

DOES DIGITAL FORENSIC CAPABILITIES DRIVES EFFICIENCY IN REVENUE INVESTIGATIONS? AN EMPIRICAL STUDY OF THE KENYA REVENUE AUTHORITY FRAMEWORK:

Author 1: PHILIP MNANGAT KAPKAI

Student Kenyatta University
Department of Public Policy and Administration
Email: kphilipmnangat@gmail.com

Author 2: DR. JANE NJOROGUE, PHD

Senior Lecturer
Kenyatta University
Department of Public Policy and Administration
Email: njoroge.jane@ku.ac.ke

ABSTRACT

The fast-digital evolution of Kenya brought modern tax administration but created sophisticated electronic fraud schemes, cybercrimes and technological-based tax avoidance methods. The Kenya Revenue Authority (KRA) created a Cyber Operations and Digital Forensics Laboratory under its Investigation and Enforcement Department in 2024 to address the developing security threats. The research investigates how people, processes and technology systems work together to enhance investigation speed and evidence strength and court victory rates through the Resource-Based View and Systems Theory frameworks. From the research, digital forensic capabilities shorten investigation periods and produce better evidence quality while improving teamwork between different organizations. The research identifies three main obstacles which include insufficient trained personnel, equipment and legal frameworks. Digital forensics serves as a dual purpose of protecting national security and maintaining fiscal integrity. The research suggests that KRA should integrate forensic capabilities into its corporate strategy while developing more experts and creating standardized digital evidence procedures for all government agencies.

Key Words: *Digital Forensic Capabilities, Efficiency, Kenya Revenue Authority*

CHAPTER ONE

1. INTRODUCTION

The economic world of taxation and financial management undergoes rapid changes because technology supports all financial operations. The Kenya Revenue Authority (KRA) benefits from digital platforms including iTax and TIMS and e-TIMS systems which improve operational efficiency and transparency in Kenya. The digital transformation has created new complex cyber threats which standard investigative methods fail to detect because they involve advanced technology-based tax evasion schemes and data manipulation and electronic fraud (Adegboyega, T. 2022)

The government faces a critical challenge because electronic fraud and illicit financial flows result in substantial revenue losses which affect its ability to generate domestic resources needed for economic independence and national defense. The main revenue collection agency KRA needs to evolve through digital-forensic system implementation for its investigative work. Digital forensics allows investigators to retrieve electronic evidence and build system activity timelines which produce court-admissible evidence (Vita MK & SM Muathe, 2023)

The Investigations and Enforcement Department of KRA created a Cyber Operations and Digital Forensics Laboratory to serve as its digital evidence analysis center. The laboratory exists to detect and analyze digital evidence which investigators can obtain from computers and mobile devices and internal database systems. The laboratory functions as a dual technical and strategic resource which enables investigators to track digital evidence from tax violators and internal security threats. The laboratory began operations in 2024 to help investigators solve cases related to VAT refund scams and identity theft and system tampering. The laboratory's forensic evidence support leads to faster case resolution and better court outcomes than traditional audit-based investigations.

The current performance of KRA's forensic capabilities remains unclear because it is unknown how well these capabilities enhance operational efficiency. The combination of tools and trained personnel and established processes delivers better investigation speed and stronger court evidence quality. The current performance of KRA's forensic capabilities faces obstacles because of institutional constraints and insufficient resources. The main reason behind this research stems from these specific questions (Wambua, J. M. (2026).

This research paper investigates how digital-forensic capabilities affect the speed of revenue investigation work at the Kenya Revenue Authority. The research investigates how people and processes and technology systems affect case results while demonstrating the essential role of digital forensics for Kenya's financial stability and national defense. The research results will help develop policy changes while demonstrating that forensic readiness functions as an essential requirement for contemporary public organizations (Choge, Kimaku & Njeri, 2026)

2. STATEMENT OF THE PROBLEM

The Kenyan government through KRA dedicated major funding to digital system development for tax compliance improvement and expanded tax base coverage during the last decade (Lutomia, Njoroge & Muna, 2026). The implemented reforms automated basic operations yet they created a

new environment which financial criminals can use for their activities. The current tax system faces three types of fraud because criminals use data security vulnerabilities to steal information and they use electronic methods to create fake invoices and they edit e-TIMS records to hide their tax evasion activities. Standard audit trails fail to detect complex cyber-enabled schemes which result in annual losses of billions of shillings (Wambua, J. M. 2026).

