Análisis comparativo de herramientas digitales forenses con IA en el marco de los delitos informáticos en Ecuador

Dario Javier Catagua Zambrano
Universidad Técnica de Manabí
dcatagua4977@utm.edu.ec
Portoviejo, Ecuador.

Denise Soraya Vera Navarrete
Universidad Técnica de Manabí
denise.vera@utm.edu.ec
Portoviejo, Ecuador.

DOI: https://doi.org/10.56124/encriptar.v9i17.007

Resumen

Este artículo describe cómo Ecuador se posiciona como el tercer país latinoamericano con mayor incidencia de ciberdelincuencia, un problema exacerbado por la rápida transformación digital y un marco legal obsoleto. Además, este estudio realiza un análisis comparativo del rendimiento de herramientas forenses digitales potenciadas con inteligencia artificial (IA)—Autopsy, Magnet AXIOM y Belkasoft Evidence X—con el objetivo de identificar soluciones para fortalecer las investigaciones digitales en el país. La metodología adoptada fue mixta, combinando el procesamiento técnico de una imagen forense estandarizada (ntfs1-gen1.E01) con una encuesta dirigida a expertos, académicos y profesionales del sector. Los resultados técnicos mostraron que Magnet AXIOM, gracias a su IA nativa integrada, procesó la evidencia en 50 segundos, demostrando excelencia en velocidad y automatización. Belkasoft Evidence X sobresalió en la recuperación de evidencia, identificando 74 elementos multimedia mediante sus filtros semánticos visuales e interfaz intuitiva. Autopsy, aunque notablemente más lento y dependiente de la instalación manual de plugins externos para emular funcionalidades de IA, se confirmó como una opción viable para instituciones con limitaciones presupuestarias. La encuesta reveló una brecha formativa crítica: el 75% de los profesionales utiliza estas herramientas solo "ocasionalmente", lo que destaca una desconexión entre el potencial tecnológico y la práctica común. Se concluye que la implementación de estas tecnologías debe ir acompañada de programas masivos de capacitación especializada y una actualización integral del marco legal ecuatoriano, el cual debe tipificar los delitos digitales modernos y establecer protocolos para validar legalmente las evidencias obtenidas mediante IA.

Palabras clave: forensia digital, inteligencia artificial, ciberdelincuencia, herramientas digitales, investigación digital.

Comparative analysis of AI-powered digital forensics tools in the context of cybercrime in Ecuador.

ABSTRACT

This article describes how Ecuador ranks as the third Latin American country with the highest incidence of cybercrime, a problem exacerbated by rapid digital transformation and an outdated legal framework. Furthermore, this study conducts a comparative analysis of the performance of digital forensic tools enhanced with artificial intelligence (AI)—Autopsy, Magnet AXIOM, and Belkasoft Evidence X—aiming to identify solutions to strengthen digital investigations in the country. The methodology adopted was mixed, combining the technical processing of a standardized forensic image (ntfs1-gen1.E01) with a survey targeting experts, academics, and industry professionals. The technical results showed that Magnet AXIOM, thanks to its integrated native AI, processed the evidence in 50 seconds, demonstrating excellence in speed and automation. Belkasoft Evidence X excelled in evidence recovery, identifying 74 multimedia items through its visual semantic filters and intuitive interface. Autopsy, although noticeably slower and reliant on the manual installation of external plugins to emulate AI functionalities, was confirmed as a viable option for institutions with budget constraints. The survey revealed a critical training gap: 75% of professionals use these tools only "sometimes," highlighting a disconnect between technological potential and common practice. It is concluded that the implementation of these technologies must be accompanied by massive specialized training programs and a comprehensive update of the Ecuadorian legal framework, which should criminalize modern digital crimes and establish protocols to legally validate evidence obtained through AI.

Keywords: digital forensics, artificial intelligence, cybercrime, digital tools, digital investigation.

