An Evaluation of The Use of Electronic Evidence in the Investigation of Procurement Corruption: A Case Study of Ethekwini Regional Office

Molondolozi Prince Hlengwa [1], Matsidinkane Solomon Manamela [2*]
[1] Special Investigating Unit, Durban, South Africa.
[2] Department of Police Practice, University of South Africa.Pretoria, South Africa.
*Corresponding authour: manamms@unisa.ac.za

OIDA International Journal of Sustainable Development, Ontario International Development Agency, Canada.
ISSN 1923-6654 (print) ISSN 1923-6662 (online) www.oidaijsd.com
Also available at https://www.ssrn.com/index.cfm/en/oida-intl-journal-sustainable-dev/

Abstract: Procurement corruption has become a major problem in South Africa, affecting both the public and private sectors, and also lowers the country's moral standards significantly. Electronic evidence is gradually becoming recognised as an important intervention in the fight against procurement corruption in both criminal and civil cases, especially that technological progress has become even more pronounced in the twenty-first century. This article evaluates the methodologies used in the collection of electronic evidence during the investigation of procurement corruption. To that effect, the paper further focuses on identification of the limitations of electronic evidence that have investigative value, and also proposes procedural improvements in order to guarantee the admissibility requirements of such evidence. The investigation and punishment of corruption rely heavily on electronic evidence. However, it is important to recognise the prevalence of other types of evidence. Each procurement corruption case presents unique characteristics and necessitates individualised handling of evidence. This study adopts a qualitative empirical research design approach to elucidate the sentiments and perspectives of forensic investigators, thereby fostering a deeper understanding of the meanings associated with their professional experiences. Findings from the research indicate an increasing importance of electronic evidence, due to the proliferation of devices and services, such as smartphones and cloud storage, and their facilitation of evidence acquisition in the context of procurement corruption investigations. The study emphasises that meticulous planning and preparation are essential for the efficient processing of identified electronic evidence at any crime scene related to procurement corruption. Furthermore, the findings and recommendations advocate for forensic investigators to seek additional forensic support when digital forensic expertise is required, whether from local forensic units or outside specialists. Such a trajectory would ensure adherence to established procedures and admissibility of evidence in judicial proceedings.

Keywords: Corruption, electronic evidence, investigation, and procurement.

Introduction

South African communities are increasingly dissatisfied with rising crime rates, exacerbated by procurement-related corruption that undermines society's ethical standards. In South Africa, this form of corruption is pervasive across various provincial and national government departments and their associated tendering and procurement processes (Deloitte, 2015; South Africa, 2019:4). The KwaZulu-Natal Department of Public Works (KZNDPW) is particularly vulnerable to this form of corruption due to insufficient controls in its procurement and property management operations. President Cyril Ramaphosa authorised the Special Investigating Unit (SIU) to investigate these claims in response to corruption allegations affecting these operations (Parliamentary Monitoring Group, 2020:n.p.). The KZNDPW is one of twelve departments and State-Owned Entities (SOEs) targeted in the SIU proclamation aimed at addressing corruption in South Africa.

Forensic investigators play a critical role in probing corruption-related issues by focusing on electronic evidence collection during procurement investigations in order to prove cases beyond reasonable doubt in court. This study

centres on the investigation of procurement practices in the KZNDPW, with particular focus on Kwa-Maphumulo, Hammersdale, and Umkomaas jurisdictions. The investigation of procurement corruption reveals a significant technological shift in the operational practices of the KZNDPW, such as document scanning for archival purposes, communication via email, and platforms such as Skype or Google Meet. This technological evolution implies that electronic evidence is becoming increasingly integral to the work of forensic investigators tasked with addressing reported fraud cases within the department. However, an evaluation of internal corruption allegations at the eThekwini Regional Office of the KZNDPW indicates that electronic evidence is not utilised effectively by forensic investigators. The Organisation for Economic Co-operation and Development (OECD) (2015) acknowledges the gradual embeddedness of electronic evidence in daily life and its increasing prominence in legal proceedings. Gultan (2012:13) further asserts that electronic evidence may exacerbate certain challenges associated with traditional evidence. The latter is induced by the increasing documentation of commercial transactions and its simplification of the tracking of an individual's history and activities, which allows for enhanced computer-assisted investigative techniques.

This study focuses exclusively on the forensic investigators affiliated with the KwaZulu-Natal Department of Public Works (KZNDPW) at the eThekwini Regional Office, who are tasked with the investigation of procurement-related corruption cases. The KZNDPW's mission encompasses leadership in infrastructure development and property management within the province of KwaZulu-Natal. The primary functions of the department include supply chain management and property management, as well as infrastructure development and maintenance.

The Aim of the Research

This article interrogates the methodologies employed in the gathering of electronic evidence pertinent to investigations of procurement-related corruption. The article further aims to identify detrimental aspects of electronic evidence that are significant to corruption enquiries, and offers insights into enhanced strategies that ensure admissibility of such evidence in judicial settings. Effective utilisation of electronic evidence significantly enhances the capacity of investigative authorities to detect, deter, and prosecute corrupt practices in procurement, thereby promoting greater accountability and integrity within public procurement systems (Duja Consulting (Pty) Ltd, 2025:n.p.).

