INSLA E-PROCEEDINGS
مقالات المؤتمر العالمي في الشريعة والقانون
E-ISSN: 2735-1742

Vol. 8, No. 1, pp. 1-6 | 2025
INSLA E-Proceedings

MODERNISING SYARIAH CRIMINAL JUSTICE: THE IMPERATIVE OF DIGITAL FORENSIC SCIENCE AND EVIDENTIARY REFORM IN MALAYSIA

[i,*]Mohamad Aniq Aiman Alias, [i]Wan Abdul Fattah Wan Ismail, [i]Ahmad Syukran Baharuddin,
[ii]Tuan Muhammad Faris Hamzi Tuan Ibrahim, [i]Hasnizam Hashim & [i]Baidar Mohammed Mohammed Hassan

[i]Faculty of Syariah and Law, Universiti Sains Islam Malaysia, Bandar Baru Nilai, 71800 Nilai, Negeri Sembilan, Malaysia
[ii]Islamic Civilization Academy, Faculty of Social Science and Humanities, Universiti Teknologi Malaysia (UTM), 81310, Johor Bahru, Johor, Malaysia

*(Corresponding author) e-mail: aniqalias@usim.edu.my

Article history:
Submission date: 1 September 2025
Received in revised form: 5 October 2025
Acceptance date: 1 November 2025
Available online: 31 December 2025

Keywords:
Digital forensic, forensic science, Syariah criminal law, Islamic law of evidence

Funding:
This research did not receive any specific grant from funding agencies in the public, commercial, or non-profit sectors.

Competing interest:
The author(s) have declared that no competing interests exist.

Cite as:
Alias, M. A. A., Wan Ismail, W. A. F., Baharuddin, A. S., Tuan Ibrahim, T. M. F. H., Hashim, H., & Hassan, B. M. M. (2025). Modernising Syariah criminal justice: The imperative of digital forensic science and evidentiary reform in Malaysia. *INSLA E-Proceedings*, *8*(1), 1–6.

ABSTRACT

The rapid evolution of science and technology has fundamentally transformed the landscape of modern criminality, leading to a rise in cyber offences that challenge the traditional boundaries of the Malaysian Syariah criminal justice system. As criminal activities migrate to the digital realm, the reliance on conventional evidence is increasingly being supplemented by digital footprints. However, the integration of digital evidence faces significant hurdles, primarily due to the rigid requirements of classical evidentiary methods such as *iqrar* (confession) and *shahadah* (eyewitness testimony), which are often unattainable in anonymous virtual environments. Furthermore, the lack of standardised procedural guidelines for handling electronic data creates a legal lacuna that may jeopardize the admissibility of such evidence. This study therefore aims to evaluate the role and significance of digital forensics as a form of *qarīnah muʿāṣirah* (contemporary circumstantial evidence) within the Syariah legal framework. Adopting a qualitative research design, this study utilises document analysis to examine relevant literature and legal texts. The gathered data is then analysed and presented through a thematic approach, categorising findings into key themes. The findings indicate that digital forensics, through rigorous processes such as cryptographic hashing and the "chain of custody", provides a scientifically objective basis for proof that aligns with the Syariah principle of *yaqin* (certainty). The study highlights that the technical capabilities of modern forensic tools can effectively reconstruct digital events and establish intent (*niyyah*) in cyber-crimes. This research is significant as it provides a fundamental bridge between forensic science and Islamic jurisprudence, offering insights for policymakers to reform existing evidence laws. In sum, the recognition of digital forensics as a robust form of *qarinah* is essential to ensure that the Syariah courts remain dynamic, equitable, and responsive to the complexities of the digital age.

Introduction

The rapid advancement of science and technology has fundamentally transformed the landscape of modern society, leading to the emergence of a "borderless world" where digital interactions are ubiquitous. This technological shift, while beneficial, has concurrently given rise to sophisticated cyber offences that challenge traditional legal frameworks. In the context of the Malaysian Syariah criminal justice system, the transition from physical to digital evidence is becoming increasingly prevalent (Alias et al., 2021). According to Strom (2016), the evolution of digital crimes necessitates a corresponding evolution in evidentiary laws to ensure that the administration of justice remains relevant in the 21st century. Consequently, digital forensics has emerged as a critical scientific discipline to assist the courts in interpreting complex electronic data and reconstructing digital events that were previously beyond the reach of conventional investigation.

