The Use of Digital Evidence in Computer Fraud Investigation in South Africa

Mandla Agrippa Tuesday Ngcobo

University of South Africa

DOI: https://doi.org/10.47772/IJRISS.2026.100601320

Received: 26 June 2026; Accepted: 01 July 2026; Published: 18 July 2026

INTRODUCTION

Casey (2011:35) notes that offenders use cell phones, notebook computers, and web servers to commit crimes. Computers are also used directly in the commission of crimes (Easttom and Taylor, 2011:3). Easttom and Taylor (2011:3) further observe that one need not be a police officer or computer-security specialist to recognise the rise in computer crime. These offences range from network administrators hacking into the computers of current or former employees to large-scale credit card theft and fraud schemes. They may also involve drug trafficking, harassment, sexual exploitation of minors, and various forms of theft. The growth of computer crime is therefore a major concern for law-enforcement agencies and anyone responsible for network security. Casey (2011:35) adds that, in some instances, computers merely serve as convenient repositories for evidence of crime. As crimes committed with the assistance of computers have expanded, updated legislation, such as the Cybercrimes Act 19 of 2020, was enacted to replace the Cybercrimes and Cybersecurity Bill. This chapter examines the role and significance of digital evidence in computer fraud investigations.

Investigations Of Computer Fraud

Van Rooyen (2013:174) defines investigation as the process through which facts required for successful prosecution or litigation are discovered, identified, collected, preserved, and prepared as evidence before legal proceedings. Arnes (2018:3) supports this view, describing investigation as a systematic examination aimed at identifying or verifying facts. Swanson, Chamelin, Territo, and Taylor (2019:2) state that an investigator systematically gathers, documents, and evaluates evidence and information through the investigative process.

Birzer and Roberson (2012:4) explain that a crime exists only where laws and official government norms define conduct that may be obeyed or violated. Such laws also identify those who breach legal limits as offenders, requiring police intervention to investigate, arrest, and prosecute them. Nelson, Phillips, and Steuart (2019:11) conclude that investigators conducting computer fraud investigations must understand computer-related crime legislation, standard legal procedures, search-and-seizure requirements, and the process of building a case.

The Purpose of Investigating Computer Fraud

Gardner and Krouskup (2019:3) maintain that the primary purpose of a criminal investigation is to establish the truth, even where the investigator does not fully understand or agree with the administration of justice. The investigator's ultimate aim is to determine objectively what happened and who was involved, while acting lawfully and without infringing the rights and freedoms of those under investigation. Investigators should therefore pursue facts impartially and without personal motive.

Swanson et al. (2019:2), Van Rooyen (2013:174), and Zinn and Dintwe (2015:11) agree with Gardner and Krouskup (2019:3) that investigations seek to determine what occurred and that investigators must rely on evidence, rather than assumptions, to prove a crime. Zinn and Dintwe (2015:11) state that the purpose of a computer fraud investigation is to examine evidence scientifically and determine how it can be used to bring the perpetrator to justice. Various methods and techniques are applied to collect evidence capable of withstanding

court scrutiny. Investigators are central to this process: they gather admissible evidence, communicate with the prosecutor, testify, and assist in presenting the evidence. Zinn and Dintwe (2015:12) further argue that computer fraud investigations aim to trace offenders through scientific techniques or to identify alleged offenders by providing scientific proof of their involvement.

The researcher therefore submits that the objective of an investigation is to gather accurate and reliable information in order to determine the truth, or to reconstruct as closely as possible the circumstances and events under investigation. Truth refers to conformity with reality, and investigation involves reconstructing an incident or sequence of events.

The Objectives in the Investigation of Computer Fraud

Arnes (2018:3) states that a key objective of investigation is to identify material facts relating to a crime or incident. These objectives may be framed as follows:

- Who: Individuals involved in the investigation, such as suspects, witnesses, and victims.
- Where: The scene of the crime as well as other relevant locations.
- What: A description of the facts of the alleged crime.
- When: The time of the crime and any subsequent events.
- Why: The reason for the crime and why it occurred at a specific time.
- How: How the crime was committed.

Swanson et al. (2019:2) outline the following objectives of investigation:

- To establish that an offense took place;
- To track down and arrest the suspect(s);
- To retrieve assets stolen; and
- To help prosecute the person(s) implicated with the crime.