Theoretical Framework

The theoretical framework highlights the significant role of electronic evidence in investigating procurement corruption. The researchers understand that electronic evidence is multifaceted and closely related to technology, network systems and the Internet. The admissibility of electronic evidence is often compounded by defence attorneys in various platforms, such as courts of law, commissions of enquiry and disciplinary hearings. This type of evidence is vulnerable to manipulation by those with technical expertise, which can lead to its rejection by courts and negatively impact on legal proceedings (Du Pokoy, 2025:1). This vulnerability stems from the ease with which digital information can be altered, potentially compromising its authenticity and reliability. This is attributable to its delicate nature, considering that electronic evidence is prone to modification by technological specialists. Occasionally, courts reject electronic evidence, adversely impacting judicial proceedings.

However, Cassim, Cassim, Cassim, Jooste and Chev (2012:466) state that the admissibility of documents from an electronic source such as e-mail, fax, Short Message Service (SMS) and social media posts is regulated by the Electronic Communications and Transactions Act (ECTA) No. 25 of 2002. The electronic evidence in an electronic format is used as evidence in court proceedings, since it is crucial to ascertain the authenticity of a document; that is, establishing that it is an unaltered original version of the electronic document or data message (Phillips, Godfrey, Steuart & Brown, 2013:58). Rogers (2013:77) further defines electronic evidence as any probative (affordance of proof or evidence) information stored or transmitted in digital form that a party to a court case may use at a trial. Meanwhile, Ferraro (2015:145) asserts that electronic evidence is the most common evidence produced during both criminal and civil proceedings. The researchers posit that electronic evidence is more convenient and realistic to store than physical evidence, whether it (such video evidence) is video footage, an electronic copy of a contract, or a document signed with an electronic signature.

Types of Electronic Evidence in the Procurement Corruption Investigation Cases

In procurement corruption investigations, electronic evidence encompasses several forms of digital information that may reveal illicit activities. Such electronic evidence includes emails and messages, spreadsheets and databases, as well as hidden or deleted items. A plethora of technical gadgets is readily accessible for analysing procurement data and identification of unusual patterns and linkages, including links between successful bidders and government officials or collusion among competing bidders. A digital evidence specialist can acquire evidence from an electronic

device, such as a computer (Arkfield, 2012:54). The researchers acknowledge the existence of diverse forms of electronic evidence, which are elaborated hereafter.

Documents and Records

Graves (2013: 174) defines "files" as the diverse array of application software utilised on a computer, encompassing programmes that allow users to create spreadsheets, databases, text documents, graphic files, multimedia, and presentations. The study posits that the files may serve as digital proof, akin to system logs that document login, logout, operational behaviours, and network activities.

Documents and files generated or altered by the user

Graves (2013:181) defines documents as text files that can be readily searched with the use of certain keywords through a process sometimes referred to as 'metadata' — data that elucidates or interprets the meaning of other data. The file's storage location on the disc constitutes metadata.

System and application files

Glister (2009:238) asserts that a system file in computing is an essential computer file necessary for the proper functioning of a computer system. McHoes and Flynn (2013:456) assert that certain system files are incorporated as part of the operating system, a third-party device driver, or other origins. The researchers recognise that system files are exemplified by those with the ".sys" filename extension in MS-DOS and Windows. Additionally, Graves (2013: 310) states that "Program Files is the designated directory name for a standard folder in Microsoft Windows operating systems where applications not integral to the operating system are typically installed; each application within the 'Program Files' directory will possess a subdirectory for its specific resources".

Ephemeral files and cache files

Casey (2011:413) asserts that when a computer connects to the Internet, the majority of its data files are stored in several temporary files. Furthermore, Graves (2013:219) ascertains that transient files of accessed websites are retained in cache files and directories. The researchers recognise that cache files and temporary files are crucial as electronic evidence in establishing facts and trends of abnormalities.

Erased documents

Following deletion of a file from a computer, the file's contents are not eradicated but are sent to the recycle bin instead (Hayes, 2014:401). The researchers concur that significant electronic evidence often resides in the recycle bin. Deleted files are frequently recoverable by examining the contents of the recycling bin (Boddington, 2016:171). In the absence of the deleted files from the recycle bin, several commercial data recovery solutions may be utilised to retrieve such files (Andrews, Dark & West, 2016:206).

Networks

The researchers posit that the majority of computers are currently linked to networks. Furthermore, the logs and data generated by individual computers can yield electronic evidence in a corruption case, encompassing email usage, Internet connectivity, and website access.

The World Wide Web

Khanlari (2015:94) defines the Internet as a global network of interconnected computer systems utilising the Internet Protocol suite (TCP/IP) to connect billions of devices globally. Khuraniya and Maniar (2016:26) assert that the Internet encompasses a vast array of information resources and services, including interlinked hypertext pages and applications of the World Wide Web (WWW), electronic mail, telephony, and peer-to-peer networks for file sharing. Das (2017:83) propounds that the Internet is an extensive global network of copious technologically interconnected networks.

Corporate intranet

Nicoletti (2016:159) asserts that corporate intranets are prevalent network tools selected or developed for major enterprises for the purpose of enhancing communication, fostering cooperation, and knowledge dissemination. Schopflin (2015:15) intimates that an intranet is typically operated by a major industrial firm to establish a network utilising Internet protocol, and accessible solely to authorised members, employees, or those whose entry is permitted. Saville (2016:132) asserts that an intranet can address numerous daily difficulties encountered by large organisations.