1. Introduction

The situation of cybercrime in Ecuador is experiencing alarming growth, positioning the country as the third with the highest incidence in Latin America, only behind Mexico and Bolivia (Saltos Salgado et al., 2021), (Del Pozo Carrasco et al., 2024). This phenomenon, aggravated by the accelerated digital transformation during the pandemic, is predominantly evidenced in electronic fraud, ransomware, phishing, and identity theft, critically affecting the financial sector and government institutions. Consequently, Ecuador ranks 119th out of 182 countries in terms of vulnerabilities to

cyberattacks (Ponce Tubay, 2024), (Hernández Alvarado et al., 2024). Faced with this reality, the investigative and judicial response is hampered by a legal framework that experts describe as obsolete and fragmented. The Organic Comprehensive Penal Code (COIP) exhibits problems similar to those identified in other countries in the region, such as in Colombia, where low effectiveness in the application of its specialized law against cybercrime has been reported (Rincón, J., Quijano, et al., 2022). In the Ecuadorian context, this translates into a lack of a specific section in the COIP for these offenses, and sanctions that may not be proportionate to the damage caused.

The inability of traditional digital forensic methods to process the volume, speed, and heterogeneity of digital data generated in these incidents aggravates the problem. Investigations become slow, prone to human error, and frequently inadequate for examining evidence from diverse sources like the cloud, IoT devices, and social networks (Jarrett & Choo, 2021), (Dunsin et al., 2024). This technological gap between criminals and investigators highlights the urgent need to adopt advanced solutions based on Artificial Intelligence (AI) and Machine Learning (ML) to automate tasks, correlate massive evidence, and detect complex patterns that conventional human analysis misses (Adam & Varol, 2020).

The integration of AI into digital forensics through methods ranging from Deep Learning (DL) for malware identification (Qureshi et al., 2024) and image forgery detection to ontological engineering for automated reasoning, promises to revolutionize the field. Tools compared in practical studies, such as Magnet AXIOM, Autopsy, and Belkasoft Evidence, demonstrate significant advances in evidence recovery and analysis (Sunardi et al., 2022). However, this automation introduces critical challenges of transparency and trust. "Black box" models make it difficult to interpret decisions, compromising the admissibility of digital evidence in court and the fundamental right to a fair legal process (Khalid et al., 2024), (Stoykova, 2024).

This latter aspect highlights an essential tension: the need for investigative efficiency versus the obligation to guarantee procedural rights. Emerging concepts such as the "right to procedural accuracy" and Explainable AI (XAI) frameworks seek to balance this equation, proposing governance that ensures digital evidence generated or processed by

AI is auditable, understandable, and contestable by the defense. This need for transparency is crucial even in contexts of international cooperation and cloud search orders, where AI-assisted protocols, like the CDRP, aim to resolve forensic disputes between providers and clients without direct human intervention (Alashjaee, 2024).

In the Ecuadorian context, this problem intensifies. Research reveals a lack of specific regulations for the use of digital forensics even in government audits (Caraguay Ramírez, 2020), insufficient training of judicial operators, and a critical disconnect between academia and forensic professionals in practice (Hargreaves et al., 2024). The disparity in the legal classification of cybercrimes, a problem also observed in Mexico (Alcalá Casillas, M. G., & Melendez Ehrenzweig, M. Á., 2023), and the need for a unified federal law, contrast with the sophistication of cybercriminals, whose criminological profile is characterized by a lack of empathy, high technical capacity, and adaptability (Díaz Samper et al., 2024).

Therefore, this research is proposed as a response to this urgent need. The general objective of this work is to compare and analyze the technical performance and suitability within the Ecuadorian legal framework of a selected set of AI-powered digital forensic tools. The central contribution of this article lies in generating a contextualized comparative analysis for Ecuador's reality, integrating technical, legal, and ethical dimensions. As a concrete product, it seeks to propose an evaluation framework or protocol that allows judicial and police institutions to select and implement these tools in an informed manner, ensuring their use is both effective and respectful of fundamental rights.

