JCARM
Journal of Contemporary Academic Research and Methodologies

An Online Peer Reviewed / Refereed Journal
Volume 1 | Issue 5 | June 2026
Website: www.journal.jcarm.in

Original Research Article

# Effectiveness of Police Training in Cyber Fraud Investigation in Kenya: A Case Study of Nairobi City County

**Melkizedek Aluko Ojijo[1*], Mark Okowa (PhD)[1], Robert Amilla Oketch (PhD)[1]**

[1] Faculty of Arts and Social Sciences, Tom Mboya University, Kenya,

Correspondence should be addressed to Melkizedek Aluko Ojijo: mojijo2@gmail.com

**Article No:** 039 | **Accepted**: 13 June 2026 | **Published:** 10 July 2026

**Abstract**: This study assessed how police training influences the technical competence of officers in the Directorate of Criminal Investigations handling cyber fraud cases in Nairobi City County. It also examined challenges that limit the effectiveness of such training and reviewed measures used to strengthen cyber fraud investigation capacity. The study used a descriptive research design and a mixed-methods approach. The target population was 200 DCI officers serving in Nairobi City County, drawn from the Financial and Banking Fraud Investigations Unit, Cybercrime Unit, and Crime Research and Intelligence Bureau. Stratified random sampling was used to select 60 officers. Fifty-four officers returned usable questionnaires, giving a 90% response rate. Data were collected through semi-structured questionnaires and key informant interviews. Quantitative data were analysed descriptively using SPSS version 26, while qualitative data were analysed thematically. The findings showed that 85.2% of respondents agreed that the quality of police training affects the competence of DCI officers in cyber fraud investigations. Technical competence also influenced investigation effectiveness, with 55.6% reporting a great effect and 33.3% reporting a moderate effect. In addition, 88.9% agreed that technical and knowledge-related challenges hinder effective cyber fraud investigations. There was strong support for advanced cyber analytic tools in training, with 81.5% agreeing that more emphasis should be placed on such tools. However, support for monitoring suspect behaviour online was lower, at 55.5%, while 35.2% disagreed, pointing to legal, ethical, practical, or capacity-related concerns. The study adds evidence from Nairobi City County on the relationship between police training, technical competence, and cyber fraud investigation performance. It shows that training is important, but its value depends on practical exposure, access to current investigative tools, digital forensic support, and clear procedures for online monitoring and digital surveillance. By focusing on DCI officers working in financial fraud, cybercrime, and intelligence-related units, the study gives context-specific insight into capacity gaps in cybercrime policing in Kenya. In practice, the study recommends targeted curriculum reform, continuous professional development, decentralization of digital forensic services, increased funding for cyber-investigation

 https://doi.org/10.5281/zenodo.21300586

infrastructure, and clearer operational guidelines for online monitoring. These measures would improve the quality, speed, and reliability of cyber-fraud investigations. In theory, the study reinforces the view that specialized training and technical competence are central to effective cybercrime investigation. It also shows that police training models must keep pace with technological change, emerging forms of cyber fraud, and the legal and ethical demands of digital investigations.

**Keywords**: cyber fraud, cybercrime, police training, technical competence, digital forensics, Directorate of Criminal Investigations, Kenya

---

## INTRODUCTION

The rapid expansion of digital technology has transformed social, economic, and institutional activities across the world. Banking, communication, commerce, public service delivery, and private transactions are increasingly conducted through digital platforms. While this transformation has improved efficiency and connectivity, it has also created new opportunities for criminal activity. Cyber fraud has therefore emerged as one of the most complex challenges facing contemporary law enforcement agencies.

Modern policing is no longer limited to traditional physical investigations. Police officers are increasingly required to understand digital platforms, online financial systems, electronic communication, data recovery, digital surveillance, and the preservation of electronic evidence. Wa Teresia (2025) observes that technological change has reshaped policing in Kenya by creating both opportunities and operational challenges. Similarly, Arigo and Sellers (2021) argue that cybercrime investigation has become a central component of modern policing because criminal behaviour increasingly occurs in technologically mediated environments.

Cyber fraud is particularly difficult to investigate because it is often fast-moving, borderless, anonymous, and technically complex. Offenders may use mobile money platforms, online banking systems, social media, phishing links, identity theft, forged documents, malware, or encrypted communication to commit fraud. Mwakio et al. (2020) note that white-collar crimes such as hacking, forgery, and cyber-enabled financial fraud require law enforcement officers to develop specialized investigative capacity. Nyabira et al. (2019) further emphasize that police training must reflect the changing environment in which officers operate.