Despite the importance of digital evidence, its integration into Syariah courts faces significant hurdles due to the rigid nature of traditional evidentiary requirements (Wan Ismail et al., 2021). The primary issue lies in the fact that classical methods of proof, such as *iqrar* (confession) and *shahadah* (eyewitness testimony), are often unattainable in the digital realm where anonymity and physical distance prevail. Furthermore, as highlighted by Yahya and Mohd Shariff (2022), there is a lack of specific procedural guidelines and a standardized framework for the handling of electronic documents in Syariah criminal cases. This legal lacuna creates a risk of digital evidence being contested or rendered inadmissible due to concerns over its integrity and authenticity. The motivation for this study stems from the urgent need to bridge this gap by proposing digital forensics as a robust form of *qarīnah muʿāṣirah* (contemporary circumstantial evidence) that can provide high-level certainty (*yaqin*) in judicial outcomes.

The primary objective of this study is to explore the role and necessity of digital forensics within the Malaysian Syariah evidentiary framework. Specifically, this study aims to discuss the conceptual definition of digital forensics in relation to Islamic legal principles and analyse its significance in addressing the evidentiary gaps found in traditional methods. Furthermore, the study examines the technical capabilities of modern forensic tools as a support system for evidence and concludes by proposing practical recommendations and legal reforms to enhance the reliability of digital evidence in Shariah proceedings.

The Conceptual Framework of Digital Forensics

Digital forensics is fundamentally defined as a specialised branch of forensic science that encompasses the systematic process of identifying, preserving, analysing, and presenting digital evidence in a manner that ensures its integrity and admissibility within a legal framework (Pavithran, 2025). According to Casey (2011), this field transcends mere technical data recovery; it is a rigorous investigative methodology designed to reconstruct digital events and establish facts that can withstand judicial scrutiny. In the modern era, the role of digital forensics has become indispensable, as almost all criminal activities—from conventional crimes to complex cyber offences—now leave some form of digital footprint. The primary objective is to maintain a "chain of custody" that proves the evidence remains untainted from the point of seizure to its presentation in court, a concept that Ismail and Zainol Ariffin (2025) argue is the cornerstone of digital evidence admissibility. Without these stringent scientific standards, digital data would be easily dismissed due to its ephemeral and alterable nature.

In the specific context of Islamic Jurisprudence (*fiqh*), digital forensics is conceptualised as *qarīnah Muʿāṣirah*, or contemporary circumstantial evidence (Tuan Ibrahim et al., 2025a). This classification is vital because digital evidence serves as *al-alamat* (signs) or *al-amarat* (indicators) that link an invisible digital action to a verifiable reality. For instance, metadata and system logs act as digital breadcrumbs that establish the presence or intent of an individual in the virtual realm. As highlighted by Alias et al., (2025a), the integration of digital forensics into Syariah law does not contradict traditional principles but rather enhances them by providing a scientific basis for *qarinah* (circumstantial evidence) in cases where traditional witnesses (*shahadah*) or confessions (*iqrar*) are absent. By utilising advanced technological tools such as cryptographic hash functions, digital forensics ensures a level of certainty (*yaqin*) that aligns with the higher objectives of Syariah (*maqasid al-shariah*) in upholding justice and protecting the community. Thus, the conceptual framework of digital forensics serves as a bridge between classical Islamic evidentiary requirements and the technical demands of the 21st-century legal system.

The Significance of Digital Forensics in Syariah Criminal Cases

The integration of digital forensic technology into the Islamic legal system is increasingly vital, particularly in addressing the complexities of modern criminality. This significance can be examined through several key perspectives that align scientific precision with Syariah objectives. Firstly, digital forensics serves to bridge the gap in traditional evidentiary methods. In the context of cyber-crimes such as online gambling (*al-maysir*) or virtual *khalwat*, classical methods like *iqrar* (confession) and *shahadah* (testimony) are often difficult to obtain due to the absence of physical interaction or direct witnesses (Tuan Ibrahim et al., 2025b). Yahya et al., (2021) note that as criminal activities migrate to the digital realm, the reliance on scientific inference becomes essential to ensure that justice is not obstructed by the limitations of traditional human observation.

Furthermore, digital forensics offers a level of accuracy and objectivity that transcends human testimony, which may be prone to subjectivity, bias, or memory decay. The use of cryptographic hash functions, such as SHA-256, provides a mathematical guarantee of data integrity (Alias et al., 2025b). As explained by Casey et al., (2011), any modification to a digital file—even by a single bit—will result in a completely different hash value, thereby alerting the court to any potential tampering. This technical certainty provides a robust foundation for *yaqin* (certainty) in judicial decisions, which is a core requirement in Syariah court proceedings.

