Syariah and Law Discourse

Vol. 6, No. 1, pp. 1-6 | 2025
Syariah and Law Discourse

A PRELIMINARY REVIEW OF DIGITAL FORENSICS AS A MEANS OF PROOF IN MODERN SYARIAH CRIMINAL OFFENCES FROM A MAQASID AL-SHARI'AH PERSPECTIVE

[i,ii,*]Tuan Muhammad Faris Hamzi Tuan Ibrahim, [ii]Mohamad Aniq Aiman Alias & [ii,iii,iv,v]Ahmad Syukran Baharuddin

[i]Islamic Civilization Academy, Faculty of Social Science and Humanities, Universiti Teknologi Malaysia (UTM), 81310, Johor Bahru, Johor, Malaysia
[ii]Faculty of Syariah and Law, Universiti Sains Islam Malaysia (USIM), 71800, Nilai, Negeri Sembilan, Malaysia
[iii]Centre of Research for Fiqh Forensics and Judiciary (CFORSJ), Faculty of Syariah and Law, Universiti Sains Islam Malaysia, Bandar Baru Nilai, 71800, Nilai, Negeri Sembilan, Malaysia
[iv]International Advisory Board Member, Mejellat Al-Afaq wa Al-Maarif (JSKP), Faculty of Humanities, Islamic Sciences and Civilization, University Amar Telidji of Laghouat, BP 37G, Road of Ghardaia, 03000 Laghouat, Algeria
[v]Associate Editor, Journal of Contemporary Maqasid Studies, Maqasid Institute, United States of America (USA)

*(Corresponding author) e-mail: tuanfaris.tf@gmail.com

Article history:
Submission date: 8 January 2023
Received in revised form: 10 March 2025
Acceptance date: 15 April 2025
Available online: 30 June 2025

Keywords:
Digital forensic, means of proof, Syariah criminal offences, maqāṣid al-sharīʿah

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:
Tuan Ibrahim, T. M. F. H., Alias, M. A. A., & Baharuddin, A. S. (2025). A preliminary review of digital forensics as a means of proof in modern syariah criminal offences from a *maqāṣid al-sharīʿah* perspective. *Syariah and Law Discourse, 6*(1), 1-6.

ABSTRACT

The rapid growth of digital technology has transformed the evidentiary landscape in Shariah criminal proceedings, with digital forensics emerging as a powerful means of presenting evidence. However, Malaysia's Shariah legal system still lacks a clear and consistent framework for the admissibility of forensic digital evidence. This study examines the role of digital forensics in proving modern Shariah criminal offences, focusing on its suitability and acceptance through the lens of *Maqāṣid al-Sharīʿah*. Using a qualitative approach, the study draws on primary sources such as Shariah evidentiary provisions, criminal procedure laws and international forensic standards (ISO/IEC 27037:2012), as well as secondary sources including scholarly works, journal articles and fiqh literature on *wasāʾil al-ithbāt* and *maqāṣid*. Data is analysed inductively to derive principles supporting the admissibility of digital evidence, which are then interpreted within the maqāṣid framework to ensure alignment with Shariah objectives. The findings emphasise that under Maqāṣid al-Sharīʿah, the principle and ultimate aim of proof in Shariah criminal law is the realisation of justice (*taḥqīq al-ʿadl*), the protection of public welfare (maṣlaḥah) and the prevention of harm (*dafʿ al-mafsadah*). Traditional means of proof such as *iqrār* (confession), *shahādah* (witness testimony) and *qarīnah* (circumstantial evidence) are procedural tools, not ends in themselves. Properly applied, digital forensics can significantly enhance evidentiary reliability, prevent wrongful convictions, and fulfil the higher objectives of Shariah. The study recommends formal legal recognition, standardised procedures, capacity building and stronger collaboration between Shariah institutions and forensic experts to ensure justice in the digital era.

Introduction

The world is witnessing a rapid transformation in the landscape of legal evidence which driven by advances in digital technology that transcend geographical, cultural, and legal boundaries (Corrales et al., 2019). This transformation not only impacts the civil justice system but also has substantial implications for the Shariah justice system, particularly in addressing modern criminal offences such as online gambling and a wide range of increasingly complex cybercrimes (Tuan Ibrahim et al., 2024). This evolution demands a new evidentiary approach that balances the technical demands of digital forensics with the evidentiary principles recognised under Shariah law.