This research is based on the analysis of several fundamental studies published between 2020 and 2025, covering topics from technical proposals for automation and big data analysis to in-depth legal (du Toit, 2022), (Álvarez-Valenzuela & Hevia Angulo, 2020), criminological, and situational crime prevention strategy analyses. This work aims to comparatively examine AI-based digital forensic analysis tools, focusing on their application in the Ecuadorian context, considering technical and legal aspects. By evaluating Autopsy, Magnet AXIOM, and Belkasoft Evidence X, it seeks to identify their

strengths and weaknesses and propose ways to strengthen the regulatory and technical framework in Ecuador, thereby contributing to a more robust cybersecurity system tailored to the country's needs.

2. Methodology

The purpose of this research is to evaluate the performance of digital forensic tools that integrate artificial intelligence and data analysis for the detection, tracking, and analysis of cybercrimes within the Ecuadorian context. The tools selected for this study are Autopsy, Magnet AXIOM, and Belkasoft Evidence X. The primary objective is to determine their effectiveness in identifying, recovering, and presenting digital evidence in real cases, ensuring the results are admissible in judicial proceedings, in accordance with current Ecuadorian regulations.

The methodological approach is based on an experimental design that includes the simulation of representative cybercrime scenarios, such as phishing attacks, malware, and unauthorized access. These scenarios were carried out in controlled environments with replicable datasets to evaluate the tools' performance. The evaluation criteria encompass data recovery capability, processing efficiency, usability for forensic experts, and compatibility with the Ecuadorian regulatory framework, ensuring that the procedures and results meet legal requirements for application in judicial processes.

Furthermore, questions were created using a Google Forms questionnaire, which helped identify many aspects of the research during the use and testing of forensic tools in the field of computer forensics.

2.1. Tool Access and Licensing

One of the main methodological challenges was acquiring licenses for the forensic tools with advanced AI capabilities, specifically Magnet AXIOM and Belkasoft Evidence X, due to their commercial nature and high cost. To overcome this barrier, the developers and official distributors of both tools were formally contacted via email to request temporary evaluation licenses for academic and research purposes. After a review and

verification process of the request, demo licenses valid for 30 days were obtained for each tool, allowing the controlled tests to be conducted within a limited timeframe. This process required rigorous planning of the experimental activities to maximize the use of the license period.

2.2. Information Collection Techniques

Data collection included a comprehensive review of technical manuals, user guides, and case studies on the use of Autopsy, Magnet AXIOM, and Belkasoft Evidence X in forensic analysis. Reliable sources were consulted, such as specialized cybersecurity forums, the official websites of the tools, and reports from forensic laboratories. Additionally, data from real cybercrime cases in Ecuador were collected, using public reports from the State Attorney General's Office and other verified sources. This approach allowed for contrasting theoretical information with the practical needs of experts in the local context.

2.3. Tools and Services

For the execution of this research, Autopsy, Magnet AXIOM, and Belkasoft Evidence X were used as the primary tools. To conduct tests for each one and compare them, a table is presented below detailing the specifics of each tool.

Table 1. Tool and Service Characteristics

Characteristic	Autopsy	Magnet AXIOM	Belkasoft Evidence X
License	Open Source	Proprietary	Proprietary
AI Integration	Requires external plugins	Advanced native integration	AI functions for classification
Compatibility	Multiple OS (Windows, Linux, macOS)	Windows	Multiple SO

Interface	Less intuitive	Intuitive and robust	Easy to use

Note: Data obtained through experimental testing conducted by the autor Catagua, D. (2025).

Subsequently, each tool was detailed. A forensic image containing some anomalous files was used to identify them.

The forensic tool **Autopsy** is an open-source platform for digital forensic analysis, with artificial intelligence modules that automate the detection of suspicious files and anomalous patterns. **Magnet AXIOM** is a comprehensive tool for digital forensic analysis that combines the acquisition and analysis of data from mobile devices, computers, and the cloud, with advanced artificial intelligence capabilities to efficiently identify and correlate digital evidence. On the other hand, **Belkasoft Evidence X** is forensic software specialized in the acquisition, analysis, and review of digital evidence, with support for multiple data types—including images, videos, messages, and documents—optimized for complex investigations with a focus on usability and generating clear reports.

Test environments were designed to replicate phishing, malware, and unauthorized access scenarios, evaluating the capability of each tool to detect and analyze digital evidence.