Globally, countries have recognized the importance of strengthening police capacity in cybercrime investigations. In the United States, police training has been reviewed to improve investigative competence and community safety, with Linda (2021) noting that structured academy and field training remain key elements of police preparation. In Africa, cyber-related financial crimes have become increasingly visible. The Central Bank of Ghana (2019) reported growth in banking fraud, including cyber-enabled financial crimes, demonstrating the need for stronger law enforcement responses. In South Africa, Aphane

and Mofokeng (2021) found that the police response to cybercrime was constrained by limited investigative capacity, poor stakeholder coordination, unclear legal frameworks, and inadequate resources.

Kenya faces similar challenges. As Nairobi City County is the country's commercial, administrative, and technological centre, it experiences a high concentration of cyber fraud cases. The Directorate of Criminal Investigations is mandated to investigate serious crimes, including cyber fraud, banking fraud, forgery, identity theft, and technology-enabled economic offences. However, traditional investigation methods are increasingly inadequate in dealing with digital crimes. Mwakio et al. (2020) argue that law enforcement agencies must adjust their methods to respond to contemporary white-collar and technology-enabled crimes.

The Government of Kenya and the National Police Service have taken steps to improve investigative capacity. These include curriculum reforms, specialized DCI training, collaboration with international partners, and enactment of cybercrime-related laws. Waswa (2023) recommends strengthening information technology tools, digital evidence quality, and officer security measures as part of improving cybercrime investigation effectiveness. Despite these efforts, concerns remain regarding the ability of police officers to investigate cyber fraud effectively. Muriuki and Mbaya (2023) identify information communication technology crimes as a growing challenge in Kenya and highlight the need for stronger institutional preparedness.

The effectiveness of cyber fraud investigations depends heavily on police training. Training equips officers with the technical knowledge, analytical skills, and legal awareness required to identify suspects, collect evidence, preserve digital material, analyze electronic transactions, and support successful prosecutions. However, training alone may not be sufficient where officers lack equipment, updated curricula, digital forensic laboratories, or continuous professional development. Wall (2017) argues that policing cybercrime requires not only trained officers but also organizational adaptation to networked technologies and online criminal spaces.

Although previous studies have addressed cybercrime, policing, and investigative challenges in Kenya, limited attention has been given to the effectiveness of police training in cyber fraud investigations among DCI officers in Nairobi City County. This study, therefore, assessed the effectiveness of police training in cyber fraud investigations in Kenya, using Nairobi City County as a case study.

Cyber fraud continues to increase in complexity, frequency, and sophistication in Kenya. Nairobi City County is especially affected because it hosts major banks, telecommunications firms, government institutions, businesses, and technology users. The DCI has introduced several measures to improve investigative capacity, including specialized training, curriculum review, and partnerships with foreign law enforcement agencies. However, cyber fraud investigations continue to experience delays, weak digital evidence handling, inadequate technical capacity, and dependence on a limited number of specialized officers.

The problem is that police training may not be keeping pace with the changing nature of cyber fraud. While officers may receive basic or general investigative training, cyber fraud requires specialized skills in digital forensics, data analysis, online surveillance, electronic evidence preservation, cyber law, and financial technology systems. Where training is insufficient or unevenly distributed, investigations may be delayed, evidence may be mishandled, suspects may evade detection, and prosecutions may fail. There is also limited recent empirical evidence on the relationship between specific training components and cyber fraud investigation effectiveness among DCI officers in Nairobi City County. This study addressed that gap by examining how police training influences technical competence, identifying challenges that affect training effectiveness, and evaluating strategies that can strengthen cyber fraud investigation capacity.

## METHODOLOGY

The study adopted a descriptive research design using a mixed-methods approach. The descriptive design was appropriate because it enabled collection, organization, and presentation of information on the effectiveness of police training in cyber fraud investigations as experienced by DCI officers. The mixed-methods approach allowed the study to combine quantitative questionnaire data with qualitative interview responses, thereby capturing both measurable trends and detailed explanations from respondents.

The target population comprised 200 DCI officers based in Nairobi City County, including officers deployed at DCI Headquarters and those serving in specialized fraud investigation units. These units included the Financial and Banking Fraud Investigations Unit, the Cybercrime Unit, and the Crime Research and Intelligence Bureau. The population included Gazetted Officers, Non-Commissioned Officers, and Constables.