The Authority created a Cyber Operations and Digital Forensics Laboratory in 2024 to fight cyber threats but there is no proof that this capability affects the speed of investigations. The internal assessment reports show better evidence quality and faster processing times but digital evidence backlogs continue to grow and most prosecutions fail because of inadmissible digital evidence. The investigation process becomes difficult because of insufficient trained personnel and outdated forensic equipment and extended procurement timelines which stop active investigations. The system faces two major obstacles because different agencies use incompatible systems and they cannot share data with each other.

The current gaps between KRA digital-forensic spending and revenue investigation performance need evaluation to determine their actual effects. Organizations base their policy decisions and resource allocations on reactive approaches because there is no empirical evidence to validate this relationship. The assessment of KRA's present forensic framework needs to happen because it protects both organizational success and Kenya's economic independence through proper tax law enforcement.

3. RATIONALE AND JUSTIFICATION OF THE STUDY

Revenue collection is the foundation of a nation's economic and political sovereignty. The ongoing occurrence of tax leakages creates difficulties for governments to allocate funds for defense and social protection and development initiatives. The digital revolution in Kenya has brought modernization to KRA operations yet it has created new opportunities for complex tax evasion methods. The research purpose exists to prove digital-forensic capability has evolved into a strategic necessity which KRA and Kenya's national security system must implement.

First, digital forensics enhances accountability. Organizations can detect insider collaboration and system tampering and cyber-fraud operations through digital transaction tracking when they collect and analyze these records properly. The integration of forensic procedures into KRA's investigative system enables investigators to collect evidence that can be proven through science and law which enhances public trust in their enforcement activities.

Second, forensic capacity directly supports efficiency. The automated evidence acquisition process enables investigators to complete their work faster because it enables them to process multiple cases simultaneously while officers dedicate their time to crime analysis and prevention efforts. The environment of billion-dollar revenue losses makes every small improvement in efficiency produce substantial financial gains for the government.

Third the capability enables the achievement of national and regional policy targets. The sustainable development framework of Vision 2030 bases its foundation on three essential elements which include security and governance and rule of law. The National ICT Policy (2024) demands government institutions to enhance their cyber-security systems while Kenya

needs to boost its ability to identify money laundering and illicit trade activities to fulfill FATF and EAC standards. The forensic program at KRA maintains a strong position to achieve these goals.

The research finds its justification through the requirement for evidence-driven educational transformation. The Authority needs to understand how current digital-forensic resources affect investigations to improve its strategy and budget allocation and support changes in existing laws. The findings will also provide a model for other public agencies seeking to balance innovation, efficiency, and accountability in the digital era.

SIGNIFICANCE OF THE STUDY

The significance of this paper extends well beyond the confines of the Kenya Revenue Authority. The example shows how digital forensics operates as an independent organizational capability which strengthens financial management and protects national security and builds trust between citizens and government institutions.

For KRA's management, the study provides an evidence base for strategic investment. The document demonstrates that digital tool investments and staff training expenses from the Authority enable faster investigations which generate better cases that result in increased revenue collection. The forensic laboratory will gain budget approval from Treasury and Parliament through evidence-based data which demonstrates its efficiency gains. The forensic laboratory will achieve revenue protection status instead of being viewed as a cost centre through its budget allocation justification process.

The research shows that law-enforcement agencies need to establish standardized digital evidence procedures which the DCI and EACC and ODPP and FRC must adopt. The implementation of shared forensic terminology with standardized technology systems reduces duplicate work while safeguarding evidence trails and improves multi-agency team operations.

The research provides policy-makers with useful information which they can use to create new laws. The research results will guide developers to enhance the Evidence Act and Tax Procedures Act for digital evidence management through modern legal framework updates. They will also support Kenya's commitments under the Financial Action Task Force (FATF), the OECD Global Forum on Transparency, and the East African Community (EAC) strategy against illicit financial flows.