A business intranet is a private computer network that permits exclusive access to authorised individuals within an organisation (Laudon & Laudon, 2003:229).

Wireless networks

Zhenyu and Wang (2013:68) assert that wireless networks are computer networks devoid of any cable connections. Miller (2016:616), on the other hand, asserts that wireless networks may be the most straightforward method for connecting technical gadgets to the Internet. Qiu, Dai and Gai (2016:270) assert that multiple types of wireless networks exist for diverse applications, with Wireless Personal Area Networks (WPANs) as the most prevalent type.

Cellular networks

Casey (2011:613) defines a cellular network as the technology that enables electronic devices to transmit information between cell phones and computers. Zhenyu and Wang (2013:30) augment that cellular networks facilitate connectivity among networks, allowing for the exchange of voice and data between mobile devices. According to Masood and Ghazanfar (2018:119), a cellular network is a mobile network that delivers services through numerous base stations with restricted power, each serving a confined geographical area.

Data obliteration

Data destruction pertains to the secure management and safe elimination of critical and personal information stored on electronic devices (McWay, 2013:139). The study posits that it is more challenging to eradicate a document in electronic format, as opposed to a tangible object or paper that may be obliterated with ease. Contrary to computer users' assumptions, data is not entirely erased by pressing the 'delete' icon. Rather, the document or data persists and may remain recoverable under specific conditions. To that effect, Hassan and Hijazi (2017:109) affirm that "data destruction is the most evident and extensively debated anti-forensics tactic, as it is essential for obscuring digital footprints".

Falsification

Falsification refers to data manipulation aimed at creating a misleading impression (Mihajlovic-Madzarevic, 2010:169). In the researchers' view, falsification entails the manipulation of electronic evidence, such as the deletion of data stored on an electronic device. There is an increase in attempts to present fake evidence in court, which is attributed to technological advancements that render electronic evidence more vulnerable to manipulation.

Concealing information

Concealing information (also referred to as cryptography) entails its deletion prior to its transformation or conversion to a significant objective (Kondo, 2012:130). Cryptography is the process of concealing information by rendering it incomprehensible (Hassan & Hijazi, 2016:12). This is a recognised anti-forensic method employed to obscure information from external entities (Hassan & Hijazi, 2016:12). The researchers are in concurrence with the view of cryptography as the concealment of information.

Challenges in determining the authenticity of electronic evidence during the investigation of procurement corruption in court

The researchers have established that there are numerous challenges regarding the authenticity and admissibility of electronic evidence in court, which includes the following factors:

- A claim that information was tampered with, and it is no longer in its original state,
- The authenticity of the electronic device (computer) which created the data might be questioned.
- The difficulty of identifying the writer who created a Word processing file, an SMS, or an email.
- Unacceptability of the evidential value of information exchanged as part of social networking.
- The difficulty of proving that an act was conducted, or can be attributed to a particular individual because of the lack of supporting evidence, or
- Whether an individual who is thought to have used their password or 'accept' tab might be responsible for any other related action.
- Whether the information in local networks is necessary for all the work.
- Therefore, it is necessary to maintain the correct procedures for maintaining and securing electronic evidence to ensure the trustworthiness and reliability of data as a source of evidence in court. The implication is that investigators must understand the standard operating procedures applicable to obtaining electronic evidence in respect of the following facts:

- Internet-based data is difficult to obtain because there might be more regulations induced by the advent of cloud computing. The issue of some investigators' compliance with some of the regulations might also mean that legal advice would be required.
- Databases are perpetually being updated, which also means that the websites are also updated. In this regard, the main challenge is that acquiring information becomes even more difficult.
- Verification of data on social networks has its own set of programmes. For instance, obtaining details about the writer is compounded by the possibility of several people writing on the same page on social network sites.

Therefore, forensic investigators should be cognisant of the difficulties associated with attempts to establish the individual responsible for a social media post, because there are people who can create fake profiles.

The Relationship Between Corruption and Electronic Evidence within the Kzndpw's Ethekwini Regional Office

This section of the paper outlines the regulatory framework established to combat corruption in public procurement in South Africa (South Africa, 2019:4). Corruption challenges still persist in the country despite the prevalence of a comprehensive legislative and administrative framework to combat this form of crime. The Constitution of the Republic of South Africa (Act No. 108 of 1996) (referred hereafter as "the Constitution") mandates fairness, equity, openness, competitiveness, and cost-effectiveness in public procurement. There are various laws, regulations, and institutions whose aim is to prevent and combat corruption. However, decentralisation in procurement processes may create vulnerabilities. The researchers concur that procurement corruption is apparent in the public sector, particularly at the national, provincial, and municipal government levels. Such corruption also manifests among the parastatals, which are entities partially controlled by the State. Nonetheless, a considerable degree of corruption still exists within the private sector as well. The detrimental force of corruption erodes the integrity of both private enterprises and public institutions. In commercial businesses, it might be argued that corruption eventually affects the owners of the company. However, corruption in public institutions negatively affects every citizen in multiple ways through tax revenue.