The study used stratified random sampling to ensure representation across different ranks. Stratification was appropriate because the target population consisted of officers at different levels of responsibility and experience. Following the recommendation by Mugenda and Mugenda (2003) that a sample of 30% is adequate for populations below 10,000, the study selected 60 officers from a target population of 200.

The sample size was calculated as follows:

$$n = N \times 30/100$$

where n = sample size and N = target population. Therefore, $n = 200 \times 30/100 = 60$.

**Table 1**

*Sample Distribution*

| Category | Target Population | Sample Size |
|---|---|---|
| Assistant Superintendent | 7 | 2 |
| Chief Inspector | 9 | 3 |
| Inspector | 16 | 5 |
| Senior Sergeant | 25 | 8 |
| Sergeant | 35 | 11 |
| Corporal | 43 | 13 |
| Constable | 65 | 20 |
| **Total** | **200** | **60** |

Data were collected using semi-structured questionnaires and key informant interviews. The questionnaires contained both closed-ended and open-ended questions. Closed-ended questions used a five-point Likert scale ranging from strongly disagree to strongly agree. The questionnaires collected information on training quality, technical competence, challenges affecting cyber fraud investigations, and strategies for improving training effectiveness. Key informant interviews were conducted with senior DCI officers to obtain deeper insights into institutional training practices, operational challenges, and cyber fraud investigation needs. Secondary data were obtained from published journal articles, books, government publications, and institutional records.

The questionnaire was reviewed by two criminology faculty members to establish face validity. Their comments were used to improve clarity, relevance, and wording of the research items. A pilot test was conducted in Kiambu County involving 10 DCI officers who were not part of the main study. Kiambu County was selected because of its proximity to Nairobi City County, comparable policing environment, and similar cyber fraud patterns. Although the pilot sample was smaller than the conventional threshold of 30 respondents, it provided useful feedback on clarity and reliability. Reliability was tested using Cronbach's alpha, with values ranging from 0.79 to 0.82. Since values above 0.70 are considered acceptable for internal consistency, the instruments were considered reliable (Nunnally, 1978).

**Table 2: Pilot Test Results**

| Instrument | N | Cronbach's Alpha | Clarity | Adjustment Made |
|---|---|---|---|---|
| Technical competence | 10 | 0.82 | Mostly clear | Simplified two technical items |
| Challenges affecting training | 10 | 0.79 | Clear overall | Reworded one ambiguous item |
| Strategies adopted | 10 | 0.81 | Clear | Added clarifying examples |

Quantitative data were cleaned, coded, and entered into SPSS version 26 for analysis. Descriptive statistics, including frequencies and percentages, were used to present the findings. Due to the relatively small sample size, inferential statistical tests were not conducted. Qualitative data from open-ended questionnaire items and interviews were analysed using thematic analysis. Responses were transcribed, coded, and grouped into recurring themes. Representative quotations were used to support the quantitative findings.

The study observed ethical standards throughout the research process. Authorization was obtained from the relevant university research committee, the National Commission for Science, Technology and Innovation, the Inspector General of Police, and the Director of Criminal Investigations. Respondents were informed about the purpose of the study and their voluntary participation. Informed consent was obtained before data collection. Confidentiality was maintained by excluding names and personal identifiers from the research instruments. Respondents were also informed of their right to withdraw from the study at any time.

## RESULTS

### Response Rate

Out of the 60 sampled DCI officers, 54 returned usable questionnaires, representing a response rate of 90%. This response rate was considered adequate for descriptive analysis.

### Effect of Training Quality on Technical Competence

Respondents were asked whether the quality of police training affects DCI officers' competence in cyber fraud investigations.

**Table 3:** *Effect of Training Quality on Competence*

| Response | Frequency | Percentage |
|---|---|---|
| Yes | 46 | 85.2 |
| No | 8 | 14.8 |
| **Total** | **54** | **100.0** |

The findings show that 85.2% of respondents agreed that the quality of police training affects officers' competence in cyber fraud investigations. This indicates that training is perceived as a major determinant of investigative effectiveness. However, 14.8% disagreed, suggesting that some officers may consider other factors, such as tools, funding, experience, or institutional support, to be more important than training alone.

**Importance of Specific Elements in Cyber Fraud Investigations**

Respondents rated the importance of selected elements in cyber fraud investigations. The results are presented in Table 4.

