Volume 11, Issue 4, April – 2026 International Journal of Innovative Science and Research Technology
ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/26apr1196

Assessing Wireless Network Forensics Tools, and Institutional Readiness: A Case Study Busitema University

Mudambi Geoffrey[1,2]; Davis Matovu[1]; Andrew Lukyamuzi[1]; Richard Angole[1]; Andrew Alunyu Egwar[3]

[1]Department of Computer Engineering and Informatics, Faculty of Engineering, Busitema University
[2]Directorate of Information Technology, Busitema University
[3]Department of Information Technology, Faculty of Computing and Information Sciences, Lira University

Publication Date: 2026/04/28

Abstract: **The study is to investigate wireless network forensics tools and institutional readiness at Busitema University. The research aims to evaluate the availability, effectiveness, and deployment of existing wireless forensic tools, as well as the university's preparedness to handle cyber incidents involving wireless networks. Using a mixed-methods approach comprising interviews with ICT personnel, system audits, and analysis of network infrastructure the study identifies critical gaps in the deployment and use of wireless forensics technologies. Findings indicate limited utilization of advanced forensic tools such as Wireshark, Aircrack-ng, and Kismet; inadequate staff training in wireless evidence handling; and the absence of structured policies guiding forensic investigations. Furthermore, the University lacks a dedicated digital forensics laboratory and a standardized incident response framework for wireless-related breaches. The study concludes that while Busitema University has foundational ICT infrastructure, its forensic readiness remains low. Recommendations include capacity building, acquisition of specialized wireless forensic tools, formulation of institutional policies, and establishment of a centralized digital forensics laboratory to enhance security and investigative capabilities.**

Keywords: *Wireless Network Forensics, Forensic Readiness, Cybersecurity, Digital Forensics Tools, Incident Response, ICT Infrastructure.*

How to Cite: Mudambi Geoffrey; Davis Matovu; Andrew Lukyamuzi; Richard Angole; Andrew Alunyu Egwar (2026) Assessing Wireless Network Forensics Tools, and Institutional Readiness: A Case Study Busitema University. *International Journal of Innovative Science and Research Technology*, 11(4), 2214-2219.
https://doi.org/10.38124/ijisrt/26apr1196

I. INTRODUCTION

In today's digitally interconnected world, wireless networks play a critical role in supporting academic, administrative, and research operations in higher education institutions. Universities increasingly depend on wireless technologies for communication, e-learning, data sharing, and remote access to academic resources. However, this growing reliance has also exposed them to a wide range of cyber threats, including unauthorized access, data interception, and denial-of-service attacks (Bedi et al., 2023). Wireless networks are inherently more vulnerable than wired networks due to their open transmission medium, making them prime targets for malicious activities that can compromise institutional data and disrupt academic functions (Ndiwalana & Kituyi, 2022).

Wireless network forensics—a specialized branch of digital forensics—focuses on the collection, preservation, and analysis of data transmitted over wireless channels to investigate and prevent such cyber incidents (Kumar & Singh, 2023). It involves techniques and tools designed to capture packets, analyze traffic behaviour, and reconstruct attack patterns from wireless communication traces. Tools such as Wireshark, Kismet, Air crack-ng, and Network Miner have become essential in identifying intrusion sources and understanding network anomalies. Despite global advances in this field, many institutions in developing countries face significant challenges in adopting effective wireless forensic tools due to limited technical capacity, insufficient funding, and lack of policy frameworks (Mirembe et al., 2023).

Busitema University is a leading public institution in Uganda wireless connectivity is central to academic and administrative operations. Yet, as with many developing country Universities, the increasing expansion of its wireless infrastructure has not been matched with equivalent growth

ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/26apr1196

in forensic readiness and cybersecurity resilience. Current systems may support basic network monitoring but fall short of providing end-to-end forensic visibility, structured incident response, or chain-of-custody assurance for digital evidence. This situation underscores the urgent need to assess the current state of wireless forensic tools and institutional preparedness to respond effectively to wireless based cyber threats.

Therefore, this study seeks to evaluate Busitema University's existing wireless forensic capabilities, identify gaps in tools and expertise, and propose a framework for improving forensic readiness. The findings are expected to contribute to enhancing cybersecurity resilience, evidence-based investigations, and policy development for higher education institutions in Uganda.