The research brings value to digital forensics in public finance administration because it supports the development of this new academic discipline. The framework connects three distinct fields of information technology and law enforcement and fiscal policy to establish a complete knowledge base. The developed model provides direction for researchers to conduct additional studies between the Uganda Revenue Authority (URA) and the Tanzania Revenue Authority (TRA) and their respective regional tax administration systems.

The research shows that Kenyan society gains advantages from investigations which use technology to achieve both fast results and open operations. Digital systems which perform tax collection and fraud detection and punishment functions lead to improved citizen compliance because they build

stronger bonds between citizens and public institutions. The research supports national goals for integrity and accountability and sustainable development which Vision 2030 has established.

SCOPE OF THE STUDY

The research scope defines the particular research domains which consist of thematic analysis and spatial and temporal boundaries to assess KRA digital-forensic capabilities. The document establishes research limits and describes the study organization and time span.

The research investigates how digital forensic capabilities affect the speed of investigations which occur during KRA enforcement operations. The independent variable digital-forensic capability consists of three fundamental elements. People: the knowledge, skills, and professional certifications of forensic investigators and analysts; Processes: the procedures, standard operating protocols, and institutional governance frameworks that guide forensic work; and The technology sector includes all hardware and software and analytical tools that enable digital evidence imaging and analysis and reporting processes. The research investigates investigative efficiency through four main indicators which include case resolution duration and evidence quality and admissibility and prosecution success rates and recovered financial gains. Organizations can evaluate digital forensics effects on operational performance by studying established connections between these elements.

Spatially, the study is confined to the Kenya Revenue Authority, with a particular focus on its Investigations and Enforcement Department and the Cyber Operations and Digital Forensics Laboratory, which was established in 2024. The IE&D collects and analyzes intelligence data which it uses to support law enforcement operations while the laboratory conducts digital evidence analysis. Although based in Nairobi, the department's forensic work has national reach since most high-value cases and digital evidence extractions are processed at the headquarters. The research includes comparative analysis of KRA's work with other essential agencies including the Directorate of Criminal Investigations (DCI) and the Ethics and Anti-Corruption Commission (EACC) and the Office of the Director of Public Prosecutions (ODPP).

The time period shows how KRA developed its forensic capabilities from external digital evidence collection to complete laboratory operations. The system enables researchers to study performance changes between the time before establishment and after establishment through its ability to track investigative timeframes and evidence quality and case results.

CHAPTER TWO

LITERATURE REVIEW

Concept of Digital Forensics

Digital forensics requires a systematic process to discover electronic evidence through evidence collection and preservation and analysis and presentation for court acceptance (Casey, 2019). The process requires special procedures which go beyond typical IT support because it needs to meet legal standards. The four canonical stages of forensic investigation follow the guidelines from ISO/IEC 27037, 27041 and 27042 frameworks which preserve integrity throughout the process from seizure to final presentation.

Digital forensics in revenue administration helps investigators track down electronic evidence which shows tax evasion and invoice tampering and insider cheating activities. The field now extends beyond computer hard-disk analysis to include mobile and network and cloud environments because financial evidence appears on various digital platforms. The scientific link between technology and law enforcement in Kenya relies on digital forensics because Kenya operates its financial system through electronic invoicing and mobile-money transactions. (Kimani, M., & Mugo, P. 2023).

Revenue Investigations and Efficiency

The evaluation of investigation efficiency depends on four essential factors which include both speed and precision and financial efficiency and successful case results. The progression of cases through revenue agencies from detection to prosecution depends on how quickly cases get resolved and the quality of evidence used for enforcement purposes. The current audit system depends on manual document verification which leads to extended processing times of months and generates evidence that can be challenged by parties involved. Digital-forensic techniques reduce investigation time through automated data extraction and hash value verification for authenticity and tamper-proof log generation (Lutomia, Njoroge & Muna, 2026)

Mutua and Kinyua (2022) found that digital tool implementation in Kenya's tax investigation process made the system more efficient by reducing case resolution times by 50%. The South African Revenue Service (SARS) used data-imaging tools to combat electronic VAT fraud which caused billions of dollars in revenue loss. These examples illustrate that efficiency gains flow not only from faster technology but also from disciplined adherence to forensic procedure.