In the context of Shariah law in Malaysia, criminal proof has traditionally relied on recognised categories of evidence such as *shahādah*, *iqrār*, *kitabah* and qarīnah (Wan Ismail, 2020). However, technological advancements have given rise to contemporary evidence, which includes digital evidence such as online transaction records, digital images and metadata (Jakub, 2024). Such evidence requires reliable scientific examination through the discipline of digital forensics to be admitted in court with a high degree of credibility.

Nevertheless, the current reality shows that the Shariah legal framework in Malaysia has yet to establish comprehensive guidelines on the handling, examination and evidentiary use of digital evidence. This gap creates a dual risk, first, the rejection of evidence by the court due to doubts over its authenticity and second, the possibility of wrongful convictions based on compromised or manipulated evidence (Yahya et al., 2024). Such circumstances not only undermine the effectiveness of prosecutions but can also erode public confidence in the Shariah justice system.

From the perspective of *Maqāṣid al-Sharīʿah*, the integration of digital forensics into Shariah criminal proceedings is not merely a technical matter but a *sharʿī* necessity to ensure that the higher objectives of Shariah are fulfilled. Principles such as the preservation of religion (*ḥifẓ al-dīn*), intellect (*ḥifẓ al-ʿaql*), honour (*ḥifẓ al-ʿirḍ*) and property (*ḥifẓ al-māl*) require that every evidentiary process be grounded in justice, transparency and authenticity. Without adherence to these principles, the risk of injustice increases, thereby contravening the maqāṣid's core aim of safeguarding and promoting societal welfare.

This study offers an in-depth examination of the role of digital forensics as a means of proof in modern Shariah criminal offences, with particular focus on an analysis grounded in *Maqāṣid al-Sharīʿah*. It explores how digital evidence can serve as a valid means of proof, the technical and procedural standards necessary to ensure its admissibility and how *maqāṣid* principles can be integrated into the formulation of a more robust evidentiary framework. This approach aims to contribute towards developing a model of proof that not only meets international forensic standards but is also fully aligned with Shariah requirements, thereby enhancing the resilience of the Shariah justice system in confronting the challenges posed by digital-age crimes.

Literature Review

Digital forensics is a branch of forensic science that focuses on the process of identifying, collecting, analysing, and presenting digital evidence in a scientifically sound manner for legal purposes (Vaishali et al., 2024). It involves the examination of various forms of electronic data, including computers, smartphones, cloud servers, internet networks, and digital storage devices. Its primary objective is to ensure that the evidence collected retains its original integrity, remains free from manipulation, and is admissible in court as reliable testimony (Hafiz Deandra et al., 2025).

In the context of courtroom proceedings, digital evidence offers unique advantages over traditional forms of testimony as it can provide detailed, objective, and scientifically verifiable information (Matijasevic et al., 2024). For instance, metadata embedded in a digital image can reveal the date, time, and location at which the image was taken, while server logs can record user activities in chronological order. However, the inherent ease with which digital evidence can be altered makes it highly susceptible to falsification or loss, necessitating meticulous handling in strict compliance with chain of custody standards.

In Shariah law, the proof of criminal offences is traditionally based on a few categories of evidence: *shahadah*, *iqrār* and *qarīnah*. Qarīnah is defined as an indication or sign that establishes a right or truth through logical inference and sharʿī reasoning (al-Zuhayli, 1982) and is traditionally employed as a complementary form of proof where *shahādah* or *iqrār* is insufficient. In contemporary practice, forensic digital evidence may be categorised as *kitabah*, *qarīnah* and *raʾy alkhabir* as long as it satisfies the requirements of fairness, authenticity, and reliability (Kallil & Che Yaacob, 2019; Tuan Ibrahim et al., 2025).

In Malaysia, the admissibility of digital evidence in civil courts is governed by the Evidence Act 1950 [Act 56] and reinforced by cases which emphasises the importance of maintaining a complete chain of custody (Alias et al., 2024). By contrast, in the Shariah Courts there is no specific statutory provision that explicitly governs the admissibility of digital evidence. Judges typically refer to the general principles of Shariah evidence as codified in the Shariah Court Evidence (Federal Territories) Act 1997 and assess admissibility based on *ijtihād*. This creates challenges where digital evidence must be evaluated simultaneously from both the technical perspective of forensic science and the *sharʿī* standards of evidentiary validity.