The application of "Locard's Exchange Principle" also plays a crucial role in this discourse (Baharuddin, 2017). This forensic principle, which posits that "every contact leaves a trace" is highly compatible with Islamic legal logic regarding *qarinah* (circumstantial evidence). In the digital world, every interaction generates residual data such as system logs, metadata, and timestamps. These digital traces allow investigators to reconstruct the sequence of events or the *niyyah* (intention) of a suspect. Al-Azhar (2012) emphasises that the systematic recovery of these traces provides a reliable means of proof that supports the truth-seeking mission of the court.

Finally, the emphasis on the "chain of custody" in digital forensics mirrors the Islamic values of *amanah* (trustworthiness) and transparency. The strict documentation required at every stage of evidence handling—from seizure to analysis—ensures that the evidence presented is authentic and has not been manipulated (Yahya et al., 2024). According to Cosic and Cosic (2012), maintaining a rigorous chain of custody is paramount to the credibility of digital forensics. From an Islamic perspective, this process fulfils the *maqasid al-shariah* (the higher objectives of Syariah) by protecting the rights of the accused while ensuring that the perpetrator is held accountable through a transparent and verifiable process.

Digital Forensic Science as Strategic Evidentiary Support

The reliability of digital evidence in court is significantly enhanced by the advanced technical capabilities of modern forensic tools. These technologies provide the necessary precision to transform raw data into admissible legal evidence. The first requirement of this capability is the use of industry-standard forensic software. Tools such as Magnet Axiom, XRY Mobile Forensics, and EnCase have become essential in modern investigations due to their ability to perform deep data extraction across diverse platforms, including smartphones, IoT devices, and cloud storage. As noted by Quick and Choo (2014), these tools are not only capable of recovering active data but are also proficient in retrieving deleted or fragmented information from unallocated clusters of a drive. This ability to "resurrect" intentionally destroyed data provides Shariah courts with a more complete factual narrative, ensuring that justice is not evaded through simple data deletion.

Furthermore, the integration of Artificial Intelligence (AI) and automation within these forensic suites has revolutionised the speed and accuracy of evidence analysis (Alias et al., 2025c). In the face of "big data" challenges, where a single device may contain terabytes of information, manual inspection is no longer feasible. AI-driven automation helps investigators detect illicit content, such as pornographic images or gambling patterns, and identify suspicious behavioural trends with far greater efficiency than human examiners. Goodison et al., (2015) emphasises that automated forensic analysis reduces human error and mitigates the risk of oversight during the examination of massive datasets. By identifying patterns of criminal conduct through algorithmic filtering, forensic tools provide a clearer link between the digital act and the perpetrator's intent (*niyyah*).

The technical robustness of these tools also ensures that the evidence produced meets the high standards of integrity required by the law. Most industry-standard tools are designed to operate on "write-blocked" environments, ensuring that the original source remains pristine. According to Casey (2011), the use of validated forensic software is a prerequisite for maintaining the scientific validity of digital evidence. When these technical capabilities are presented in a Shariah court, they function as a powerful form of *Qarinah*, providing objective, verifiable, and reproducible results. This technological support ultimately strengthens the judicial process, allowing for a more sophisticated and accurate adjudication of Shariah criminal cases in the digital age.

Recommendations for Legal Reform

To ensure that the Syariah legal system remains resilient in the face of rapid technological evolution, several legal reforms and strategic recommendations are proposed. These suggestions aim to harmonise the technical precision of digital forensics with the procedural requirements of Islamic evidence law.