Regulatory frameworks and institutional responses to procurement corruption in South Africa

According to Bonell and Meyer (2015:320), the pivotal legislation pertaining to corruption in South Africa is the Prevention and Combating of Corrupt Activities Act, No. 12 of 2004 (PRECCA). This Act aligns with the United Nations (UN) Convention against Corruption and the African Union (AU) Convention on Preventing and Combating Corruption, which came into effect on 11 July 2003, in Maputo. Cascarino (2012:53) states that the Combating of Corrupt Activities Act, No. 12 of 2004 aims to:

- Improve strategies to combat graft and fraudulent activities.
- Criminalise corruption.
- Handle corruption enquiries.
- Create a database of all individuals accused of corruption in order to prevent them from obtaining government contracts.
- Mandate reporting of all cases over R100 000.00.
- Discourage and prevent South Africans from being involved in corrupt activities.
- The researchers contend that while the PRECCA is the most significant legislation directly addressing corruption, there are other Acts and statutes that are also crucial in combating corruption in South Africa, including:
- The Constitution of the Republic of South Africa, which emphasises integrity, transparency, accountability, and good governance (Hatchard, 2014: 153).
- The Public Finance Management Act (PFMA), No. 1 of 1999, which establishes a framework for the transparent and accountable administration of finances at national and provincial government tiers, as well as in other public entities. The Act enhances the efficient and effective use of resources through prudent financial management for the intended purpose of improving service delivery (Woolham, 2013: 304).
- The Promotion of Access to Information Act (PAIA), No. 2 of 2000, which lays the foundation for open, transparent, and accountable governance. The Act enables access to data held by the State or any individual, deemed to be essential for the enforcement and protection of rights (Hatchard, 2014:165).

Forensic investigators' challenges in detecting and investigating cases of corruption related to procurement

In South Africa, the investigation of procurement corruption entails recognising diverse fraudulent actions within the public procurement system. These actions encompass bid-rigging, bribery, kickbacks, and inflated bills, among others (Makhadi, 2021:10). The researchers are of the opinion that procurement corruption is a very difficult crime to detect and investigate. For instance, there has to be compelling electronical evidence that must be presented in a court in order to prove guilt beyond reasonable doubt and be successful with the conviction of the perpetrators. Moreover, the crime is always concealed and often happens in the shadows away from the office for fear of detection. It is also very challenging for witnesses who will testify and support the cases. In most instances, corruption individuals are politically well connected, and pose threats to any prospective witnesses. These individuals are also adept at exploiting legal gaps and loopholes to their advantage. Notwithstanding such challenges, Joh (2016) makes a compelling case that data mining, artificial intelligence and machine learning technologies can be harnessed to solve corruption cases.

Evidence management

Smith (2007:50) asserts that numerous beneficiaries of corruption might disguise illicit funds as commodities, including loans, benefits, or other concessions. Procurement corruption cases lack the potential for crime scene investigations, in contrast with offences such as rape and murder. As such, investigators must trace financial transactions and detect anomalies that may be obscured within the minutiae. In addition, bank accounts and business agreements must be examined meticulously. Nortjé and Myburgh (2019:1) acknowledge that the intrinsic characteristics of electronic data complicate its management, as it does not conform readily to conventional protocols for data handling. The afore-cited authors further contend that "digital evidence is frequently collected improperly and analysed ineffectively or merely disregarded due to the complexities that digital evidence presents to forensic investigators".

Electronic surveillance

In procurement corruption investigations, investigators typically employ conventional investigative techniques, such as undercover operations, eavesdropping, and communication interception, among others. Certain tasks necessitate the expertise of skilled and highly experienced technicians for execution. These actions must adhere to legal parameters. Otherwise, the evidence may be dismissed by the court (Olaniyan, 2014:103).

Interviews

The researchers recognise that an interview is an essential component of the investigative process. Typically, the scarcity of corruption witnesses necessitates that investigators should mostly rely on the information they can obtain. The majority of interviewees in corruption cases exhibit a lack of cooperation and occasionally display hostility. However, addressing the shortcomings within the system is crucial in order to improve support and safeguards for those courageous individuals who vehemently expose corruption. By reinforcing enforcement mechanisms and increasing awareness of existing policies, we can foster a more secure atmosphere for whistle-blowers, enabling them to present their concerns without the apprehension of facing repercussions. In this context, it is important to highlight that there are established policies designed to protect interviewees who provide information of this nature, such as the following:

- The Promotion of Administrative Justice Act, No. 3 of 2000 permits citizens to hold the government accountable and to assess its service delivery efficacy (Hatchard, 2014:167).
- The Protected Disclosures Act, No. 26 of 2000 provides safeguards to employees who report corrupt practices (Williams-Elegbe, 2012:89).

On 31 August 2017, Mr Ebrahim Patel, South Africa's erstwhile Minister of Economic Development, stated at the Competition Law, Economics and Policy Conference held at the Gordon Institute of Business Science (GIBS) that: "Corruption incurs an annual cost of at least R27 billion to the South African Gross Domestic Product [GDP] and results in the loss of 76,000 jobs that could have been generated from a mere 10% rise in infrastructure project costs due to corruption". The statement underscores the imperative for the South African government to address corruption, emphasising its significant and widespread impact on the nation (South Africa, 2019). Corruption undermines the economy, diverts funds from public services, and erodes public trust (Mamvura, 2024:n.p.). The government must enhance anti-corruption initiatives to foster transparency and guarantee accountability in addressing procurement corruption.