Zinn and Dintwe (2015:12) caution that, once the purpose of an investigation has been identified, the computer fraud investigator must determine the objectives needed to achieve it. Every investigation should therefore have a clear purpose and defined objectives.

The Role of Computers in Fraud

To clarify the terminology used in this field, it is useful to define the role of computers in fraud. Precise terminology supports a better understanding of how computers are involved in crime and assists investigators in developing appropriate investigative approaches. Computer fraud refers to any incident involving computer technology in which a victim suffered, or could have suffered, a loss and a perpetrator unlawfully gained, or could have gained, a benefit or advantage (Van Rooyen, 2013:262).

Easttom and Taylor (2011:4) persuasively argue that in contrast, computer crime is often classified as focusing on the precise illegal action occurring rather than the technological technique employed to carry out the attack. These lists would be similar to the following:

- identification theft
- cyberstalking/harassment
- unauthorized access to computer systems or data
- fraud
- non-access computer crimes

According to Casey (2011:39), investigating computer fraud requires a different approach from investigating a murder that merely involves related digital evidence. The role a computer plays in a crime determines how it may be used as evidence (Britz, 2013:306; Casey, 2011:39). Where a computer contains only limited digital

evidence, investigators may not need to seize the entire device. However, where the computer is central to the investigation and contains substantial digital evidence, it is often necessary to collect the whole computer and its contents. In addition, when a computer plays a significant role in the crime, it is generally easier to obtain a search warrant authorising the search and seizure of the entire device.

The role of computers in a crime determines whether the conduct qualifies as cybercrime. For an offence to be classified as cybercrime, a computer must either be the target of the crime or the tool used to commit it. Casey (2011:40) and Maras (2015:27-28) identify Parker as one of the first scholars to recognise the emergence of computer-related crime as a serious problem in the 1970s. Parker proposed four categories, notably without referring specifically to digital evidence:

- The computer is the object, or the data in the computer are the §objects, of the act.
- The computer creates a unique environment or unique form of assets.
- The computer is the instrument or the tool of the act.
- The computer represents a symbol used for intimidation or deception.

Distinguishing between a computer as a tool and as the target of a crime is useful because it relates to the offender's purpose. Casey (2011:40) explains that further terminology is needed to clarify this distinction. From the offender's perspective, a target is the object of an attack and may include computers or the information stored on them. An "intended victim" is the person, organisation, or institution meant to suffer loss or harm. The intended victim and the target may be the same, and there may be more than one intended victim. Because computer networks are highly interconnected, collateral damage may also occur. This refers to harm suffered by victims as a result of the offender's pursuit of another victim (Casey, 2011:40).

Computer Fraud Versus Traditional Fraud

Computer fraud differs from traditional fraud in several respects. Maras (2015:21) identifies one key difference: computer fraud is not limited by physical or geographical boundaries, because the Internet enables offenders to reach individuals, organisations, and businesses worldwide. Traditional fraud often involves face-to-face interaction or prolonged telephone communication to gain the victim's trust. In contrast, fraudulent emails and websites can now be used to deceive victims across the world (Easttom & Taylor, 2011:204-205). The Internet has increased the ease and speed with which unlawful activities can be committed. Before the Internet, a person seeking to steal from a bank had to rob it during business hours or remove money physically after hours. In either case, the offender could take only what could be carried away. In the Internet context, these physical limits no longer apply, and large sums of money can be transferred within minutes. The Internet has also simplified other forms of fraud. For example, mail fraud has changed significantly with the development of computers: criminals now send fraudulent correspondence electronically rather than by ordinary post. While conventional mail could contain sensitive financial information that criminals might steal, fraudsters now use email to obtain the same information. Computer technology has also transformed the theft of proprietary information and trade secrets. In the past, offenders might have used spies, wiretaps, cameras, recorders, stolen files, or discarded documents to obtain competitors' information. With computers, once unauthorised access is gained, the offender may immediately access the required information.