Theoretical Review

Systems Theory: The enforcement ecosystem of KRA contains four interconnected subsystems which include intelligence operations and investigation activities and prosecution services and information communication technology systems. Systems Theory shows that performance results from the successful interaction between different subsystems. A laboratory with strong technical abilities will not reach its objectives because data-sharing

systems and legal frameworks need to operate correctly. Hence, forensic efficiency is a function of both internal capacity and external coordination. The following frameworks help us study capability maturity by looking at institutional system integration instead of tool ownership. (Englbrecht, Meier , & Pernul 2020)

Digital-Forensic Capability Models

The Digital Forensic Capability Maturity Model (DFCMM) and NIST Cybersecurity Framework present capability-maturity models which show development from unstructured response to peak operational performance. External experts serve as the main source of support for new organizations but intermediate organizations create their own labs and procedures and mature organizations integrate forensics into their policy framework and ongoing improvement processes (Hanaei, & Rashid, 2014)

The Authority used the Directorate of Criminal Investigations (DCI) to obtain digital evidence until 2024. The Cyber Operations and Digital Forensics Laboratory established the "defined" stage through its development of structured processes and dedicated budgets and specialized staff. Organizations need to achieve "optimised" status through automation system implementation and predictive analytics deployment and continuous human capital development (Englbrecht, Meier & Pernul, 2020).

CHAPTER THREE

RESEARCH DESIGN AND METHODOLOGY

Research Design

The research design uses qualitative descriptive research design to study how KRA digital-forensic capabilities affect the speed of investigation processes. The research method should employ qualitative approaches when human elements and institutional operations and organizational cultural factors need to be studied. The researcher conducts descriptive analysis to document KRA's present forensic development status before using analytical interpretation to connect observed data with performance metrics that include case processing speed and evidence quality.

Study target Population

The study is situated within the Investigations and Enforcement Department of the Kenya Revenue Authority. The department responsible for intelligence collection and enforcement strategy development and forensic crime investigation. The program targets forensic analysts and investigators and intelligence officers and ICT security specialists and liaison officers who work at the Directorate of Criminal Investigations (DCI) and Ethics and Anti-Corruption Commission (EACC) and Office of the Director of Public Prosecutions (ODPP).

1. The research selects participants through purposive sampling because they possess direct experience with digital evidence management and investigative work. The organization depends on twenty-five officers who provide both technical and managerial expertise as its main information source.

Data Sources and Collection Methods

Documentary Review:

The research uses data from KRA internal reports and laboratory case registers and ISO/IEC compliance manuals and annual performance statistics which cover the period from 2020 to 2025. The documents contain numerical data which shows the total number of cases processed and case resolution times and the full amount of recovered funds.

Key Informant Interviews (KIIs):

The research includes semi-structured interviews with forensic specialists and investigators to obtain direct information about digital-evidence management operations from acquisition through analysis and reporting to courtroom presentation.

Process Tracing:

The research tracks all cases from start to finish to evaluate how forensic evidence collection methods affect both investigation duration and evidence integrity. The method shows how forensic

maturity develops causal links which result in particular efficiency outcomes. The combination of these methods creates triangulation which enhances the reliability and validity of research results.

Data Analysis

The research team conducted thematic analysis on all collected data for analysis. The research team applied recurring categories to analyze notes and interview transcripts for coding purposes which included forensic maturity and turnaround time and evidence integrity and inter-agency coordination. Patterns are compared with quantitative indicators derived from case statistics. Analytical matrices are then used to map relationships between capability dimensions (people, process, technology) and performance metrics.

The Digital Forensics Laboratory established in 2024 shows empirical changes through average values and percentage data and trend analysis results. The quantitative data receives additional interpretation through qualitative methods which explain the reasons behind reaching targets and failing to reach them.

CHAPTER FOUR

FINDINGS AND RESULTS

The purpose of this section is to interpret findings from the reviewed data and field information in relation to the objectives of the study. The document shows how digital forensic capabilities affect KRA investigation timelines by studying both positive and negative aspects of this change.

Current Capability Status

The Kenya Revenue Authority received digital evidence collection and analysis services from the Directorate of Criminal Investigations (DCI) until 2024. Though very supportive, the system created unintended delays in case processing. The Cyber Operations and Digital Forensics Laboratory which KRA established under the Investigations and Enforcement Department became a pivotal tool in the Authority's organizational growth.