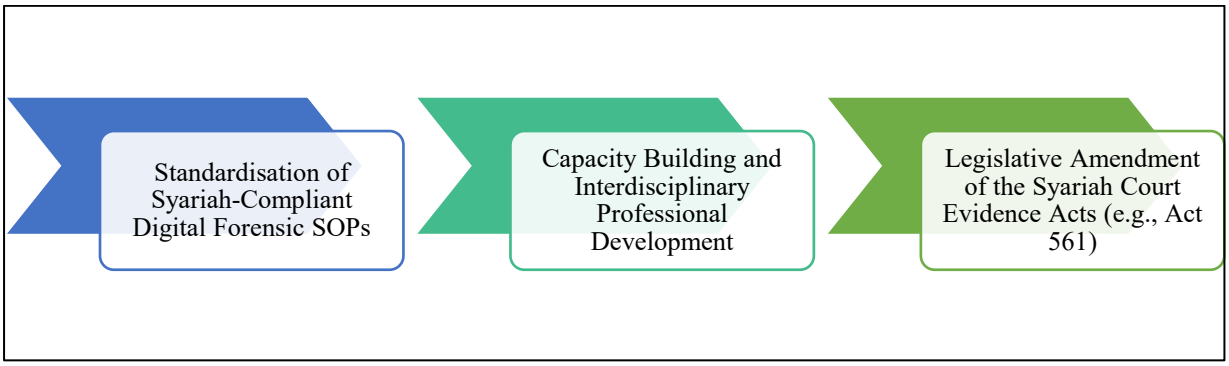

Figure 1. Strategic Framework for Legal Reform in Syariah Digital Forensics

First, there is an urgent need to standardise the Digital Forensic Standard Operating Procedures (SOPs) specifically for Syariah law enforcement agencies. Currently, while civil authorities follow established standards, Syariah enforcement often lacks a specialized framework that aligns forensic extraction with Syariah-compliant privacy (*satar al-awrāt*) and data integrity protocols. According to Alias et al., (2024), the absence of specific guidelines for searching and seizing electronic evidence in Syariah criminal cases may lead to the inadmissibility of crucial evidence due to procedural technicalities.

Second, the expansion of the legal definition of *qarinah* within the Syariah Court Evidence Acts (such as Act 561) is necessary. The current provisions should be amended to explicitly recognise digital forensic reports as a form of expert evidence (*al-ra'yu al-khubara'*) that can reach the level of *qarinah qat'iyyah* (conclusive circumstantial evidence). Tuan Ibrahim et al., (2025c) argue that explicit legal recognition would provide Syariah judges with the necessary confidence to rely on complex digital data, such as encrypted messages or blockchain transactions, without hesitation.

Third, the focus must be shifted towards providing extensive exposure and specialised training for Syariah legal practitioners, including judges, prosecutors, and enforcement officers. It is vital to equip these stakeholders with a foundational understanding of how digital evidence is retrieved and analysed. As emphasized by Nicole (n.d.), the credibility of digital evidence is heavily dependent on the competency of those handling and interpreting it. By bridging the knowledge gap between computer science and Islamic jurisprudence through continuous professional development, the judicial system can ensure that digital evidence is not only technically sound but also ethically and legally robust according to Shariah principles.

Conclusion

In conclusion, this study emphasises that the integration of digital forensic science into the Syariah criminal justice system in Malaysia is no longer an option but a critical necessity for addressing the complexities of crime in the digital age. By recognising digital forensics as a form of *qarīnah mu'āṣirah* grounded in scientific precision and data integrity, the evidentiary gaps inherent in traditional methods can be bridged with greater objectivity and effectiveness. However, the success of this transformation is

heavily dependent on comprehensive legal reforms, the standardisation of specialised operating procedures (SOPs), and the continuous capacity building of Syariah legal practitioners. Ultimately, empowering scientific evidence within the Syariah courts will ensure that Islamic judicial institutions remain dynamic, relevant, and capable of upholding justice and *maqasid al-shariah* amidst rapid technological advancements.

References

Al-Azhar, M. N. (2012). *Digital forensics: Panduan praktis investigasi komputer*. Salemba Infotek.

Alias, M. A. A., Wan Ismail, W. A. F., Baharuddin, A. S., & Abdul Mutalib, L. (2021). Legal analysis of Syariah Court evidence law on digital document as evidence and its admissibility in court proceedings. *Journal of Management and Muamalah*, *11*(2), 54–64.

Alias, M. A. A., Wan Ismail, W. A. F., Baharuddin, A. S., & Syah Mallow, M. (2024). Wasa'il Ithbat dalam undang-undang keterangan Islam: Analisis perundangan terhadap keabsahan dokumen elektronik di Mahkamah Syariah Malaysia. *Malaysian Journal of Syariah and Law*, *12*(1), 1–15.

Alias, M. A. A., Wan Ismail, W. A. F., Baharuddin, A. S., Hashim, H., & Tuan Ibrahim, T. M. F. H. (2025a). Digital forensics and the admissibility of electronic evidence in Malaysian Syariah courts: Towards a standardised legal framework. *LexForensica: Forensic Justice and Socio-Legal Research Journal*, *2*(1), 84–91.