Computer-integrity crimes are relatively new offences that cannot be committed without computers or computer networks and often involve the computer as the target. Casey (2011:132) explains that computer-assisted crimes are traditional offences committed with the aid of a computer. Such offences may require legislative attention where conventional legal provisions do not adequately apply in the digital environment. A key distinction between computer fraud and traditional fraud is therefore that traditional fraud generally requires deception of the victim, whereas computer fraud may occur without the victim's knowledge through unauthorised interference with computer data or the operation of a computer system.

The Qualities of Investigators in the Investigation of Computer Fraud

Houck and Siegel (2015:18) and Silverstone, Sheetz, Pedneault, and Rudewicz (2012:92) state that investigators perform two key roles in computer fraud investigations: they conduct forensic examinations of evidence and provide expert testimony in criminal and civil proceedings. An investigator must understand general scientific methods and standards, as well as the specific techniques used in the relevant field. The investigator must also be familiar with the laws of evidence and court procedures in the applicable jurisdiction (Houck & Siegel, 2015:18). The necessary knowledge, skills, and abilities are acquired through formal education, training, and experience. Silverstone et al. (2012:18) further state that a competent computer fraud investigator must understand computer fraud generally and within the relevant industry. This knowledge enables the investigator to identify quickly which forms of digital evidence are likely to be most useful. Because much information is now created and stored electronically, a sound understanding of computers and information technology is essential to the investigator's toolkit. Computer forensic techniques are therefore widely used in financial investigations (Silverstone et al., 2012:92).

Silverstone et al. (2012:91) emphasise that computer crime investigators must understand and apply the scientific method consistently in order to make effective use of digital evidence. When combined with digital forensic methods and tools, the scientific method enables investigators to adapt to changing circumstances while ensuring that findings remain grounded in fact. Casey (2011:401) agrees that, as in other forms of computer fraud investigation, the scientific method should guide investigative analysis.

According to Zinn and Dintwe (2015:29), a professional computer fraud investigator possesses particular personal qualities, knowledge, and specialised investigative skills. An effective computer fraud investigator should demonstrate the following characteristics:

- intellectual and emotional intelligence
- sound moral and ethical character
- the ability to operate independently and as part of a team
- the ability to improvise and adapt to challenging situations
- the ability to interact effectively with other people
- being an analytical and critical thinker
- following an organized and systematic approach
- being well-versed in new technology
- perseverance.

Furthermore, Zinn and Dintwe (2015:35) believe that the following are crucial attributes of an investigator:

- An investigator should have a thorough understanding of what drives human behavior. This is directly related to a solid study of the discipline of criminology, which will assist the investigator in answering the question of why people behave the way they do.
- Being streetwise is a requirement, an investigator must understand both how and where to look for and find information.

Characteristics Of Digital Evidence

The use of the Internet and technological devices in criminal activity has made digital evidence increasingly important. As technology becomes more widespread and significant, reliance on digital evidence has grown in criminal, civil, and corporate justice processes. Evidence is anything legally presented to a tribunal or trier of fact that tends to prove or disprove a disputed fact (Birzer & Roberson, 2012:81). In practical terms, the two central questions in any criminal investigation are what happened and who committed the offence. When a crime occurs, a forensic investigation is undertaken. Beyond formal investigations, anything described as forensic involves uncovering information that may be used in an investigation. Investigations not only seek to identify offenders, but also enable authorities to develop new crime-fighting strategies as new patterns emerge. Two

essential aspects of investigation are securing the crime scene and collecting evidence that may explain what happened and lead to the arrest and conviction of the offender.

Digital evidence is fragile by nature and may be easily manipulated, damaged, destroyed, copied, or altered if handled or examined improperly. Precautions must therefore be taken to document, collect, preserve, and examine it appropriately (Lin, 2018:15). Its use in court presents several challenges, particularly because it can be changed deliberately or accidentally without leaving obvious traces. Lin (2018:15) defines digital evidence as data of investigative value stored on, or transmitted by, a digital device. Like DNA or fingerprint evidence, digital evidence may be hidden and cannot be understood merely by examining the physical item that contains it. Investigative reports may therefore be needed to explain the examination process and its limitations. Birzer and Roberson (2012:83) describe digital evidence as tangible material collected during criminal investigations for further examination, analysis, and presentation. The term "digital" does not necessarily mean that the evidence is visible to the naked eye; often, specialised development or instrumentation is required to make it visible. The value of digital evidence lies in its factual and objective nature. When properly used, it provides a framework of facts that assists both the investigator's understanding of the crime and the court's determination of guilt or innocence (Birzer & Roberson, 2012:83).