➢ *Research Purpose*

The purpose of this study is to assess wireless network forensic tools and the institutional readiness at Busitema University to effectively detect, investigate, and respond to cyber incidents involving wireless networks. The study seeks to identify the existing tools, technologies, and practices in use; evaluate their adequacy in supporting wireless forensic investigations; and analyse the capacity of technical personnel and infrastructure to handle wireless related cyber threats. Ultimately, the research aims to establish a clear understanding of the gaps between Busitema University's current wireless forensic capabilities and the required standards for effective forensic readiness. The findings will inform the development of recommendations and a strategic framework to enhance tool deployment, staff capacity building, policy formulation, and overall institutional preparedness for wireless network forensics. Identify existing gaps, challenges, and opportunities for improvement. Propose strategies for strengthening wireless forensic readiness and security resilience within the university.

➢ *Research Gap*

Despite the growing adoption of wireless technologies in higher education institutions, there remains a significant gap in the implementation and utilization of wireless network forensic tools, particularly in developing countries such as Uganda. While global studies have explored wireless forensics from a technical and theoretical perspective, there is limited context-specific research addressing the readiness of universities to deploy, operate, and sustain such tools within their ICT environments (Mirembe et al., 2023; Bedi et al., 2023).

At Busitema University, wireless networks are widely used to support e-learning, research, and administrative operations. However, the existing systems primarily focus on connectivity and performance monitoring rather than forensic investigation and evidence preservation. There is little documentation on the presence, effectiveness, or integration of forensic tools such as Wireshark, Kismet, or Aircrack-ng within the university's network management practices. Moreover, institutional readiness in terms of technical skills, policy frameworks, and digital evidence handling remains largely unexamined. Another critical gap lies in the absence of structured frameworks for assessing wireless forensic readiness in an academic institution like Busitema University. Existing research tends to emphasize enterprise or national security environments, overlooking universities that handle equally sensitive academic and research data. Furthermore, capacity limitations such as lack of trained forensic personnel, inadequate funding for specialized tools, and absence of standard operating procedures continue to hinder effective forensic response to wireless-based cyber incidents.

This study therefore fills these gaps by systematically assessing the current state of wireless network forensic tools and institutional preparedness at Busitema University, identifying weaknesses, and proposing an evidence-based framework to enhance forensic readiness and network security resilience.

➢ *Tools Used in Wireless Network Forensics*

Below are some of the tools commonly used. its main purpose, strengths, and how it could be applied in a campus environment.

Table 1 Above Shows the Wireless Network Forensics Tools Used in an Institution

Tool	Description & Strengths	Application in a University Wireless Network Setting
Wireshark	Packet-capture and protocol analyser. Free/open-source, cross-platform.	Use to capture WiFi network traffic (with appropriate hardware) and analyse specific suspicious flows, reconstruct sessions, etc. Good for forensic detail.
Kismet	Wireless network detector, packet sniffer, intrusion detection for 802.11. Works in monitoring mode.	Useful for passively detecting all access points/clients in a campus area, identifying hidden networks, rogue APs, etc. Good for reconnaissance & baseline mapping.
Xplico	Network forensics analysis tool (NFAT) that aims to reconstruct application-level data from packet captures.	After capturing traffic from WiFi, use Xplico to reconstruct sessions (e.g., HTTP, FTP) which can help in investigations of misuse (if permitted by policy/legal).
Aircrack-ng (and related toolsets)	Wireless auditing / penetration testing suite (not always framed as forensic, but relevant for vulnerability discovery).	In a university, the IT/security team might use Aircrack-ng to test their WiFi security posture (e.g., WEP/WPA key cracking) and thus help prepare for forensic readiness (recognise attack vectors).

ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/26apr1196

Tool	Description & Strengths	Application in a University Wireless Network Setting
Feature-Sniffer	A newer tool (research) aimed at extracting traffic features from WiFi access points (OpenWrt) for IoT/wireless forensic analysis.	If the campus has many IoT / smart devices connected via WiFi (e.g., smart labs, sensors), this tool could be adapted to monitor unusual device behaviour.
Commercial product example: Wireless-Detective	A professional tool for WLAN interception and forensic investigation (commercial, law-enforcement focus).	Although likely expensive, this type of tool could be considered if Busitema University's IT/security team has high-level forensic/investigation requirements (e.g., compliance, legal investigations).

➢ *Relevance of the Wireless Network Forensics Tools in Institutions*

The emerging wireless network forensic tools identified Feature-Sniffer, CSI Sniffer, IoTScent, and Decentralized Forensic Readiness Frameworks are highly relevant to improving the University's ability to monitor, investigate, and secure its wireless network infrastructure. Their adoption directly addresses the gaps in Busitema University's current forensic capabilities, particularly in tool deployment, data visibility, and evidence management. In the event of a security incident, specialized tools allow for effective collection and analysis of wireless traffic, logs, and device information, which are crucial for investigating breaches (Rathore et al., 2017).