The laboratory operates with trained forensic analysts who receive support from a developing technical team that specializes in mobile and network forensics and malware analysis and data recovery. The lab follows ISO/IEC 27037 standards and has created standard operating procedures (SOPs) which outline evidence management and imaging and documentation protocols.

A summary of digital-forensic cases handled between 2021 and 2024 is shown below:

Year	No. of Cases	Amount (KSh)	% of Total
2021	2	250,987,897	0.66%
2022	10	1,809,754,674	4.75%
2023	13	2,970,849,170	7.79%
2024	21	33,079,561,783	86.80%
Total	46	38,111,153,524	100%

Table 1: *Summary of digital-forensic cases*

The data shows that both case numbers and recovery in Kenya Shillings amounts rose substantially after the forensic laboratory began operations in 2024. The trend demonstrates that digital-forensic capability leads to measurable enhancements in KRA's investigative operations.

Effect on Investigative Efficiency

The assessment of efficiency used three primary indicators which included timeliness and evidence quality and case outcomes: The average case resolution period decreased from six months to two months. The combination of imaging tools with automated analysis software allows investigators to analyze multiple devices simultaneously which shortens evidence processing times. Hash-based verification, systematic chain-of-custody documentation, and use of validated forensic tools have improved the credibility of digital reports. Digital evidence faces minimal opposition from courts which has increased the trust levels of investigators and prosecutors.

Case Outcomes:

The success rate of prosecutions shows major growth when forensic evidence exists in criminal cases. The forensic reports establish digital financial transaction links to taxpayer bank accounts which makes revenue prosecution cases more powerful. The organization has developed its forensic capabilities through data-based investigation methods which now substitute for its previous manual audit system.

Organizational and Operational Challenges

The organization has reached multiple achievements yet multiple barriers exist to stop it from achieving its highest operational potential: **Human Capacity Gaps:** The forensic laboratory operates with limited personnel who possess only basic certifications while only a few members hold advanced EnCase and CHFI and GCFA certifications. The continuous movement of staff members between departments leads to a loss of institutional knowledge. **Resource Constraints:** The high cost of forensic equipment including imaging and analysis software presents a significant challenge. The long duration of procurement activities leads to software license expiration and tool compatibility problems. The laboratory operates without a complete digital-evidence management system which would consolidate all digital evidence into a single platform. The current state of secure storage systems and redundancy solutions for big data collections lacks proper development. **Legal and Policy Weaknesses:** The Evidence Act of Kenya (Cap 80) lacks full procedures for digital evidence management which creates court uncertainty about evidence acceptance. **Inter-Agency Coordination:** The lack of database integration between institutions together with trust issues between organizations creates delays in collaborative investigations. The KRA and DCI and EACC maintain separate operations which result in duplicated work and inconsistent evidence handling methods. The existing limitations require institutions to develop their capabilities for achieving complete digital-forensic capability potential.

Comparative and Regional Insights

The peer institutions in Africa have established functional methods which KRA should adopt. **Uganda Revenue Authority (URA):** The URA established a Forensic Data Centre which combines digital evidence analysis with tax-risk evaluation functions. The system enables early detection of irregularities which helps prevent cases from advancing to investigation level. **South African Revenue Service (SARS):** SARS uses its enterprise data warehouse to merge forensic intelligence which helps predict and detect VAT and customs fraud. The combination of data science with forensic auditing proved successful in SARS because it established an effective deterrent system. **Federal Inland Revenue Service (Nigeria):** The FIRS of Nigeria operates with the Economic and Financial Crimes Commission (EFCC) through cross-agency collaboration to track illegal financial activities. The examples demonstrate that KRA follows continental development patterns but its long-term success depends on achieving operational independence and financial stability and complete integration of analytical tools into daily work activities.

Organizational Culture and Leadership

Organizational culture together with leadership determines how well any technological innovation will succeed. Senior management at KRA supports digital forensics adoption which demonstrates their commitment to using data for making organizational decisions. Middle-level officers resist forensics because they believe this field needs specific knowledge that they do not possess.

All investigation units require continuous leadership support to establish digital forensics as their standard operational practice. Leadership needs to establish a learning environment through professional certification sponsorship for officers and departmental mentorship programs between different units. Digital forensics will evolve into an organizational standard through effective leadership which will make it a standard practice instead of a specialized function.