2.4. Surveyed Experts and Academics

A survey was conducted among 20 professionals, including cybersecurity experts and university professors, selected for their experience and knowledge in digital forensics and cybersecurity. The inclusion criteria considered were:

- Experience in computer forensics or university teaching in areas related to cybersecurity.
- Participation in investigations or expert reports related to cybercrime in Ecuador.

The respondent group consisted of professors from the Technical University of Manabí, with profiles such as systems engineers, IT auditors, IT managers, IT engineers, and masters in data science, as well as experts from the National Police and criminalistics units. This composition aimed to create a comprehensive overview integrating technical, legal, and educational perspectives.

It should be noted that while the involvement of academics benefits the analysis from a formative and theoretical focus, the sample shows a significant density in this area. Therefore, the findings derived from the survey should be interpreted considering that the perspective of professionals working exclusively in digital forensics within the public or private sector might be underrepresented.

Participation in the survey, conducted via a Google Form, was optional and collaborative, allowing for the collection of valuable information about the level of confidence and usage of forensic tools among the consulted professionals.

2.5. Configuration and Initial Testing

Data from simulated and real cases such as phishing emails, logs, compromised files, and incident reports was collected. This data was processed and normalized during analysis using tools that integrate artificial intelligence to identify any anomaly attacks and vulnerabilities.

Tools including Autopsy, Magnet AXIOM, and Belkasoft Evidence X were installed and configured to proceed with forensic protocols and ensure evidence integrity. This process included: creating forensic images, hashing to verify data, timeline analysis, and automated correlation of indicators of compromise.

In the tool comparison, results showed that AXIOM was consistently faster in processing traditional storage; Belkasoft demonstrated clear advantages in memory analysis, while Autopsy proved viable for limited budgets.

Finally, reports containing findings were prepared in compliance with forensic standards for presentation in judicial proceedings. These included complete chain of custody documentation, technically accurate explanations adapted to legal language, annexes with certified digital evidence (hashes, metadata), and conclusions regarding the identified attack origin.

2.6. Data Processing and Analysis

The forensic analysis was conducted through controlled tests using Magnet AXIOM, Autopsy, and Belkasoft Evidence X tools. The data was obtained from the following website: https://digitalcorpora.s3.amazonaws.com/s3_browser.html#corpora/drives/nps-2009-ntfs1/, (DigitalCorpora), where a forensic image in .E01 format (492 MB, NTFS file system) was used. The executed technical procedures can therefore be described, supported by key visual evidence:

Table 2. Configuration and Processing Results of the Forensic Image

Parameter	Magnet AXIOM	Autopsy	Belkasoft Evidence X
Case Configuration	Unique identifier: Case-01. Activation of all native AI modules (image classification, content detection, chat analysis).	Standard image load. Required manual search and installation of the deepfake_photo plugin for basic AI capabilities.	Automated case setup. Activation of preconfigured visual semantic filters (nudity, weapons, faces detection).
Processing and Analysis	Automated analysis with hashing (MD5/SHA-1) for integrity verification. Execution of keyword searches (e.g., "confidential", "hacking"). Use of timeline for event correlation.	Sequential modular processing. Metadata analysis and file recovery using the PhotoRec tool, requiring manual intervention for classification.	Automated sequential process. Comprehensive artifact analysis with a focus on efficient recovery and visual filtering.
Execution Time	50 seconds (Fastest)	2 minutes 10 seconds.	2 minutes 42 seconds.

Recovered Evidence	46 images automatically classified by content and case relevance.	Basic file recovery. Classification depended on correct user configuration.	74 graphic items and 6 documents identified, with a clear visual presentation.
User Intervention	Minimal. Guided and automated workflow.	High. Less intuitive tree navigation and need for manual plugin configuration.	**Moderate.** Interactive dashboard that facilitates results exploration.

Note: Data obtained through experimental testing conducted by the autor Catagua, D. (2025).