As a result, the researcher believes that the characteristics of digital evidence are:

- is invisible
- can be easily changed or destroyed
- needs precaution to be taken to prevent modification
- requires special tools and equipment
- requires specialized training
- requires expert testimony.

Sources Of Digital Evidence

Hassan (2019:20) notes that digital evidence may be found on hard drives; however, as computing technology advances, it is now present in almost all digital devices. Nelson et al. (2019:144) state that digital evidence may consist of any information stored or transmitted in digital form. Because digital data cannot be seen or touched directly, it can be difficult to explain and describe. Arnes (2018:5) explains that a digital device is a physical object, such as a laptop or smartphone, that contains one or more storage media, including a hard drive or memory. These storage media hold data in binary form, known as digital data. Casey (2011:7) observes that computers are everywhere, with digital data transmitted through wireless signals and underground cables. When considering the various sources of digital evidence, it is useful to classify computer systems into three categories:

- Most people consider open computer systems to be computer systems made out of hard drives, keyboards, and monitors, such as laptops, desktops, and servers that adhere to standards. These devices, with their ever-increasing storage capacity, can be valuable sources of digital evidence (Casey, 2011:7).
- Communication systems include both traditional telephone networks and wireless telecommunications systems. The Internet, and networks in general, can serve as sources of digital evidence (Casey, 2011:8).
- Digital evidence may be found in microcomputer systems, mobile devices, smart cards, and a variety of other computer-based systems. Mobile devices can save messages, digital photos, and videos, as well as other personal information. Navigation systems can be used to track where a vehicle has been (Casey, 2011:8).

Digital Crime Scene

Computers, mobile devices, and networks should be treated as extensions of the crime scene, even when they did not directly facilitate the crime, because they may contain vital information and add a digital dimension to the investigation (Casey, 2011:227). Like physical crime scenes, digital crime scenes may contain substantial evidence and must therefore be surveyed, preserved, and documented using forensic procedures. Lin (2018:15) notes that computer crimes have increased significantly in recent years as digital devices, including computers and mobile devices, are used to commit or become involved in crime.

Casey (2011:227) further states that to maintain the integrity of prospective evidence, both physical and digital crime scenes must be examined carefully. The appropriate handling of computers and networks as evidence is at the heart of a digital investigation, which usually involves several stages.

A crime scene must be secured and processed in accordance with forensic science principles. Because digital evidence is fragile, investigators must be trained to preserve and collect digital evidentiary material properly (Lin, 2018:215-216). They must also protect its integrity because it can be easily altered. Training first responders to recognise and manage digital crime scenes is therefore essential for law-enforcement agencies. Given the widespread presence of computers, answering machines, personal digital assistants, facsimile machines, and other electronic devices, almost any crime scene may contain valuable digital information. The recovery of this information depends heavily on the first responding officer's ability to recognise potential digital evidence.

Processes Of Seizing The Digital Evidence

In digital forensic investigations, the collection phase refers to acquiring or copying data. During this stage, the forensic investigator gains access to electronic devices containing raw data considered relevant to the case. Collection is widely discussed in digital forensics literature and scientific studies. The term "collection" is common in forensic literature, while more technical sources may use "acquisition" or "extraction" (Arnes, 2018:24). Section 14 of the Electronic Communications and Transactions Act 25 of 2002 requires evidence to be presented or retained in its original form; this requirement is met if the integrity of the digital evidence, from its creation to its final form, can be demonstrated. Nelson et al. (2019:145) argue that digital devices must be collected systematically when processing a crime or incident scene. Where practical, only one team should collect and catalogue digital evidence at a scene or laboratory to minimise confusion, reduce the risk of loss, and prevent damage. Birzer and Roberson (2012:104) add that a trained investigator may use linking theory and Locard's exchange principle to guide decisions, formulate questions for involved persons, focus evidence-collection efforts, and strengthen the case.