Regional and Policy Implications

The experiences of Kenya provide essential knowledge which other East African nations can learn from. The proliferation of mobile-money platforms and cross-border digital trade demands harmonized forensic standards. The East African Community (EAC) should create a Regional Digital Forensics Forum which would allow member states to exchange their financial crime investigation approaches and educational programs and criminal activity data.

Kenya should use its experience to develop African Union Convention on Cyber Security and Personal Data Protection (Malabo Convention) guidelines at the policy level. National security policy frameworks will achieve better results in stopping tax evasion and money laundering and terrorism financing through digital forensic capabilities.

Strategic Opportunities

The success of KRA's laboratory provides several opportunities for expansion: Academic Partnerships: The organization can develop skilled analysts through university partnerships while supporting local innovation in forensic software development. Regional Leadership: KRA can position itself as a regional training hub, exporting expertise to neighboring tax administrations and enhancing Kenya's influence in regional fiscal-governance forums. The government needs to establish particular policies and distribute money and build an effective workforce plan to reach these opportunities.

CONCLUSION AND RECOMMENDATIONS

Conclusion

The research investigated how digital forensic capabilities impact the operational speed of revenue investigations at the Kenya Revenue Authority. The Cyber Operations and Digital Forensics Laboratory has achieved complete transformation of investigative work according to evidence obtained from case records and institutional reports and interview data. The time needed to resolve cases has decreased while evidence quality and court acceptance have improved through scientifically backed reports that judges find more convincing.

The system brings operational advantages to KRA while making its institutional framework more solid. The forensic practice system provides complete visibility into all evidence collection and processing steps which investigators can use to show their evidence handling procedures. The process establishes trust between citizens and revenue enforcement agencies because it demonstrates their work follows established rules instead of personal choices. The research findings show digital forensics functions as a core security component which defends national defense and financial systems.

The research reveals multiple structural problems which threaten to diminish the achieved progress. The program faces multiple major obstacles because it lacks sufficient certified specialists and proper funding and modern equipment and insufficient coordination between agencies. The Evidence Act and Tax Procedures Act contain legal gaps which create additional obstacles for achieving uniform electronic evidence management. The complete deployment of digital forensics requires organizations to address their current system security weaknesses.

The digital-forensic capability of KRA shows better operational efficiency but needs ongoing leadership support and funding and policy changes to maintain its current level. The lessons learned by KRA provide other revenue authorities in the region with guidance to protect their internal financial resources and maintain their economic self-reliance.

Recommendations

The following are recommended:

Institutionalize a National Forensic Strategy; KRA needs to create a full Digital Forensics Strategy which will support its Corporate Plan 2023-2027 and Vision 2030.

Human-Resource Development: The Investigations and Enforcement Department needs to develop a particular career progression system for forensic experts.

Modernize Infrastructure and Tools: The organization needs to create a specific funding allocation for tool replacement expenses and cloud evidence storage and protected large data storage solutions.

Strengthen Inter-Agency Coordination: The organization should establish formal Memoranda of Understanding between KRA, DCI, EACC, ODPP and the Financial Reporting Centre to establish rules for evidence exchange and collaborative work and personnel transfers.

Legislative and Policy Reform: The Evidence Act (Cap 80) and Tax Procedures Act (2015) need amendments to add specific rules about digital evidence management and court acceptance and safeguarding of investigators.

Enhance Organizational Culture and Leadership Support: Management needs to establish an innovative and honest work environment through reward systems for forensic achievements and by making forensic training standard for all investigative personnel.

Regional Collaboration and Benchmarking: Kenya needs to establish an EAC Digital Forensics Forum which will unite standards while sharing investigative examples to develop digital forensic capabilities across the region.

Public Accountability and Transparency: The organization needs to develop annual digital-forensics performance reports which will show statistical information about processed cases and retrieved funds and learned knowledge.

REFERENCES

Adegboyega, T. (2022). Digital forensics and anti-corruption enforcement in Nigeria. *Journal of African Governance and Development*, 9(3), 42–58.