Methodology

A qualitative empirical study was conducted to assess the utilisation of electronic evidence in the investigation of procurement corruption. This methodological approach was aimed at enhancing the collection and admissibility of such evidence in court. The study population were the Forensic Internal Risk Unit Investigators at the KZNDWP, which is tasked with the daily investigation of procurement corruption in the area. The unit comprises a personnel component of 30 members, all of whom are members of Forensic Internal Risk Unit Investigators. Seventeen of these members provide support, including personal assistants, clerks, and administrative officials. The remaining 13 are forensic investigators tasked with examining procurement wrongdoing in the eThekwini district.

From the identified population, five volunteers were purposively selected on the basis of their investigation extensive experience. The researchers developed a semi-structured interview guide to guarantee uniformity in the questions posed to all participants as stated by Sabapathy (2014:78). The semi-structured interview guide included the following open-ended questions:

1. What are the various types of electronic evidence in the investigation of procurement corruption cases?
2. What are the challenges relating to determination of the authenticity of electronic evidence during the investigation of procurement corruption in court?
3. What are the criteria or legal requirements for the collection and preservation of electronic evidence?
4. What problems do investigators face in detecting and combating procurement corruption?

The questions were formulated for the purpose of gaining insights into participants' experiences regarding the investigative methods employed by their departments in investigating procurement corruption cases. Prior to commencement of data collection, the interview guide was amended following the outcomes of two pilot interviews conducted with two forensic investigators in order to ensure that relevant information is gathered from participants, as stated by Sabapathy (2014:78). Ethical Clearance was obtained from the College of Law at Unisa prior to the start of the study as part of the research project (Certificate No: CLAW/ERC Reference No: ST142-2020.

This article employed the bracketing technique to mitigate biases in the collection of vocal, textual, and visual data. Creswell and Poth (2018:109) describe bracketing as a research technique employed to set aside prejudices, assumptions, and expectations to enhance understanding of the study phenomena. Baxter and Jack (2018:32) assert that engaging in research requires an open and non-judgmental attitude, necessitating the conscious recognition and suspension of one's own views and values. Bracketing in an article entails researchers engaging in reflexivity, self-monitoring, or self-examination to identify and mitigate bias as stated by Spirko (2019).

Findings and Discussion

The primary issue of the paper focuses on the methods utilised in the collection of electronic evidence relevant to investigations of procurement-related wrongdoing in the KZNDPW, eThekwini Regional Office. The findings yielded one major theme and four sub-themes, namely: 1) the various types of electronic evidence in the investigation of procurement corruption cases, 2) challenges in determining the authenticity of electronic evidence during the investigation of procurement corruption in court, 3) the criteria or legal requirements for the collecting and preservation of electronic evidence, 4) the problems that investigators face in detecting and combating procurement corruption. The major theme, sub-themes, and verbatim participant responses are discussed hereafter.

Major theme: The methods utilised in the collection of electronic evidence relevant to investigations of procurement-related wrongdoing

Sub-theme 1: The various types of electronic evidence in the procurement corruption cases

Participants were asked to describe “electronic evidence”, which emanates from the study’s focus on electronic evidence. In their respective responses, the participants listed multiple forms of communication and digital formats, as well as forms of exchanges. The below-cited excerpts are a depiction of some of their responses in this regard:

> *“Electronic evidence includes any interaction between two people or some evidence that a certain action happened on a computer or anywhere else for that matter.”* – **Participant 1**
> *“It’s evidence in digital form, such as email, SMS, videos and audios, but its authenticity is always questionable.”* – **Participant 3**
> *“It is significant that the role of procurement evidence takes many forms. This can be in the form of phone conversation transcripts. They can also be in the form of video surveillance or email conversations on a certain topic.”* – **Participant 4**

"In financial terms electronic evidence may mean financial data collected over a long time." – **Participant 5**

The afore-mentioned responses indicate that electronic evidence lacks a singular definition, as its interpretation is contingent upon circumstances. A dominant theme in the participants' responses is that of electronic evidence as information that is digitally generated and stored within a computer-based system. It is noteworthy that the majority of participants understood the notion of the significance of electronic evidence in the investigation of procurement misconduct in the public sector. This indicates the criticality of participants' recognition of the significance of electronic evidence in addressing alcohol-related issues in the country.

Sub-theme 2: Challenges in determining the authenticity of electronic evidence during the investigation of procurement corruption cases

In the quest to determine the participants ability to establish the authenticity of electronic evidence, they were asked to relate any challenges they may have faced with regard to the handling of such evidence. Below are their respective responses in this regard:

"*So far I have not experienced any challenges regarding handling electronic evidence. The only challenge I have is collecting or accessing the evidence. However, once I have it, there are minimal challenges in handling or preserving the evidence."* – **Participant 1**

"*Yes, because most of the time investigators are not the ones who collected the evidence. Sometimes the evidence is presented to you to sift and see if there is something useful that can help in a case. Sometimes you wish you had different sets of files or files that maybe the investigators or those who collected the evidence should have focused on a certain facet of the case*" – **Participant 2**

"*No. Handling electronic evidence is not overly difficult since in almost all cases there are always some backups, which means even in cases where there is mishandling of evidence or where files get accidentally deleted or corrupted, there is always a backup from the source to replace that evidence. As a result, in my case the challenge is not on the handling of evidence but rather the gathering of evidence in the first place*" – **Participant 3**

The afore-cited responses are reflective of participants' varied perspectives. A slight majority of the participants indicated some challenges in handling electronic evidence, while few of the participants highlighted that they did not have any challenges at all.