Once evidence is located, investigators must determine whether it may lawfully be seized. Some items may be seized immediately, while others may not (Britz, 2013:322). Arnes (2018:25), Britz (2013:322), and Hassan (2019:26-27) agree that data under investigation should be copied to separate media and that forensic examination should be conducted on the copy, not the original. This reduces the risk of accidental alteration during the forensic process. Britz (2013:322) further states that computers that are switched on should not be powered down until the scene has been photographed and documented, unless the risk to data outweighs the need for documentation. The condition of the computer and monitor should be recorded before shutdown. Some investigators also recommend copying open documents to external storage before powering down. Computers should not simply be switched off, as doing so may destroy potential evidence. As with any scientific evidence, digital evidence must be collected and preserved with care. Chain of custody and continuity of possession must be maintained at all times to support admissibility in court. Investigators should follow standard operating procedures for custodial evidence collection, recognising that proper procedures strengthen witness credibility and evidential validity. Although policies differ between departments, certain principles remain constant (Britz, 2013:324).

Maintaining The Chain Of Custody

Every physical item of evidence taken into possession by an investigator or agency must be supported by a continuously maintained chain-of-custody record (Graves, 2014:41). Hassan (2019:24) states that the chain of custody is an essential part of any digital forensic investigation. A proper chain of custody must clearly record how digital evidence was discovered, acquired, transported, examined, preserved, and handled by all parties involved. Its purpose is to preserve the integrity of digital evidence by identifying everyone who had contact with it from acquisition to presentation in court. If investigators cannot account for who handled the evidence at any stage, the chain of custody may be compromised, rendering the evidence unusable in court. Lin (2018:18) emphasises that documenting the chain of custody from the crime scene to court is essential to establishing authenticity. This is particularly important for digital evidence, which has more specific integrity requirements than traditional evidence. It is far easier to alter metadata on a critical file than to tamper with physical evidence such as a bloody knife. Casey (2011:21) similarly argues that maintaining and documenting the chain of custody is central to authentication. Each person who handled the evidence may be required to testify that the evidence presented in court is the same as when it was processed during the investigation. Without a reliable chain of custody, it may be argued that the evidence was improperly handled, altered, substituted, or contaminated. Consequences of a broken chain of custody include misidentification, contamination, loss of evidence, or loss of relevant evidential elements (Casey, 2011:22).

Admissibility And Relevance Of Digital Evidence

Whether digital evidence is accepted in court depends on the relevant legal system and the rules governing digital investigations and evidence (Arnes, 2018:122). Graves (2014:90) argues that, as with an archaeological discovery, the investigator bears the burden of proving that the evidence is authentic and genuine. Casey (2011:56) explains that admissibility requires courts to determine whether evidence is sufficiently reliable to be placed before a judge and whether it will assist in deciding the case. Graves (2014:90) adds that the investigator must prove not only that the evidence is genuine, but also that it is relevant. In practice, admissibility involves legal tests applied by a judge to assess the evidence. This process may become complex, especially where evidence has been mishandled or has characteristics that reduce its reliability or increase its prejudicial effect. Common-law systems require the party seeking to present evidence to justify its admission, whereas civil-law systems require justification for exclusion (Arnes, 2018:68). Arnes (2018:122) further states that evidence not collected in a forensically sound manner has reduced quality and credibility in court.

Graves (2014:90) and Casey (2011:57) agree that any information or exhibit presented in a civil or criminal case will be scrutinised by both parties and by the judge to determine whether it meets the general requirements for admissibility. Evidence is admissible if the court permits it to be presented. Several factors inform this decision, including the following questions:

- Is the evidence relevant?
- Is the evidence authentic and credible?
- Is the evidence competent?

Biasiotti, Bonnici, Canntaci, and Turchi (2018:135) state that courts assess admissibility using a three-part test: relevance, probative value, and potential prejudice. For exclusion, the Law of Evidence Act 45 of 1988 provides that evidence obtained in violation of the statute or internationally recognised human rights will be inadmissible if:

- the admission of the evidence would be antithetical to, and would seriously damage the integrity of the proceedings.

Casey (2011:57) states that improper handling and unlawful search and seizure may also prevent digital evidence from being admitted in court. Although courts have previously been relatively lenient regarding mishandling of digital evidence, challenges to evidence-handling procedures have increased as judges and attorneys have

become more familiar with digital evidence. Courts are far less tolerant of unlawful search and seizure. The admissibility and evidential weight of digital evidence are addressed in Section 15 of the Electronic Communications and Transactions Act 25 of 2002.