Feature-Sniffer. This tool enhances wireless forensic readiness by enabling metadata-based traffic analysis rather than full packet captures. At Busitema University, where bandwidth and storage resources are limited, Feature Sniffer would make it feasible to monitor Wi-Fi activity across access points without overwhelming storage systems. It helps detect rogue devices, unusual connection attempts, and unauthorized access patterns, all essential for campus-wide forensic monitoring. Wireless forensics tools help detect unauthorized or rogue access points and devices that could compromise the network's security (Sangroya et al., 2021).

CSI Sniffer (Channel State Information Collection). CSI Sniffer adds a physical-layer perspective to forensics by analysing channel characteristics like signal fluctuations, interference, or device movement. In the university setting, this tool can detect anomalies such as rogue access points, spoofed MAC addresses, or unauthorized wireless activity even when data is encrypted. It therefore enhances the accuracy and depth of forensic investigations beyond traditional packet analysis tools like Wireshark.

IoTScent. As Busitema University integrates more IoT devices (e.g., biometric systems, environmental sensors, and laboratory equipment), IoTScent offers the ability to capture and analyze communication from non-Wi-Fi wireless protocols such as Zigbee, Thread, and Bluetooth. This widens the forensic scope to include all wireless data flows on campus, ensuring that forensic readiness extends beyond traditional Wi-Fi networks to the broader digital ecosystem. Wireless networks are vulnerable to unauthorized access, eavesdropping, and malicious attacks. Forensic tools help identify breaches, track sources of attacks, and analyse malicious activities (Kundur et al., 2020).

Decentralized Forensic Readiness Frameworks. These frameworks support secure, distributed storage of forensic data and logs collected from multiple wireless access points. Implementing such a framework would strengthen evidence integrity, enhance scalability, and reduce the risk of data tampering or loss. For a multi-campus institution like Busitema University, decentralized forensic readiness ensures that wireless forensic evidence is synchronized, protected, and easily retrievable during investigations. Regular forensic analysis helps institutions identify vulnerabilities, improve security policies, and ensure operational resilience (Sharma et al., 2019).

Integration with Existing Tools (Wireshark, Air crack-ng, Kismet). The new tools can complement existing open-source forensic platforms. For instance, metadata from Feature-Sniffer and CSI Sniffer can be correlated with packet-level data from Wireshark, providing a multi-layered forensic perspective. This integrated approach enhances the accuracy and comprehensiveness of network investigations.

- *Relevance of Wireless Network Forensics Tools in a Table form (Summery)*

Table 2 Summarises the Relevance of Wireless Network Forensics Tools that are Used at Busitema University.

Tool	Relevance to Busitema University Wireless Network	Key Benefit
Feature-Sniffer	Enables lightweight monitoring across campus Wi-Fi without heavy storage requirements.	Efficient forensic capture and anomaly detection.
CSI Sniffer	Provides physical-layer evidence for encrypted traffic and device movement.	Detects hidden or rogue wireless activities.
IoTScent	Expands forensic visibility to IoT and non-Wi-Fi networks.	Comprehensive device and protocol coverage.
Decentralized Forensic Framework	Ensures secure, distributed log storage and evidence retention.	Enhances evidence integrity and scalability.

ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/26apr1196

➢ *Wireless Network Forensics Readiness Framework*

Busitema has key building blocks (managed campus Wi-Fi, institutional ICT support, and teaching/research in forensics & security) but there's little public evidence of a complete, production-ready *wireless network forensics* framework (centralized packet capture, long-term retention, dedicated wireless forensics lab, formal incident-response playbooks, or published tool inventory). I rate current readiness **40–55%** (able to teach and prototype forensics, but needs investment to be operational for campus incident response).

A Wireless Network Forensics Readiness Framework (WNFRF) provides a structured approach that enables an organization or institution (Busitema University) to prepare its systems, processes, and people for effective forensic investigation of wireless network incidents. The goal of the framework is to ensure that potential digital evidence is systematically captured, preserved, analysed, and presented when security incidents occur.