The participants were further asked whether the electronic evidence collected via authorised software tools was evaluated and acknowledged as evidence in a procurement corruption trial.

The participants provided a two-dimensional response to the question. Firstly, it seemed that they regarded the alteration of electronic evidence gathered throughout the investigation as a manipulation through software, rendering that evidence inadmissible in court. A further instance of tampering or alteration involves the modification of an audio file to reduce its length, truncating certain segments, altering a photograph to obscure specific areas, or digitally eliminating portions entirely. Secondly, other participants contended that files produced by software applications such as Microsoft Outlook in the form of emails, or financial spreadsheets generated by Microsoft Excel, should be permissible as evidence in court. The researchers got permission for conducting empirical research from the Department of Public work in Kwazulu Natal (South Africa). Participant 1's response below exemplifies the view that electronic evidence should not be altered by software, because such actions constitute tampering.

"No, because then the evidence is tampered with." – **Participant 1**

"Yes. There are instances where a secret recording was done, and it's not clear and needs to be cleaned to digitally remove some background noises. Some photos might not be clear, so they need to be edited to make them clear. Or some files might be encrypted, and there might be a need for a third-party software programme to decrypt the files." – **Participant 3**

"Yes. Within reasonable limits and assuming all applicable laws were observed during the collection of evidence, the evidence will be admissible in court." – **Participant 4**

Based on the responses by Participants 3 and 4 above, some files could be deemed admissible in the event that the manipulation is within reason. Ultimately, the admissibility of evidence depends on the motivation for the manipulation in the first place.

Sub-theme 3: The standards or legal requirements for collecting and preserving electronic evidence

The participants were asked to outline the standards and legal requirements applicable to the collection and preservation of electronic evidence. Below are some of their responses:

> *"There are different laws which exist when it comes to collecting evidence. Some of the evidence depends on whether it's collected in a private or public place, and whether a court order is needed or not. In short, the nature of the issue being investigated, the location where the electronic evidence is collected and the means used to collect the evidence determine significantly what can, and cannot be done during the collection and preservation of evidence."* – **Participant 2**

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

> *"In financial terms there is no standard electronic evidence. It all depends on the specific case that is being investigated."* – **Participant 5**

As previously mentioned, the collection, handling, and preservation of electronic evidence in corruption cases lacks rigid protocols. The procedures are determined by factors such as the investigation's nature, the specific files involved, and numerous other variables that vary in each case. It is clear that the handling of electronic evidence varies according to the type of evidence and specifics of the case under investigation. The latter assertion is corroborated by the participants' responses regarding variations in management of the evidence due to idiosyncratic case factors. One of the concerns arising from the comments is that the evidence must be managed in accordance with legal framework because it is essential to comply with the regulations in order to avoid any undue legal consequences.

Sub-theme 4: The problems that investigators face in detecting and combating procurement corruption

Participants were asked whether the presence of electronic evidence has some effect on the investigation of corruption. There was overwhelming agreement by a majority of the participants responding to the question. Below are some of the selected responses concerning the effect of electronic evidence on corruption investigations:

> "*The presence of electronic evidence has a positive effect on the investigation of corruption. However, it is also important that the collected evidence is of sufficiently high quality*." – **Participant 1**

> "*Yes. For example, electronic evidence might be in the form of audio evidence of people planning or colluding to do some corruption. Another example is that of the actual crime having been committed with evidence like emails where conversations took place of funds having been diverted. The presence of electronic evidence can play a significant role in determining the outcome of a corruption case*." – **Participant 4**

> "*Yes. Considering that these days most people actively use electronic devices like mobile phones, computers, cameras and tablets, all of which generate electronic data, it therefore makes sense that having access to the data that is generated by these devices will make a significant difference during an investigation."* – **Participant 5**

As noted in the verbatim responses above, the presence of electronic evidence significantly affects an investigation, especially when it is the only evidence available in a particular investigated case. In some cases, the documentary evidence might not be enough to secure a conviction, but may need to be complemented with electronic evidence. Notwithstanding, the overwhelming participant responses above, signify that electronic evidence is important in corruption investigations.

The Ten Basic Steps of Investigating Corruption

Both researchers bring a wealth of experience in the investigation of corruption-related cases by exploring a diverse array of investigative techniques drawn from both public and corporate realms. This experience was foundational to

the researchers' development of ten steps that are appropriate and effective for use by investigators in procurement corruption cases. The steps are discussed in Table 1 below.