Al Hanaei, E. H. S. S., & Rashid, A. (2014). *DF-C²M²: A capability maturity model for digital forensics organisations*. In 2014 IEEE Security and Privacy Workshops (SPW), 57–60. IEEE. <https://doi.org/10.1109/SPW.2014.17>

Alenezi, A., Alqahtani, H., & Abu-Hassan, A. (2020). Digital-forensic capability and investigative performance in Gulf-region law-enforcement agencies. *International Journal of Cyber Security*, 9(2), 44–63.

Barney, J. (1991). Firm resources and sustained competitive advantage. *Journal of Management*, 17(1), 99–120.

Braun, V., & Clarke, V. (2006). Using thematic analysis in psychology. *Qualitative Research in Psychology*, 3(2), 77–101.

Casey, E. (2019). *Digital Evidence and Computer Crime: Forensic Science, Computers, and the Internet*. Academic Press.

Central Bank of Kenya. (2023). *National Risk Assessment on Money Laundering and Terrorism Financing*. Nairobi: CBK.

Choudhary, M., & Jain, R. (2021). Digital forensics: Applications in financial-crime investigation. *Journal of Financial Crime*, 28(3), 745–760.

Choge S.J, Kimaku P.M and Njeri I.N (2026) Digital Technologies and Tax Revenue Collection Efficiency at the Kenya Revenue Authority, Taita Taveta County, Kenya. *Journal of Management Research and Review Volume: 02 Issue: 06 June-2026*

- Englbrecht, L., Meier, S., & Pernul, G. (2020). *Towards a capability maturity model for digital forensic readiness*. *Wireless Networks*, 26, 4895–4907. <https://doi.org/10.1007/S11276-018-01920-5>
- Hope, K. R. (2022). Corruption, governance and development in Africa. *Journal of Public Affairs*, 22(4), e2812.
- International Monetary Fund. (2022). *Revenue Mobilization in Sub-Saharan Africa: Digitalization and Compliance*. Washington DC: IMF.
- ISO/IEC 27037: 2012. *Information Technology – Security Techniques – Guidelines for Identification, Collection, Acquisition and Preservation of Digital Evidence*. Geneva: International Organization for Standardization.
- ISO/IEC 27042: 2015. *Information Technology – Security Techniques – Guidelines for the Analysis and Interpretation of Digital Evidence*. Geneva: International Organization for Standardization.
- Kenya Revenue Authority. (2023). *Strategic Plan 2023 – 2027*. Nairobi: KRA.
- Kenya Revenue Authority. (2024). *Annual Revenue Performance Report 2023/24*. Nairobi: KRA.
- Kimani, M., & Mugo, P. (2023). Digital forensics and public-sector investigations in Kenya. *African Journal of Information Systems*, 13(4), 55–70.
- Lutomia, J Njoroge, W Muna (2026) Predictable Tax Systems: A Key Driver of Business Performance in Liquor Manufacturers in Nairobi City County, Kenya *Reviewed International Journal of Social Science & Humanities*, 7 (1), 427–449
- Mutua, J., & Kinyua, P. (2022). Integrating digital forensics in tax investigations. *Kenya Law Review*, 8(1), 101–120.
- Ngari, J. M. (2021). Cybercrime and digital forensics in East Africa. *African Journal of Criminology and Justice Studies*, 14(2), 45–62.
- Organisation for Economic Co-operation and Development (OECD). (2021). *Tax Crime Investigation and Digital Evidence: Emerging Practices*. Paris: OECD Publishing.
- United Nations Office on Drugs and Crime (UNODC). (2022). *Handbook on Digital Evidence and Electronic Signatures for Courts in Africa*. Vienna: UNODC.

Vision 2030 Delivery Secretariat. (2023). *Third Medium-Term Plan 2018 – 2022*. Nairobi: Government of Kenya.

Wambua, J. M. (2026). The Effect of Digital Tax Payment Platforms Integration on Turnover Tax Compliance Among Manufacturing Small and Medium Enterprises in the West of Nairobi, Kenya. *Journal of Finance and Accounting*, 6(3), 13-30.

Vita MK & SM Muathe (2023). The Role of Technology Adoption, Tax Base Expansion, Taxpayers' Education, Customer Service, and Strategy Communication on the Organizational. *International Journal of Organizational Leadership*, 277-294