➢ *Components of the Wireless Network Forensics Readiness Framework*

- *Policy and Governance Layer*

Establish clear policies defining the collection, retention, and use of wireless network evidence. Ensure adherence to national cyber laws, privacy regulations, and institutional data policies. Define responsibilities for ICT staff, security officers, and forensic investigators, Kasassbeh & Alshar'e (2022), Casey (2020); Scarfone & Mell, (2021)

- *Infrastructure and Tools Layer*

Deploy wireless access points (APs) capable of logging authentication, association, and disassociation events. Utilize both open-source and commercial tools for capturing and analysing network traffic: *Open-source:* Kismet, Aircrack-ng, Wireshark, Tcpdump. *Commercial:* Air Magnet WiFi Analyzer, MetaGeek Eye P.A., SolarWinds Network Analyzer. Data Collection Mechanisms: Implement centralized log servers and packet capture appliances that support real-time monitoring. Kismet Documentation (2024); Aircrack-ng Project (2024); Al-Kasassbeh et al. (2021), Kasassbeh et al. (2021).

- *Data Management and Evidence Handling Layer*

Capture wireless packets, authentication logs, and system events continuously or on demand. Establish standardized procedures to document evidence handling from acquisition to storage. Use hash-based integrity verification and secure storage (encrypted drives or forensic containers). Define how long data and logs are stored and under what access controls. Casey (2020);

- *Human and Capacity Development Layer*

Regularly train IT and security personnel on wireless forensic tools and best practices. Conduct mock investigations and capture-the-flag exercises to test readiness. Engage with academic programs, law enforcement, and cybersecurity agencies for knowledge sharing. Busitema University Graduate Studies (2023);

- *Incident Response and Forensic Process Layer*

Wireless Intrusion Detection/Prevention Systems (WIDS/WIPS) identify anomalies. Capture volatile data before it's lost; isolate compromised systems. Reconstruct events using captured logs, traffic data, and device associations. Present findings in structured reports suitable for disciplinary or legal proceedings in digital forensics research Baryamureeba & Tushabe (2004); Palmer (2001).

- *Continuous Improvement Layer*

Analyse investigation outcomes to refine procedures. Regularly update forensic tools and firmware of access points. Conduct periodic audits to assess and enhance forensic capabilities. a Ten-Step Process for Forensic Readiness; Kasassbeh & Alshar'e (2022).

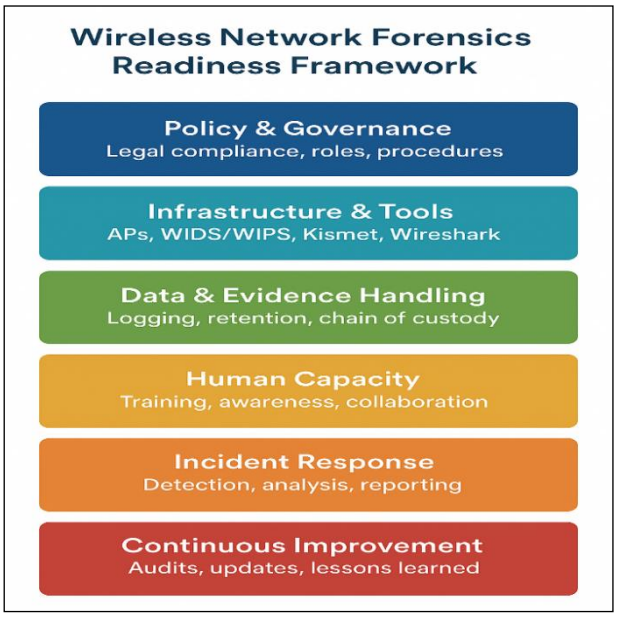

Fig 1: Shows the Wiresless Network Forensics Readiness Framework

ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/26apr1196

II. APPLICATION TO BUSITEMA UNIVERSITY

In Busitema University, implementing this framework means: Developing a forensic readiness policy under the Directorate of ICT Services (DICTS). Integrating open-source forensic tools (Kismet, Aircrack-ng, Wireshark) within laboratory environments. Training ICT and Computer Forensics students on wireless capture and analysis. Setting up centralized logging for Eduroam authentication and AP events. Establishing a chain-of-custody procedure for evidence management.

III. THEORETICAL REVIEW

The theoretical review highlights the foundational concepts and frameworks that guide wireless network forensics. It is grounded in established digital forensics process models such as those by NIST (SP 800-86) and ISO/IEC 27037/27042, which emphasize the systematic handling of digital evidence identification, preservation, collection, analysis, and reporting. In wireless environments, these theories are extended to address the volatile and distributed nature of wireless data, where evidence comes from transient 802.11 frames, authentication logs, and multiple network devices. Core forensic theories focus on correlation of heterogeneous data sources, time synchronization, and chain-of-custody integrity, which are essential for reconstructing wireless incidents. The review also integrates attribution theory and the cyber kill chain model, explaining how investigators trace intrusions or rogue access points through observed network behaviours.