Alias, M. A. A., Wan Ismail, W. A. F., Baharuddin, A. S., Hashim, H., & Tuan Ibrahim, T. M. F. H. (2025b). Digital forensics and the authentication of electronic evidence: Enhancing integrity, admissibility, and legal reform in Malaysian Syariah courts. *Syariah and Law Discourse*, *6*(1), 7–14.

Baharuddin, A. S. (2017). *The integration of forensic science fundamentals and Al-Qarinah towards achieving Maqasid Al-Shari'ah* (Doctoral dissertation). Universiti Teknologi Malaysia.

Casey, E. (2011). *Digital evidence and computer crime: Forensic science, computers, and the internet* (3rd ed.). Academic Press.

Goodison, S. E., Davis, R. C., & Jackson, B. A. (2015). *"Digital evidence and the U.S. criminal justice system: Identifying technology and other needs to more effectively acquire and utilize digital evidence"*. RAND Corporation. https://www.rand.org/pubs/research_reports/RR890.html

Ismail, I., & Akram Zainol Ariffin, K. (2025). The admissibility of digital evidence from open-source forensic tools: Development of a framework for legal acceptance. *PLOS ONE*, *20*(9), e0331683. https://doi.org/10.1371/journal.pone.0331683

Mohamad Aniq Aiman, M. A. A., Wan Abdul Fattah, W. A. F., Ahmad Syukran, A. S., Hasnizam, H., Tuan Muhammad Faris Hamzi, T. M. F. H., & Muhamad Nabilunnaim, M. N. (2025c). The integration of artificial intelligence (AI) into the Sharīʿah judiciary: A Maqāṣid al-Sharīʿah approach to ethical and legal transformation. *CFORSJ Procedia*, *3*(1), 119–127. https://alnadwah.usim.edu.my/cforsjprocedia/paper/view/204

Nicole. (n.d.). *"What is chain of custody and how is handling digital evidence any different?"*. Page Vault. https://blog.page-vault.com/digital-chain-of-custody

Pavithran, P. (2025, January 25). *"Role of digital forensics in modern enterprise security: Investigate & prevent cyber threats"*. Fidelis Security. https://fidelissecurity.com/cybersecurity-101/learn/digital-forensics/

Quick, D., & Choo, K. K. R. (2014). *Data reduction and data mining framework for digital forensic evidence: Storage, intelligence, review and archive* (Trends & Issues in Crime and Criminal Justice No. 480). Australian Institute of Criminology. https://doi.org/10.52922/ti180697

Strom, K. (2016). *Research on the impact of technology on policing strategy in the 21st century*. RTI International.

Tuan Ibrahim, T. M. F. H., Alias, M. A. A., Nor Muhamad, N. H., & Baharuddin, A. S. (2025a). Pembuktian forensik digital di Mahkamah Syariah: Kerangka kebolehterimaan dan integriti dalam jenayah Syariah. *Journal of Muwafaqat*, *8*(2), 78–100. https://doi.org/10.53840/muwafaqat.v8i2.197

Tuan Ibrahim, T. M. F. H., Nor Muhamad, N. H., Alias, M. A. A., & Baharuddin, A. S. (2025b). Fiqh al-Waqi': Teras revolusi keterangan forensik digital dalam membendung jenayah Syariah siber. *Jurnal 'Ulwan*, *10*(1), 28–46.

Tuan Muhammad Faris Hamzi, T. M. F. H., Nasrul Hisyam, N. H., Ahmad Syukran, A. S., & Mohamad Aniq Aiman, M. A. A. (2025c). The role of religious enforcement officers as Digital Evidence First Responders (DEFRs) in Syariah criminal investigations: A preliminary review. *CFORSJ Procedia*, *3*(1), 229–237. https://alnadwah.usim.edu.my/cforsjprocedia/paper/view/206

Wan Ismail, W. A. F., Baharuddin, A. S., Abdul Mutalib, L., & Alias, M. A. A. (2021). An appraisal of digital document as evidence in Islamic law. *Academic Journal of Interdisciplinary Studies*, *10*(3), 198–205.

Yahya, M. A., & Mohd Shariff, A. A. (2022). Proses penggeledahan keterangan dokumen elektronik dalam kes jenayah Syariah: Analysis the admissibility of electronic document evidence. *Journal of Muwafaqat*, *5*(2), 153–163. https://doi.org/10.53840/muwafaqat.v5i2.122

Yahya, M. A., Mohd Shariff, A. A., & Khalid, N. N. (2024). *Proses pengumpulan keterangan dokumen elektronik*. Penerbit UKM.