2.7. Detailed Description by Tool:

- **Magnet AXIOM:**
  - A new case was configured with the identifier Caso-01.
  - The forensic image ntfs1-gen1.E01 was loaded.
  - All integrated AI functionalities for automatic image and chat classification, as well as specific content detection, were activated.
  - A search was executed using key terms related to the simulated case ("confidential", "hacking").
  - The tool automatically calculated hashes (MD5/SHA-1) to ensure data integrity throughout the process.
  - The total analysis time was 50 seconds, making it the fastest tool.
  - 46 images of evidentiary interest were automatically recovered and classified.

- **Autopsy:**
  - The process began with the standard loading of the forensic image.

- To emulate AI functionalities, it was necessary to manually search for, download, and install the external deepfake_photo plugin.
- The interface, based on a navigation tree, proved less intuitive and required greater manual intervention from the investigator.
- File recovery was supported by the PhotoRec tool, but the classification of evidence depended almost entirely on the user's judgment and effort.
- The processing time was 2 minutes and 10 seconds.

- **Belkasoft Evidence X:**
  - The case configuration was automated and straightforward.
  - Preconfigured visual semantic filters were utilized to detect categories of sensitive content such as nudity, weapons, and faces.
  - The analysis was sequential and comprehensive, examining a wide range of digital artifacts.
  - The tool presented the results in a visual and interactive dashboard, facilitating data exploration.
  - The processing time was 2 minutes and 42 seconds.
  - A total of 74 graphic items and 6 documents relevant to the investigation were identified.

2.8. Study Limitations:

The research faced several limitations inherent to the dynamic nature of digital forensics and the framework in which it was developed:

- Variability in Real-World Scenarios: The simulated cases did not replicate the full spectrum of advanced attacks documented in the literature or reported in recent incidents.
- Tool Updates: The versions used may not include the most modern artificial intelligence functionalities designed to counter evolving threats.
- Access to Sensitive Data: Legal and ethical restrictions prevented the use of evidence from ongoing legal proceedings, leading to reliance on controlled simulations.

- Survey Sample Composition: The predominance of academics in the sample of surveyed professionals may introduce a bias in the results, as their experiences and needs may differ from those of professionals who work exclusively and operationally in digital forensics within police institutions, prosecutor's offices, or consulting firms. Future research should expand the sample to more proportionally include profiles dedicated primarily to forensic practice, in order to achieve a more representative overview of the sector in Ecuador.

These limitations are documented to guide and enrich future research, ideally in collaboration with public authorities that can facilitate access to realistic data and a broader range of active professionals.

2.9. Ethical Considerations:

This study ensured the privacy of the obtained data and removed personal information from the real datasets. Survey participants consented to their responses being used for scientific purposes. Furthermore, the protocols of the Organic Law on Personal Data Protection (Ecuador) were respected, and practices that could compromise external systems or networks during testing were avoided.

3. Results:

The evaluation of Magnet AXIOM, Autopsy, and Belkasoft Evidence X was conducted through controlled tests using a standardized forensic image in E01 format (492 MB, NTFS system).

The results are analyzed across two dimensions:

- ✓ The quantifiable technical performance of each tool.
- ✓ The preliminary findings from an exploratory survey on the perception and usage of these technologies in the local context.

3.1. Comparative Analysis of Technical Performance:

Table 2 (presented in section 3.6) shows the detailed results of the forensic image processing, highlighting significant differences in speed, automation, and effectiveness. The key technical findings are described below:

3.2. Key Technical Findings:

- ✓ Speed and Automation: Magnet AXIOM demonstrated overwhelming superiority in speed, processing the evidence in 50 seconds. Its integrated native AI enabled a nearly fully automated workflow, minimizing investigator intervention.
- ✓ Recovery Effectiveness: Belkasoft Evidence X excelled in evidence recovery capability, identifying 74 multimedia items. Its powerful visual semantic filters and intuitive interface facilitated the location and presentation of findings.
- ✓ Viability for Limited Budgets: Autopsy confirmed its robustness as an open-source tool. However, its reliance on manual plugin installation to emulate AI functionalities and its less intuitive interface resulted in a significantly slower process demanding greater technical expertise.

To visualize the significant difference in tool efficiency, **Figure 1** compares the processing times.