Table 1: Proposed 10 stages of effective investigations in procurement corruption

Step	Action
Step 1	A complainant must undergo debriefing if a case commences with a complaint report. If the case represents a red flag, it must correspond with a potential strategy or programme.
Step 2	Assess the validity of the accusations to justify an investigation. If it is concluded that there is justification for investigation, a prompt assessment of the complaint's accuracy should be conducted.
Step 3	Conduct extensive research on the records of the suspected organisation, company, or person's character to confirm and validate the allegations.
Step 4	Complete the data collection on the suspicious company or organisation. Review all other significant corporate documents such as proposals, curricula vitae, etc. Obtain, with the requisite authorisation, the pertinent email and computer hard drive data. Assess the necessity of conducting an early interview with the subject.
Step 5	Review the findings of the preliminary investigation to verify and reconcile all the facts. Upon completion of the review, determine whether or not to advance with the comprehensive inquiry.
Step 6	Conduct interviews with the designated number of witnesses who are external to the investigative organisation.
Step 7	Devise a method to thoroughly investigate the allegations of illicit payments.
Step 8	Identify the most effective method to engage sincere and committed volunteers who will fully cooperate with the inquiry.
Step 9	In instances of corruption, it is imperative to meticulously investigate and examine every detail and fragment of evidence. Obtain information from the primary suspect to comprehend their involvement and motivations, ensuring documentation is maintained for future reference.
Step 10	Based on the outcomes, it is essential to devise an effective solution. Recommendations should be provided in order to prevent the recurrence of such situations.

Conclusion

Semi-structured interviews assisted the researchers in preparing for data collection. Participants were asked both open and closed questions, as outlined in the interview schedule, to evaluate the procedures used in the collecting of electronic evidence during the investigation of procurement misconduct. To ensure accuracy, the researcher documents participants' replies in field notes during interviews. Through the use of a systematic data collection method, the researcher successfully obtained comprehensive and detailed data, as reflected in the findings and discussion of the article. Participants were permitted to engage in open discussion on any interview-related issue, while the interviewer had the discretion to explore intriguing subjects that emerged from participants' interests, so enabling the researcher to mitigate personal biases.

In light of the vast volume of available digital evidence and the increasing number of devices capable of generating digital data, the study recommends that investigators should receive specialised training and be equipped with the latest technologies and methodologies in order to perform their duties effectively. Electronic evidence demonstrates that each case is distinct, and requires that the electronic evidence gathered must be treated accordingly. The research indicated that electronic evidence is crucial in the investigation of corruption cases. A principal finding of the study is that, the importance of electronic evidence is increasing due to the proliferation of devices and services, such as smartphones and cloud storage, from which evidence can be gathered in corruption investigations. However, documentary evidence still remains valuable for detecting and investigating corruption-related offences.

Reference

1. Arkfield, M. 2012. *Arkfeld's Best Practices Guide: ESI Pre-trial Discovery: Strategy and Tactic.* Phoenix: Law Partner Publishing.
2. Baxter, P. & Jack, S. 2018. Qualitative case study methodology: Study design and implementation for novice researchers. *The Qualitative Report*, 13(4), pp. 34-56.
3. Boddington, R. 2016. *Practical Digital Forensics*. Birmingham: Packt Publishing Ltd.
4. Bonell, M. & Meyer, O. 2015. *The Impact of Corruption on International Commercial Contracts*. Switzerland: Springer International Publishing.
5. Cascarino, R. 2012. *Corporate Fraud and Internal Control: A Framework for Prevention*. West Sussex: John Wiley & Sons.
6. Casey, E. 2011. *Digital Evidence and Computer Crime: Forensic Science, Computers and the Internet*. 3rd edition. Amsterdam: Elsevier.
7. Cassim, F., Cassim, M., Cassim, R., Jooste, R. & Shev, J. 2012. *Contemporary Company Law.* 2nd edition. Claremont: Juta & Co.
8. Creswell, J.W. & Poth, C.N. 2017. *Qualitative inquiry and research design: Choosing among five approaches* (4th ed). Thousand Oaks, CA: Sage.
9. Das, R.C. 2017. *Handbook of Research on Economic, Financial, and Industrial Impacts on Infrastructure Development*. Hershey: IGI Global.
10. Deloitte. 2015. *Preventing Procurement Fraud and Corruption*. Available at: https://www2.deloitte.com/content/dam/Deloitte/za/Documents/risk/ZA_RA_PreventingProcurementFraudCorruption_2015.pdf. Accessed on 21 August 2019.
11. Duja Consulting (Pty) Ltd. 2025. *Strengthening Transparency in Public Procurement: A Framework for Clean Governance.* Available at: https://www.duja.co.za/strengthening-transparency-in-public-procurement-a-framework-for-clean-governance/ Accessed on 17 May 2025.
12. Du Pokoy, C. Reconsidering the admissibility of expert forensic evidence in South African criminal proceedings. *Potchefstroom Electronic Law Journal,* 28:1-25.
13. Ferraro, E. 2015. *Investigative Interviewing: Psychology, Method and Practice*. Boca Raton: CRC Press.
14. Glister, R. 2009. *Internet Core and Computing IC3 Certification Global Standard 3 Study Guide*. New York: McGraw Hill.
15. Graves, M.W. 2013. *Digital Archaeology. The Art and Science of Digital Forensics*. New Jersey: Addison-Wesley.
16. Gultan, G. 2012. Concerns regarding the privacy of electronic evidence associated with its collection under the Turkish legal system and the Cybercrime Convention. Available at: https://www.duo.uio.no/bitstream/handle/10852/39023/THESIS-xDUO.pdf Accessed on 26 February 2018.
17. Hassan, N. & Hijazi, R. 2016. *Data Hiding Techniques in Windows OS: A Practical Approach to Investigation and Defence.* Amsterdam: Syngress.
18. Hassan, N. & Hijazi, R. 2017. *Digital Privacy and Security Using Windows: A Practical Guide.* New York: A Press.
19. Hatchard, J. 2014. *Combating Corruption: Legal Approaches to Supporting Good Governance and Integrity in Africa*. Cheltenham: Edward Elgar Publishing Limited.
20. Hayes, L. 2016. *Empirical Design*. New Hampshire: Wentworth Press.
21. Joh, E.E. 2016. The New Surveillance Discretion: Automated Suspicion, Big Data, and Policing. Harvard Law & Policy Review., 10, p.15.
22. Khanlari, A. 2015. Strategic Customer Relationship Management in the Age of Social Media. Hershey: Business Science Reference.
23. Khuraniya, N. & Maniar, A. 2016. *A Study on the Usage of the Internet by Working Women of Vadodara City for Performing Their Household Responsibilities*. Hamburg: Anchor Academic Publishing.
24. Kondo, K. 2012. *Multimedia Information Hiding Technologies and Methodologies for Controlling Data.* Hershey: Information Science Reference.
25. Laudon, K. & Laudon, J. 2003. ActiveBook, Management Information Systems. New Jersey: Prentice Hall.
26. Makhadi P. 2021. Types of Procurement Fraud. *Institute of Forensic Science Practitioner's,* 2: (10-12).
27. Masood, R. & Ghazanfar, A. 2018. *LTE Communications and Networks: Femtocells and Antenna Design Challenge*. New Jersey: John Wiley & Sons.