The Role Of Digital Evidence In The Investigation Of Computer Fraud

A central aim of investigation is to attribute a crime to its perpetrator by establishing persuasive links between the offender, victim, and crime scene. Although witnesses may identify a suspect, evidence of a person's involvement is often more compelling and reliable (Birzer & Robertson, 2012:84). Locard's exchange principle holds that anyone or anything entering a crime scene takes something from it and leaves something behind (Birzer & Roberson, 2012:85). Casey (2011:49) argues that the purpose of a courtroom is to administer justice and that digital investigators must present supporting evidence and possible explanations. Courts depend on digital investigators' honesty and ability to present technical evidence accurately. Their findings must be clear, factual, and objective. They must avoid being influenced by the opinions of others and refrain from making unsupported judgments. A digital investigator's professional work product, whether in testimony or expert reports, should not contain advocacy or judgmental views.

Arnes (2018:120) identifies the role of digital evidence as follows:

- Digital evidence can prove a computer fraud has been committed.
- Digital evidence establishes key elements of computer fraud.
- Digital evidence links the suspect to a victim, a victim to a crime scene, using digital evidence.
- Digital evidence can establish the identity of a person associated with computer fraud.
- Digital evidence can support or refute alibi.

CONCLUSION

This chapter examined the use of digital evidence in the investigation of computer fraud, with specific focus on the nature of computer-related crime, the investigative process, and the characteristics and handling of digital evidence. The analysis reveals several critical conclusions.

First, the role of computers in criminal activity is multifaceted. Computers may serve as the object of an offence, the instrument used to perpetrate it, a storage repository for incriminating data, or a medium that creates unique opportunities for fraud. The specific role a computer plays directly influences the investigative approach and the scope of evidence that must be secured. This distinction is fundamental to ensuring that digital evidence is lawfully and effectively collected.

Second, computer fraud is substantively different from traditional fraud. The absence of physical and geographic boundaries, combined with the speed and scale at which offences can be committed, presents unique challenges for investigators. Traditional investigative methods alone are insufficient. The Internet enables offenders to target victims globally, transfer large sums of money within minutes, and commit fraud without direct victim interaction or knowledge. These factors necessitate specialized legal frameworks, such as the *Cybercrimes Act 19 of 2020*, and investigative techniques tailored to the digital environment.

Third, digital evidence is both indispensable and inherently fragile. It is invisible, easily altered or destroyed, and requires specialized tools, expertise, and methodologies for proper acquisition and analysis. The integrity of digital evidence depends on strict adherence to forensic principles, including working on forensic copies rather than originals, thorough documentation of the crime scene, and an unbroken chain of custody from seizure to presentation in court. Failure to comply with these requirements jeopardizes the admissibility and evidential weight of the evidence, regardless of its technical relevance.

Fourth, the effectiveness of a computer fraud investigation is determined largely by the qualities and competencies of the investigator. An investigator must possess not only technical proficiency in digital forensics

but also a sound understanding of criminal law, rules of evidence, and judicial procedures. Intellectual and emotional intelligence, ethical conduct, analytical thinking, and the ability to apply the scientific method are essential characteristics. The objective of any investigation remains the establishment of truth through evidence, not presumption, and the preparation of that evidence in a manner that will withstand judicial scrutiny.

Finally, the admissibility of digital evidence is governed by legal standards of relevance, authenticity, and lawful collection. South African legislation, including the *Electronic Communications and Transactions Act 25 of 2002* and the *Law of Evidence Act 45 of 1988*, provides the framework within which digital evidence must be managed. Improper handling, illegal search and seizure, or a break in the chain of custody can render otherwise compelling evidence inadmissible.

RECOMMENDATIONS

To enhance the investigation of computer fraud, the following measures are recommended:

1. **Training and Capacity Building**: Law enforcement agencies should institutionalize continuous training for first responders and investigators in digital crime scene management, evidence preservation, and forensic procedures. Given the prevalence of digital devices in all forms of crime, basic digital evidence competence must become a core investigative skill.