**Table 4:** *Importance of Selected Elements in Cyber Fraud Investigations*

| Statement | Strongly Agree n (%) | Agree n (%) | Undecided n (%) | Disagree n (%) | Strongly Disagree n (%) | Total Agree (%) | Total Disagree (%) |
|---|---|---|---|---|---|---|---|
| Emphasis on officer digital security | 24 (44.4) | 19 (35.2) | 1 (1.9) | 6 (11.1) | 4 (7.4) | 79.6 | 18.5 |
| Public education on cyber fraud | 30 (55.6) | 10 (18.5) | 1 (1.9) | 7 (13.0) | 6 (11.1) | 74.1 | 24.1 |
| Regular digital awareness training | 28 (51.9) | 12 (22.2) | 0 (0.0) | 10 (18.5) | 4 (7.4) | 74.1 | 25.9 |
| Monitoring suspect behaviour online | 12 (22.2) | 18 (33.3) | 5 (9.3) | 9 (16.7) | 10 (18.5) | 55.5 | 35.2 |
| Use of digital surveillance technologies | 17 (31.5) | 23 (42.6) | 2 (3.7) | 5 (9.3) | 7 (13.0) | 74.1 | 22.3 |

*Note.* Percentages are rounded to one decimal place.

The findings show strong support for officer digital security, public education, regular digital awareness training, and digital surveillance technologies. Officer digital security recorded the highest agreement at 79.6%, suggesting that respondents recognized the need to protect investigators from cyber risks while performing their duties.

Public education and regular digital awareness training each recorded 74.1% agreement, indicating that officers considered prevention and continuous learning important in cyber fraud control. However, monitoring suspect behaviour online recorded lower support, with 55.5% agreement and 35.2% disagreement. This suggests a divided view among officers, possibly due to legal, ethical, technical, or resource-related concerns.

**Extent to Which Technical Competence Affects Investigation Effectiveness**

Respondents were asked to rate the extent to which technical competence affects the effectiveness of cyber fraud investigations.

**Table 5: Technical Competence and Investigation Effectiveness**

| Extent of Influence | Frequency | Percentage |
|---|---|---|
| Great extent | 30 | 55.6 |
| Moderate extent | 18 | 33.3 |
| Small extent | 4 | 7.4 |
| No extent | 2 | 3.7 |
| **Total** | **54** | **100.0** |

The findings show that 55.6% of respondents indicated that technical competence affects investigation effectiveness to a great extent, while 33.3% indicated a moderate extent. This means that 88.9% of respondents recognized technical competence as an important factor in effective cyber fraud investigations.

Qualitative findings supported this result. Respondents explained that cyber fraud investigations require knowledge of digital evidence, electronic transactions, mobile money systems, online communication, and digital forensic procedures. One respondent stated: *"Without the right technical know-how, even the most committed investigator becomes ineffective against sophisticated cybercriminals."* Another respondent emphasized the importance of evidence handling: *"Many of our delays come from not knowing how to extract or interpret data correctly; by the time we learn, evidence may already be lost."*

A senior officer also observed that technical skills were unevenly distributed across the department:

"In our department, some officers are highly skilled in digital forensics, but others still struggle with basic computer operations. This imbalance slows down investigations and creates dependency on a few technical officers. When those officers are unavailable, entire cases stall."

These responses show that the effectiveness of training is not only affected by whether training exists, but also by how evenly technical skills are distributed across ranks and units.

**Technical and Knowledge Challenges Affecting Cyber Fraud Investigations**

Respondents were asked whether technical and knowledge challenges hinder effective cyber fraud investigations.

**Table 6: Technical and Knowledge Challenges**

| Response | Frequency | Percentage |
|---|---|---|
| Strongly agree | 30 | 55.6 |
| Agree | 18 | 33.3 |
| Undecided | 2 | 3.7 |
| Disagree | 1 | 1.9 |
| Strongly disagree | 3 | 5.6 |
| **Total** | **54** | **100.0** |

The findings show that 88.9% of respondents agreed that technical and knowledge challenges hinder cyber fraud investigations. This indicates strong consensus that skill gaps, limited technical exposure, and inadequate knowledge of emerging technologies affect investigative performance.

Qualitative responses showed that officers were particularly concerned about the fast pace of technological change. One respondent stated: *"The majority of the technical issues originate from the rapid expansion of digital platforms that our training has not yet covered."* Another respondent highlighted the digital forensic gap: *"Lack of specialized digital forensic skills makes it impossible to collect and maintain electronic evidence correctly."* These findings suggest that cyber fraud training must be continuous, practical, and regularly updated to respond to emerging technologies and new criminal methods.