28. Mamvura, N. 2024. *Economic Sabotage and Corruption: Shifting Public Trust in Southern Africa's Governments.* Available at: https://myafrikamag.com/economic-sabotage-and-corruption-shifting-public-trust-in-southern-africas-governments/ Accessed on 26 August 2025.
29. McWay, D. 2013. *Today's Health Information Management: An Integrated Approach.* 2nd edition. Amsterdam: Cengage Learning.
30. Miller, M. 2016. *Wireless Networking Absolute Beginner's Guide*. London: Que Publishing.
31. Mihajlovic-Madzarevic, V. 2010. *Clinical Trials Audit Preparation: A Guide for Good Clinical Practice (GCP) Inspections*. New Jersey: John Wiley & Sons.
32. Nicoletti, B. 2016. *Digital Insurance: Business Innovation in the Post-Crisis Era - Palgrave Studies in Financial Services Technology*. Switzerland: Springer.
33. Nortjé, J.G. & Myburgh, D.C. 2019. The Search and Seizure of Digital Evidence by Forensic Investigators in South Africa. *PER: Potchefstroomse Elektroniese Regsblad,* 22(1):1-42.
34. Olaniyan, K. 2014. *Corruption and Human Rights Law in Africa*. Oxford: Hart Publishing.
35. Parliamentary Monitoring Group. 2020. PWI & PMTE: Consequence management regarding fraud and corruption cases & termination of employment contracts that has led to incapacity; with Deputy Minister. Public Works and Infrastructure. Available at: https://pmg.org.za/committee-meeting/30016/ Accessed on 26 July 2024.
36. Phillips, A., Godfrey, R., Steuart, C. & Brown, C. 2013. *E-Discovery: An Introduction to Digital Evidence*. Boston: Cengage Learning.
37. Qiu, M., Dai, W. & Gai, K. 2016. *Mobile Applications Development with Android: Technologies and Algorithms*. Boca Raton: CRC Press.
38. Rogers, R. 2013. *Digital Methods*. Cambridge: The MIT Press.
39. Sabapathy, K. 2014. *Singapore Mainstream Preschool Teachers and the Inclusion of Children with Special Needs in the Classroom*. Singapore: Partridge Publishing.
40. Saville, P. 2016. *From Obscurity to Clarity in Psychometric Testing: Selected Works of Professor Peter Saville*. New York: Routledge.
41. Smith, D. 2007. *A Culture of Corruption: Everyday Deception and Popular Discontent in Nigeria*. Princeton: Princeton University.
42. South Africa. 2019. *National Anti-Corruption Strategy 2020-2030.* Pretoria: Government Gazette.
43. Spirko, J. 2019. How to use bracketing in qualitative research. 17 May. The classroom. Retrieved from: https://www.theclassroom.com/use-bracketing-qualitative-research-7850523.html (Accessed on: 01/20/2025).
44. The Organisation for Economic Co-operation and Development. 2015. *OECD Digital Government Studies Open Government Data Review of Poland: Unlocking the Value of Government Data*. Paris: OECD Publishing.
45. Williams-Elegbe, S. 2012. *Fighting Corruption in Public Procurement: A Comparative Analysis of Disqualification or Debarment Measures*. Oxford. Hart Publishing.
46. Woolham, S. 2013. *The Selfless Constitution: Experimentalism and Flourishing as Foundations of South Africa's Basic Law*. Cape Town: Juta & Co.
47. Zhenyu, L. & Wang, C. 2013. *One-Dimensional Nanostructures: Electrospinning Technique and Unique Nanofibers*. Heidelberg: Springer.