phone record evidence?

_____

29. In your opinion, what guidelines should an investigating officer take in consideration when collecting cell phone record evidence?

_____

30. In your experience, what happens to the statement of the investigating officer that is submitted to request cell phone records?

_____

31. In your opinion, what information should be contained in an investigating officer's statement when cell phone records are requested?

_____

32. In your opinion, what is the most important information that should be mentioned in an application to obtain cell phone records from a network service provider in terms of Section 205 subpoena of the Criminal Procedure Act 51 of 1977?

_____

33. In your opinion, what purpose does a Section 205 subpoena in terms of the Criminal Procedure Act 51 of 1977 fulfill in the investigation of serious and violent crime?

_____

34. In your experience, what type of information can be requested from a network service provider in a Section 205 Subpoena in terms of Section 205 subpoena of the Criminal Procedure Act 51 of 1977 which can add value in the investigation of serious and violent crime?

_____

35. What practical guidelines, procedures and recommendations can be offered to the SAPS to successfully obtain cell phone records from network service providers in terms of section 205 of the Criminal Procedure Act 51 of 1977?

_____

36. Were you ever subpoenaed as a witness to testify in terms of a section 205 subpoena of Criminal Procedure Act 51 of 1977?

_____

37. On which aspects did you have to testify when you were subpoenaed as a witness in terms of section 205 subpoena of Criminal Procedure Act 51 of 1977?

_____

38. In your experience, which aspects of your testimony was tested?

_____

39. In your experience, what evidential value can analysed cell phone records add to the investigation of serious and violent crime?

_____

40. In your opinion, how can the geographical positioning of the caller or receiver be identified?

_____

41. In your opinion, how can the geographical positioning of the caller or receiver be useful in cell phone record analysis?

_____

42. In your opinion, what are the key components of a cellular network?

_____

43. Based on your experience, what practical guidelines can you suggest on how to successfully obtain cell phone records from a network service provider in terms of section 205 of the Criminal Procedure Act 51 of 1977?

_____

44. In your experience, what practical guidelines, procedures and recommendations can you suggest to the SAPS on how to analyse cell phone records?

_____

45. In your opinion, what are the most important lessons you have learnt regarding the analysis of cell phone records in the investigation of serious and violent crime that you would want to share with others?

_____

46. Do you have any additional comments or suggestions regarding the analysis of cell phone records during the investigation of serious and violent crime have not been discussed?

_____

SECTION D: ANALYSIS OF SIM CARDS DATA

47. In your understanding, what is a sim card?

_____

48. In your opinion, what is the different formats of sim cards?

_____

49. In your understanding, what information is stored on a sim card?

_____

50. In your experience, when a cell phone and sim card is seized, what is the procedure to obtain data from a sim card?

_____

51. In your opinion, how are the retrieved sim card data analysed?

_____

52. In your opinion, what evidential value does SIM card data analysis holds in the investigation of serious and violent crime?

_____

53. In your experience, what practical guidelines, procedures and recommendations can be offered to the SAPS to successfully use analysed sim card data that appears on a cell phone record in the investigation of serious and violent crimes?

_____

54. In your experience, what practical guidelines, procedures and recommendations can you suggest to the SAPS on how to analyse sim card data that appears on cell phone records?

_____

55. In your opinion, what are the most important lessons learnt regarding the analysis of sim card data that you would want to share with others?

_____

56. Do you have any additional comments or suggestions regarding the analysis of sim card data that have not been discussed?

_____

Thank you for participating in this interview.

8.7 ANNEXURE G: TURNITIN DIGITAL RECEIPT

turnitin

Digital Receipt

This receipt acknowledges that Turnitin received your paper. Below you will find the receipt information regarding your submission.

The first page of your submissions is displayed below.

Submission author:	Donavin van Rooyen
Assignment title:	Revision 1
Submission title:	An exploration of the investigative value of cell phone recor...
File name:	4290-375-0_Dissertation_Final.docx
File size:	4.63M
Page count:	287
Word count:	90,015
Character count:	504,782
Submission date:	06-Jul-2022 10:56AM (UTC+0200)
Submission ID:	1867249330

AN EXPLORATION OF THE INVESTIGATIVE VALUE OF CELL PHONE RECORD ANALYSIS IN THE INVESTIGATION OF SERIOUS AND VIOLENT CRIMES IN THE WINELANDS DISTRICT, WESTERN CAPE PROVINCE

by

DONAVIN ADAM VAN ROOYEN

Student Number: 4290-375-0

Submitted in partial fulfilment of the requirements for the degree of

MASTER OF ARTS IN CRIMINAL JUSTICE

in the subject

FORENSIC INVESTIGATION

at the

UNIVERSITY OF SOUTH AFRICA

SUPERVISOR: PROF J.C. KOTZE
CO-SUPERVISOR: DR F. MACHETHE

DATE: JULY 2022

8.8 ANNEXURE H: EDITORS LETTER

EDITOR'S DECLARATION

I, the undersigned, hereby confirm my involvement in the academic editing, language control, text redaction, research methodology compatibility and technical compliance for the **Master's dissertation** manuscript of **Mr Donavin Adam Van Rooyen (Student Number: 4290-375-0)** submitted to me in respect of her fulfilment of the requirements for the Master of Arts (MA) in Criminal Justice degree registered with the University of South Africa (UNISA), and entitled:

An exploration of the investigative value of cell phone record analysis in the investigation of serious and violent crimes in the Winelands District, Western Cape Province

As an independent academic editor, I attest that all possible means have been expended to ensure the final draft of **Mr D.A. Van Rooyen's** dissertation manuscript reflects both acceptable research methodology practices and language control standards expected of postgraduate research studies at her academic level.

In compliance with expected ethical requirements in research, I have further undertaken to keep all aspects of **Mr D.A. Van Rooyen's** study confidential, and as her own individual initiative.

Sincerely.

TJ Mkhonto
BA Ed: North-West University, Mafikeng (1985)
MEd: School Administration; University of Massachusetts-at-Boston, USA, Harbor Campus (1987)
DTech: Higher Education Curriculum Policy Reform, Design & Management; University of Johannesburg, (2008)

All enquiries:

Email: mkhonto9039@gmail.com
Cell: +27(0)60 401 8279

Signed: _____ **Date:** 16 May 2022
Dr TJ Mkhonto dd/mm/yyyy

Independent Academic Editor

Professional EDITORS Guild
Themba J Mkhonto
Associate Member
Membership number: MKH001
Membership year: February 2022 to March 2023
060 401 8279
mkhonto9039@gmail.com
www.editors.org.za