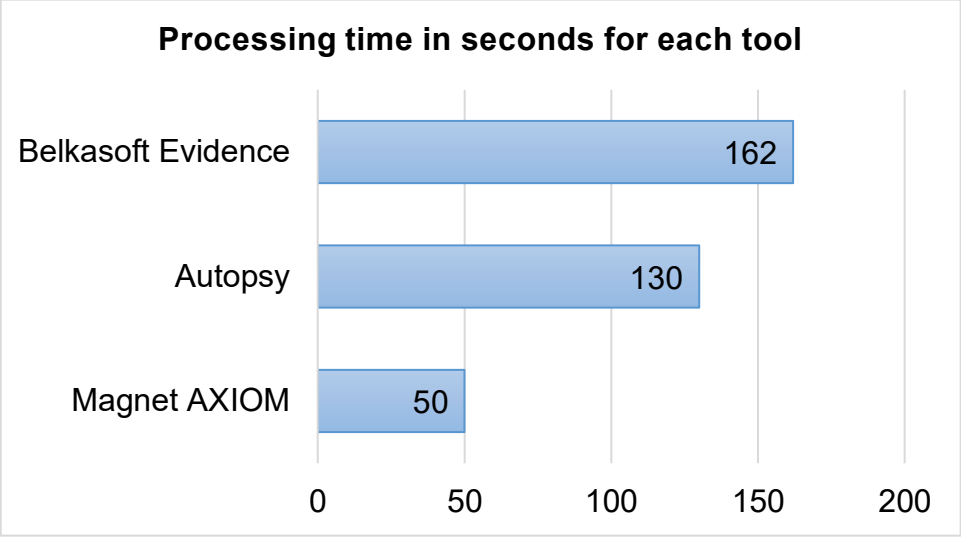

Figure 1. Comparison of the forensic image processing time (in seconds)

3.3. Findings from an Exploratory Survey of Professionals:

In a complementary manner, a preliminary survey was conducted with 20 sector professionals (experts, academics, and IT professionals) aiming to gain an initial understanding of their familiarity with this type of tool. It is important to note that, due to the limited sample size, these results should be interpreted as initial trends and not as generalizations of the national situation.

The results, summarized in Table 3, reveal valuable insights into the adoption context.

Table 3. Perception and Use of Digital Forensic Tools (n=20)

Aspect	Results (%)
Prior Knowledge	35% were unfamiliar with them
Perceived Usefulness	63% consider them "very useful"
Selection Priority	72% value “accuracy” over “legality”
Frequency of use	75% use them “sometimes”

Note: Data obtained through experimental testing conducted by the author Catagua, D. (2025).

These findings point to a potential disconnect between the technological potential and the common practice within the surveyed professional circle. The low frequency of use (75%) contrasts with the high perceived usefulness (63%), which could be related to factors such as access to licenses, availability of specialized training, or institutional routines.

Figure 2. It illustrates the perceptions and usage habits identified through the survey.

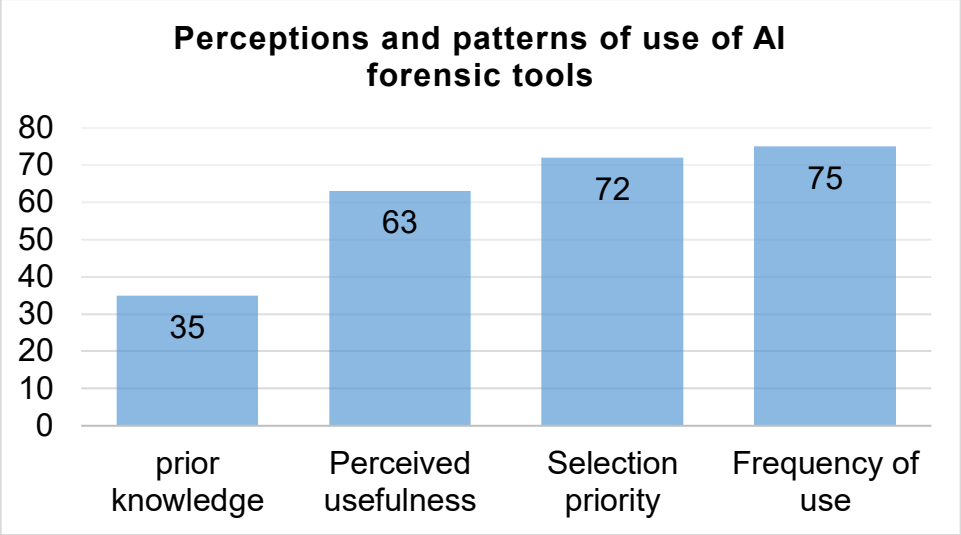

Figure 2. Perceptions and patterns of use of AI forensic tools.