2. **Standardized Procedures**: Standard operating procedures for the seizure, imaging, analysis, and documentation of digital evidence should be developed and enforced. These procedures must align with legal requirements to ensure admissibility.

3. **Specialized Units**: The establishment of dedicated computer fraud investigation units, staffed with personnel trained in both law and digital forensics, will improve investigative outcomes and ensure compliance with the *Cybercrimes Act 19 of 2020*.

4. **Interdisciplinary Cooperation**: Effective investigation requires cooperation between investigators, prosecutors, and digital forensic experts to ensure that technical findings are correctly interpreted and presented in court.

5. **Legislative Responsiveness**: Legislation must continue to evolve to address emerging forms of computer-assisted crime and to clarify the treatment of new sources of digital evidence.

In summary, digital evidence is now central to the investigation and prosecution of computer fraud. Its probative value is significant, as it can prove that a crime occurred, establish key elements of the offence, link suspects to victims and crime scenes, and support or refute alibis. However, the value of digital evidence is entirely dependent on the human factors governing its identification, collection, preservation, and presentation. As computer-related crime continues to rise, the criminal justice system must prioritize forensic readiness, professional competence, and procedural rigor to ensure that digital evidence fulfils its role in the administration of justice.

REFERENCE LIST

1. Arnes, A. 2018. Digital forensics. Hoboken, NJ: Wiley.
2. Biasiotti, M. A., Bonnici, J. P. M., Canntaci, J., & Turchi, F. 2018. Handling and exchanging electronic evidence across Europe. Cham: Springer International Publishing AG.
3. Birzer, M. L., & Roberson, C. 2012. Introduction to criminal investigation.
4. New York: Taylor & Francis.
5. Britz, M. T. 2013. Computer forensics and cybercrime: An introduction, 3rd ed.
6. Upper Saddle River, NJ: Pearson Education.
7. Casey, E. 2011. Digital Evidence and Computer Crime 3rd ed. Waltham, MA: Academic Press.

8. Easttom, C., & Taylor, J. 2011. Computer crime investigation and the law.
9. Boston: Cengage Learning Course Technology.
10. Gardner, R. M., & Krouskup, D. R. 2019. Practical Crime Scene Processing and Investigation, 3rd ed. London: Taylor and Francis, CRC Press.
11. Graves, M. W. 2014. Digital archaeology: The art and science of digital forensics. Upper Saddle River, NJ: Pearson Education.
12. Hassan, N. A. 2019. Digital forensics basics: A practical guide using Windows OS. New York: A press Media LLC.
13. Houck, M. M., & Siegel, J. A. 2015. Fundamentals of forensic science 3rd ed.
14. Oxford: Academic Press.
15. Lin, X. 2018. Introductory computer forensics: A hands-on practical approach.
16. Cham: Springer Nature.
17. Maras, M. 2015. Computer forensics: Cybercriminal laws and evidence
18. 2nd ed. Burlington, MA: Jones and Bartlett Learning.
19. Nelson, B., Phillips, A., & Steuart, C. 2016. Guide to computer forensics and investigations: Processing digital evidence, 5th ed. Boston: Cengage Learning.
20. Silverstone, H., Sheetz, M., Pedneault, S., & Rudewicz, F. 2012. Forensic accounting and fraud investigation for non-expert's 3rd ed. Hoboken: Wiley.
21. Swanson, C. R., Chamelin, N. C., Territo, L., & Taylor, R. W. 2019.
22. Criminal Investigation, 12th ed. New York: McGraw-Hill.
23. Van Rooyen, H. J. N. 2013. Investigate corruption. Centurion: HJN Training: Henmar Publishers.
24. Zinn, R. J., & Dintwe, S. I. 2015. Forensic investigation: Legislative principles and investigative practice. Cape Town: Juta.

Legislation

1. Republic of South Africa. 1988. Law of Evidence Act 45 of 1988. Pretoria: Government Printer.
2. Republic of South Africa. 2002. Electronic Communications and Transactions Act 25 of 2002. Pretoria: Government Printer.
3. Republic of South Africa. 2020. Cybercrimes Act 19 of 2020. Pretoria: Government Printer.
4. Cybercrimes and Cybersecurity Bill - superseded by the Cybercrimes Act 19 of 2020.