**Emphasis on Advanced Cyber Analytic Tools**

Respondents were asked whether more emphasis should be placed on advanced cyber analytic tools during police training.

**Table 7: Emphasis on Advanced Cyber Analytic Tools**

| Response | Frequency | Percentage |
|---|---|---|
| Strongly agree | 31 | 57.4 |
| Agree | 13 | 24.1 |
| Undecided | 1 | 1.9 |
| Disagree | 5 | 9.3 |
| Strongly disagree | 4 | 7.4 |
| **Total** | **54** | **100.0** |

The findings show that 81.5% of respondents supported greater emphasis on advanced cyber analytic tools in police training. This indicates that most officers recognize the need for practical exposure to modern investigative technologies. However, 16.7% disagreed or strongly disagreed, suggesting that some officers may have concerns about access, implementation, cost, or their own preparedness to use advanced tools effectively.

## DISCUSSION

The study found that police training plays a major role in improving the technical competence of DCI officers involved in cyber fraud investigations. The finding that 85.2% of respondents agreed that training quality affects competence aligns with Mugo and Mwangi (2017), who observed that cyber fraud poses serious challenges for Kenyan police officers and requires targeted capacity building. It also aligns with Holt and Bossler (2014), who emphasize that cybercrime investigation requires specialized knowledge of digital systems, data recovery, network security, and electronic evidence. The findings further support the argument that traditional policing methods are inadequate for cyber fraud investigations. Mwakio et al. (2020) argue that law enforcement agencies must improve their preparedness to address white-collar and technology-enabled crimes. In the present study, respondents identified digital forensic skills, evidence preservation, and technical analysis as important areas of competence. This confirms that cyber fraud investigations require skills beyond conventional interviewing, statement-taking, and physical evidence collection.

Further, technical competence affects investigation effectiveness. A total of 88.9% of respondents reported that technical competence affects effectiveness either to a great or moderate extent. This finding agrees with Wamuyu (2019), who found that cybersecurity training influences the competence of law enforcement agencies in Kenya. It also supports Otieno and Ouko (2021), who identified inadequate technical capacity as one of the challenges facing cybercrime investigations in Kenya. A key issue emerging from the qualitative findings is the uneven distribution of technical skills among officers. Some officers were reported to have strong digital forensic skills, while others struggled with basic computer operations. This imbalance creates dependence on a few specialized officers, delays investigations, and weakens institutional capacity. This finding is important because it shows that training effectiveness should not only be measured by the presence of trained personnel, but also by the extent to which competence is distributed across relevant units and ranks.

The finding that 88.9% of respondents agreed that technical and knowledge challenges hinder cyber fraud investigations demonstrates the seriousness of the training gap. Cyber fraud methods change rapidly, and officers require regular exposure to new tools, digital platforms, and investigative procedures. Wall (2017) argues that cybercrime policing requires adaptation to networked technologies and online criminal environments. The present study confirms this argument by showing that officers face difficulties when training does not keep pace with changing technologies. The study also found that 81.5% of respondents supported greater emphasis on advanced cyber analytic tools. This suggests

that officers recognize the value of technology-based investigation methods. Ong'ale et al. (2025) similarly show that technological reforms influence performance among DCI officers in Kenya. However, the study also found that a minority of respondents disagreed with the emphasis on advanced tools. This may reflect concerns about inadequate basic digital literacy, limited resources, poor implementation, or lack of confidence in using advanced systems.

One of the most notable findings was the divided response on monitoring suspect behaviour online. Although 55.5% of respondents supported it, 35.2% disagreed. This level of disagreement suggests that officers may have concerns regarding legality, privacy, ethics, technical ability, or availability of approved surveillance tools. Cyber fraud investigations often require online monitoring, but such activities must be guided by clear legal and operational safeguards. The finding therefore points to the need for training that covers not only technical surveillance skills, but also data protection, privacy rights, evidentiary standards, and lawful investigative procedures.

The findings also show that cyber fraud investigation is not solely a training issue. While training improves competence, effectiveness is also influenced by institutional resources, digital forensic infrastructure, inter-agency cooperation, and access to modern tools. Aphane and Mofokeng (2021) found similar challenges in South Africa, where police response to cybercrime was affected by limited resources, capacity gaps, and coordination problems. This suggests that Kenya's DCI requires both improved training and stronger institutional support systems.

Overall, the study confirms that police training is essential for effective cyber fraud investigations in Nairobi City County. However, training must be specialized, practical, continuous, and supported by adequate tools and institutional structures. Without this support, even trained officers may face difficulties in handling sophisticated cyber fraud cases.