3.4. Correlation Between Technical Evidence and Professional Perception:

Although the survey data is preliminary, a coherence with the technical results is observed:

AI as a Key Differentiator: The high performance of Magnet AXIOM and Belkasoft Evidence X, driven by integrated AI, aligns with the perception of 63% of professionals who consider AI "very useful" for forensic processes.

Accuracy Over Usability: Although users value intuitive interfaces (Figure 2), the primary selection criterion is accuracy (72%), reinforcing the importance of the technical robustness demonstrated by the commercial tools.

The Niche of Open-Source Tools: The relevance of Autopsy in academic or budget-constrained environments is contextualized by the low reported frequency of use, suggesting that cost barriers may influence the adoption of more advanced tools.

4. Conclusions:

In conclusion, not all the analyzed forensic tools offer the same performance. Magnet AXIOM stood out for its speed and accuracy, making it ideal for urgent cases, while Belkasoft Evidence X demonstrated greater effectiveness in analyzing photos and

videos. For its part, Autopsy, although notably slower, presents itself as an accessible option for teams with limited resources.

Furthermore, the study revealed a critical problem: many of the surveyed professionals were unfamiliar with or did not use these tools, reflecting an urgent need for training in the digital forensics field. While artificial intelligence emerges as a promising solution, its effective implementation first requires professionals to acquire the necessary competencies to employ it adequately.

On the other hand, it is essential for laws to stay updated with technological advancements. In the case of Ecuador, it is imperative to modernize the legal framework, particularly the COIP, to address digital crimes such as ransomware and phishing. Without clear and adapted legislation, cybercriminals will maintain operational advantages.

Finally, it is recommended to train more experts in forensic tools and AI, foster alliances between universities, governments, and businesses to strengthen security, and additionally, update regulations using countries with greater experience, such as Mexico, as a reference.

Bibliographic References:

Adam, I. Y., & Varol, C. (2020). **Intelligence in Digital Forensics Process.** 2020 8th International Symposium on Digital Forensics and Security (ISDFS), 1–6. https://doi.org/10.1109/ISDFS49300.2020.9116442

Alashjaee, A. M. (2024). **Toward a Conflict Resolution Protocol for Cloud Forensics Investigation.** *IEEE Access, 12,* 72013–72022. https://doi.org/10.1109/ACCESS.2024.3402623

Álvarez-Valenzuela, D., & Hevia Angulo, A. (2020). **Protección legal para la búsqueda y notificación de vulnerabilidades de ciberseguridad en Chile.** *Revista Chilena de Derecho y Tecnología, 9(2),* 1. https://doi.org/10.5354/0719-2584.2020.60658

Rincón, J., Quijano, A., Castiblanco, S., Urquijo, J., & Pregonero, Y. (2022). **Ciberdelincuencia en Colombia: ¿qué tan eficiente ha sido la Ley de Delitos Informáticos?** *Revista Criminalidad, 64(3),* 95-116. https://doi.org/10.47741/17943108.368

Caraguay Ramírez, S. X. (2020). **Aplicación de informática forense en auditorías gubernamentales para la determinación de indicios de responsabilidad penal con delitos informáticos en**

Ecuador, México y Perú, 2007-2019. *Estado & comunes, 2(11),* 135–153. https://doi.org/10.37228/estado_comunes.v2.n11.2020.178

Del Pozo Carrasco, J. G., Lumbi Salazar, S. J., y Paucar Paucar, C. E. (2024). **Programa de prevención de ciberdelitos en instituciones educativas de Ecuador.** *Revista Conrado, 20(96),* 675-686. http://scielo.sld.cu/scielo.php?script=sci_arttext&pid=S1990-86442024000100675&lang=pt