Theoretically, wireless forensics relies on layered evidence collection from the radio and data link layers (capturing frames and signal traces) to the network/application layers (logs and flows). Tools like Wireshark, Kismet, Air cracking, and Zeek operationalize these principles, though no single tool satisfies all forensic requirements. Therefore, tool validation and standardized procedures remain critical.

Applied to Busitema University, the theoretical framework suggests that institutional readiness depends on aligning its existing ICT infrastructure and academic resources (e.g., computer forensics programs) with these forensic models. However, theoretical gaps exist where formal forensic policies, centralized logging, and validated wireless-capture practices are not yet evident.

In essence, the theoretical review provides the conceptual foundation for evaluating and enhancing Busitema University's readiness by linking digital forensic standards, wireless-specific evidence theory, and institutional practice into one coherent framework.

IV. CONCEPTUAL FRAMEWORK

Demonstrates that Busitema University's wireless forensic readiness is a function of theoretical adherence, technological capability, and institutional support. The effective integration of these dimensions leads to improved capacity to secure wireless networks, preserve digital evidence, and sustain academic and operational resilience against cyber threats.

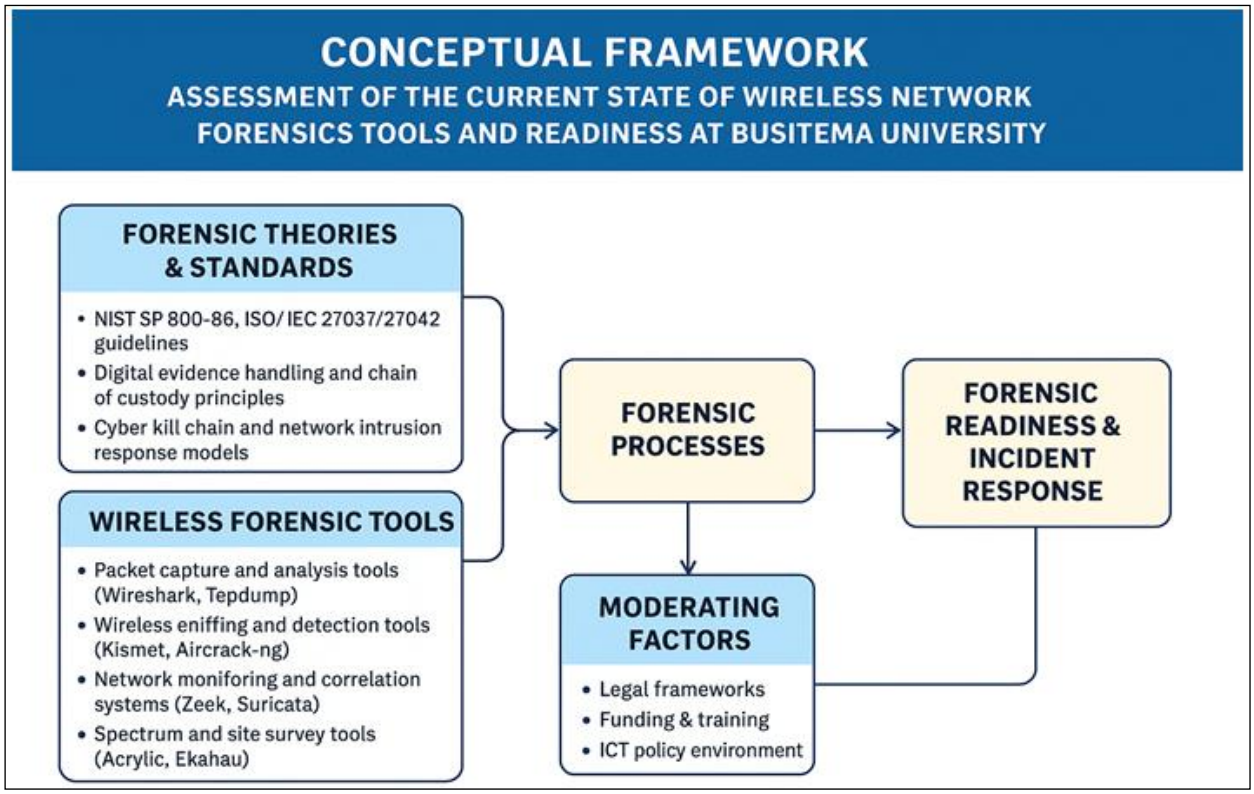

Fig 2: Above Shows the Conceptual Framework of the Current State of Wireless Network Forensics Tools and Readiness at Busitema University

ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/26apr1196

V. CONCLUSIONS

The assessment of Busitema University's wireless network forensics tools and readiness indicates that the institution possesses a solid academic and infrastructural foundation, but practical forensic readiness remains in an early developmental stage. The university has integrated cybersecurity and digital forensics programs within its academic structure, producing skilled personnel capable of conducting forensic investigations. Additionally, the Directorate of ICT (DICTS) maintains a functional wireless network infrastructure (notably through Eduroam), which provides a baseline for authentication and network activity logging key components for forensic evidence collection. However, the readiness of the tools framework is limited by the absence of a formal forensic policy, dedicated forensic hardware, and comprehensive logging or monitoring systems for wireless activities. Most of the tools currently available such as Wireshark, Air crack-ng, and Kismet are open-source and suitable for teaching and basic research but lack enterprise level capabilities for large scale or legally admissible investigations. The inadequate deployment of wireless intrusion detection/prevention systems (WIDS/WIPS) and absence of a documented chain of custody procedure further limit full forensic preparedness. Busitema University is moderately ready for wireless network forensics in terms of knowledge capacity and technical awareness, but operational readiness remains partial due to gaps in infrastructure, policies, and specialized forensic tools. Strengthening this readiness requires implementing a formal forensic readiness framework, expanding the toolset to include both open source and commercial solutions, developing standard evidence handling procedure, and fostering collaboration between DICTS and academic researchers to operationalize forensic investigations within the campus network.

REFERENCES

[1]. Bedi, P., Kumar, R., & Sharma, A. (2023). *Advances in wireless network forensics and security analytics*. *Journal of Network and Computer Applications*, 212, 103567.

[2]. Kumar, S., & Singh, R. (2023). *Wireless forensics frameworks for intrusion detection in academic networks*. *IEEE Access*, 11, 86532–86547.

[3]. Mirembe, R., Katumba, A., & Namusoke, J. (2023). *Cybersecurity readiness in Ugandan universities: Gaps and opportunities*. *African Journal of Information Systems*, 15(2), 1–15.

[4]. Ndiwalana, A., & Kituyi, G. M. (2022). *Challenges of implementing network security in higher education institutions in developing countries*. *International Journal of Information Security Research*, 12(4), 230–241.

[5]. Al-Kasassbeh, M., & Alshar'e, M. (2022). *Wireless Network Forensics: Frameworks, Tools, and Readiness Assessment Models. Journal of Digital Forensics, Security and Law*, 17(3), 45–58.

[6]. Baryamureeba, V., & Tushabe, F. (2004). *The Enhanced Digital Investigation Process Model. Proceedings of the Digital Forensics Research Workshop (DFRWS)*.

[7]. Casey, E. (2020). *Digital Evidence and Computer Crime: Forensic Science, Computers, and the Internet.* Academic Press.

[8]. Kent, K., Chevalier, S., Grance, T., & Dang, H. (2006). *Guide to Integrating Forensic Techniques into Incident Response (NIST SP 800-86).*

[9]. NIST (2021). *Guide to Intrusion Detection and Prevention Systems (SP 800-94).*

[10]. NIST (2022). *Computer Security Incident Handling Guide (SP 800-61 Rev.2).*

[11]. Palmer, G. (2001). *A Road Map for Digital Forensics Research.* Technical Report DTR-T001-01.

[12]. Rowlingson, R. (2004). *A Ten-Step Process for Forensic Readiness. International Journal of Digital Evidence*, 2(3), 1–28.

[13]. Busitema University (2023). *Master of Science in Computer Forensics Curriculum Outline.*

[14]. Wireshark Foundation. (2024). *Wireshark Documentation.* https://www.wireshark.org

[15]. Kismet Wireless. (2024). *Kismet Documentation.* https://www.kismetwireless.net

[16]. R. Ahmed and R. V. Dharaskar, "Mobile forensics: An introduction from indian law enforcement perspective," in Proc. Third International Conference on Information Systems, Technology and Management (ICISTM 2009), 2009, pp. 173–184.

[17]. K. Restino. (2012, Jun.) Android expected to reach its peak this year as mobile phone shipments slow, according to idc. [Online]. Available: ttp://www.idc.com/getdoc.jsp?containerId=prUS23523812