## Conclusions

The study concludes that police training plays an important role in improving the technical competence of DCI officers in cyber fraud investigations, particularly in handling digital evidence, analysing online transactions, and responding to cyber-enabled offences and that the effectiveness of police training is weakened by technical and knowledge-related challenges such as rapid technological change, inadequate digital forensic skills, uneven technical capacity among officers, and limited practical exposure to emerging cyber fraud methods. Further, although the DCI has adopted strategies to improve cyber fraud investigation capacity, these strategies need to be strengthened through continuous professional development, modern cyber analytic tools, improved forensic infrastructure, and clear guidelines on lawful online monitoring.

## Recommendations

To enhance the technical competence of DCI officers in cyber fraud investigations, the National Police Service and DCI should strengthen training on practical digital forensic

skills, electronic evidence handling, cyber law, and online transaction analysis. In addition, to address challenges affecting the effectiveness of police training, the DCI should introduce mandatory continuous professional development to keep officers updated on emerging cyber fraud methods, new digital platforms, and lawful online monitoring procedures. Government should provide modern cyber investigation tools, digital forensic software, secure data storage systems, and improved forensic laboratory access.

## References

1. Aphane, M., & Mofokeng, J. (2021). South African Police Service's capacity to respond to cybercrimes: Challenges and potentials. Journal of Southwest Jiaotong University, 56(4). https://doi.org/10.3514/issn.0258-2724.56.4.15
2. Arigo, B. A., & Sellers, B. G. (2021). The pre-crime society: Crime, culture, and control in the ultra-modern age. Policy Press.
3. Central Bank of Ghana. (2019). The 2019 banking industry fraud report. https://www.bog.gov.gh/news/the-2019-banking-industry-fraud-report
4. Holt, T. J., & Bossler, A. (2014). Cybercrime. In Oxford handbooks online. Oxford University Press. https://doi.org/10.1093/oxfordhb/9780199935383.013.002
5. Linda, K. (2021). Increasing public safety in Baltimore through building transformative community and police partnerships.
6. Mugenda, O. M., & Mugenda, A. G. (2003). Research methods: Quantitative and qualitative approaches. Acts Press.
7. Mugo, M., & Mwangi, J. (2017). Cyber-fraud and its challenges to the Kenyan police: A case study of Nairobi County. Journal of Cybersecurity Studies, 3(2), 120–133.
8. Muriuki, P., & Mbaya, K. B. (2023). Information communication technology crimes and offences in Kenya. National Crime Research Centre.
9. Mwakio, P., Mathenge, G., & Maroko, G. (2020). Assessing preparedness of law enforcement agencies in dealing with white collar crimes in Kenya: A case of Nairobi City County. International Journal of Research and Innovation in Social Science, 4(7), 134–144.
10. Nyabira, B. O., Otiso, W. O., & Kaguta, J. (2019). Effect of police training programme content and delivery methods on counter-terrorism capability in Kenya. International Journal of Academic Research in Accounting, Finance and Management Sciences, 3(1), 1–10.
11. Nunnally, J. C. (1978). Psychometric theory (2nd ed.). McGraw-Hill.
12. Ong'ale, M. A., Sirera, M. A., & Mwangi, J. W. (2025). Influence of technological reforms and performance in law enforcement among Directorate of Criminal Investigations officers in Kenya. International Journal of Advanced Research, 13(5), 1516–1529. https://dx.doi.org/10.21474/IJAR01/21043
13. Otieno, S., & Ouko, J. (2021). Challenges facing cybercrime investigations in Kenya: A law enforcement perspective. African Journal of Criminology and Justice Studies, 14(1), 45–63.
14. Wa Teresia, N. J. (2025). Digital policing in Kenya: Opportunities and challenges. East African Journal of Law and Ethics, 8(1). https://doi.org/10.37284/2707-5338
15. Wall, D. S. (2017). Policing cybercrime: Networked and social media technologies and the challenges for policing. Policing and Society, 27(3), 284–298. https://doi.org/10.1080/10439463.2016.1212418
16. Wamuyu, P. K. (2019). Cybersecurity training and its effectiveness on the competence of law enforcement agencies in Kenya. African Journal of Criminology and Justice Studies, 12(1), 81–98.
17. Waswa, B. (2023). Enhancing cybercrime investigation effectiveness: A multi-faceted analysis of information technology tools, digital evidence quality, and law enforcement security measures [Unpublished master's thesis]. KCA University.