Díaz Samper, G. A. J., Molina Garzón, A. L., & Serrador Osorio, L. E. (2024). **Aproximación al ciberdelincuente desde la perspectiva del control social.** *Revista Criminalidad, 65(3),* 81–95. https://doi.org/10.47741/17943108.508

du Toit, P. (2022). **The search warrant provisions of the cybercrimes act and their relationship with the criminal procedure act.** *Obiter, 43(4),* 764–778. http://www.scielo.org.za/scielo.php?script=sci_abstract&pid=S1682-58532022000400007&lng=en&nrm=iso&tlng=en

Dunsin, D., Ghanem, M. C., Ouazzane, K., & Vassilev, V. (2024). **A comprehensive analysis of the role of artificial intelligence and machine learning in modern digital forensics and incident response.** *Forensic Science International: Digital Investigation, 48,* 301675. https://doi.org/10.1016/j.fsidi.2023.301675

Hargreaves, C., Breitinger, F., Dowthwaite, L., Webb, H., & Scanlon, M. (2024). **DFPulse: The 2024 digital forensic practitioner survey.** *Forensic Science International: Digital Investigation, 51,* 301844. https://doi.org/10.1016/j.fsidi.2024.301844

Hernández Alvarado, V. J., Granja Huacón, S. H. & Arias Hernández, J. L. (2024). **Efectividad de las políticas implementadas para garantizar la seguridad cibernética en Ecuador.** *Universidad y Sociedad 16(5),* 288-296 http://scielo.sld.cu/scielo.php?script=sci_arttext&pid=S2218-36202024000500288&lang=pt

Jarrett, A., & Choo, K. R. (2021). **The impact of automation and artificial intelligence on digital forensics.** *WIREs Forensic Science, 3(6),* e1418. https://doi.org/10.1002/wfs2.1418

Khalid, Z., Iqbal, F., & Fung, B. C. M. (2024). **Towards a unified XAI-based framework for digital forensic investigations.** *Forensic Science International: Digital Investigation, 50,* 301806. https://doi.org/10.1016/j.fsidi.2024.301806

Ponce Tubay, M. A. (2024). **Desafíos y respuestas legales ante los delitos informáticos en Ecuador.** *Revista San Gregorio, 1(58),* 111–118. https://doi.org/10.36097/rsan.v1i58.2667

Qureshi, S. U., He, J., Tunio, S., Zhu, N., Nazir, A., Wajahat, A., Ullah, F., & Wadud, A. (2024). **Systematic review of deep learning solutions for malware detection and forensic analysis in IoT.** *Journal of King Saud University - Computer and Information Sciences, 36(8),* 102164. https://doi.org/10.1016/j.jksuci.2024.102164

Saltos Salgado, M. F., Robalino Villafuerte, J. L., & Pazmiño Salazar, L. D. (2021). **Análisis conceptual del delito informático en Ecuador.** *Revista Conrado, 17(78),* 343-351.

http://scielo.sld.cu/scielo.php?script=sci_abstract&pid=S1990-86442021000100343&lng=es&nrm=iso&tlng=es

Stoykova, R. (Adi). (2024). **A New Right to Procedural Accuracy: A Governance Model for Digital Evidence in Criminal Proceedings.** *Computer Law & Security Review, 55,* 106040. https://doi.org/10.1016/j.clsr.2024.106040

Sunardi, Herman, & Ardiningtias, S. R. (2022). **A Comparative Analysis of Digital Forensic Investigation Tools on Facebook Messenger Applications.** *Journal of Cyber Security and Mobility,* 655–672. https://doi.org/10.13052/jcsm2245-1439.1151

Alcalá Casillas, M. G., & Melendez Ehrenzweig, M. Á. (2023). **Computer crimes in Mexico. Recognition in the criminal laws of the Mexican entities.** *Paakat: Revista de Tecnología y Sociedad,* 1–36. https://doi.org/10.32870/Pk.a13n24.759