Moreover, the chain of custody plays a critical role in ensuring the admissibility of digital evidence, as it provides a continuous record of the ownership, control, transfer and storage of evidence from the time it is obtained until it is presented in court (Nath et al., 2024). Given the intangible nature of digital evidence, which can be altered without leaving visible traces, every stage of handling must be meticulously documented. Standards such as ISO/IEC 27037:2012 offer guidance on identifying, collecting, preserving, and examining digital evidence, yet their adaptation within the context of Shariah criminal cases remains limited. This highlights the urgent need to develop standard operating procedures (SOPs) that integrate forensic standards with Shariah principles to ensure that digital evidence is admissible without compromising the integrity of the Shariah legal framework.

Methodology

This study adopts a qualitative research design to examine the role of digital forensics as a means of proof in modern Shariah criminal offences from the perspective of Maqāṣid al-Sharīʿah. The analysis covers primary sources including Shariah evidentiary and criminal procedure provisions and technical standards for digital forensics. Secondary sources, such as scholarly works, journal articles and fiqh literature relating to the concepts of *wathail ithbat* and maqāṣid, are also consulted. The data is analysed inductively to identify principles supporting the admissibility of digital evidence, which are then interpreted within the *maqāṣid* framework to ensure that the recommendations produced align with the objectives of Shariah while meeting the technical standards of digital evidentiary practice.

Results and Findings

Within the context of *al-ʿuqūbāt* (criminal sanctions), *Maqāṣid al-Sharīʿah* emphasises that the ultimate purpose of implementing criminal penalties is to uphold justice (*al-ʿadl*), safeguard the public interest (*maṣlaḥah ʿāmmah*) and prevent harm (*mafsadah*) (Baharuddin, 2017). Scholars such as al-ʿAllāmah al-Fāsī, Wahbah al-Zuḥaylī and Aḥmad al-Raysūnī concur that every provision of Shariah carries a clear objective either in the form of general objectives (*maqāṣid ʿāmmah*) or specific objectives (*maqāṣid khāṣṣah*) to protect the al-ḍarūriyyāt al-khams: religion, life, intellect, honour/lineage, and property (Muhd Yusof, 2019). Justice, therefore, is the fundamental aim, whereas evidentiary procedures are merely tools to realise that aim

In Shariah criminal proof, *iqrār*, *shahadah,* and *qarīnah* are among the recognised *wasaʾil al-ithbāt* (means of proof). However, the underlying principle is clear: they are not ends in themselves but rather means to assist the judge in reaching a just verdict. A person may confess (*iqrār*) under coercion or with a dishonest motive, witnesses (*shahādah*) may blunder or lie, and *qarīnah* may be weak or subject to manipulation. Therefore, all these means must be assessed in terms of their capacity to genuinely uphold justice.

In line with contemporary developments, digital forensics has emerged as one of the *wasāʾil al-ithbāt al-muʿāṣirah* (modern means of proof), which may potentially be subsumed under the classical evidentiary categories of *kitābah* (documentary evidence), *qarīnah* (circumstantial evidence) or *raʾy al-khabīr* (expert opinion). The precise classification, however, requires further scholarly investigation to determine its proper jurisprudential placement within the Islamic evidentiary framework. Nevertheless, it is undeniable that digital forensics possesses significant potential to strengthen the probative value of evidence in Syariah criminal proceedings, thereby ensuring that the overarching objective of justice (*taḥqīq al-ʿadl*) is achieved in line with the principles of *Maqāṣid al-Sharīʿah*. Through scientific methods adhering to international standards such as ISO/IEC 27037:2012 and the principles of chain of custody, digital evidence can be analysed and its authenticity verified to a high degree of reliability. This enables offences to be proved or disproved based on objective facts, thereby reducing the risk of wrongful conviction or unjust acquittal.

It should be emphasised that within the framework of Maqāṣid al-Sharīʿah, the highest objective (maqṣad ʿāmm) of the judicial and penal system is the realisation of justice. The various evidentiary methods recognised in Islamic law, such as *shahādah*, *iqrār*, *kitābah* and *qarīnah* are not themselves the ultimate ends of the maqāṣid. Rather, they are procedural instruments designed to establish the truth of facts, safeguard individual rights, and ensure that proceedings are conducted fairly.

In this context, the classification of digital forensics as part of the *wasāʾil al-ithbāt al-muʿāṣirah* (contemporary means of proof) should be understood not as an end in itself, but as a mechanism whose validity and effectiveness are measured by its capacity to uphold justice in accordance with the principles of *Maqāṣid al-Sharīʿah*. This foundational perspective is essential in understanding evidentiary principles in Islamic criminal law, as it underscores that procedural rules must always be evaluated in terms of their contribution to the achievement of *taḥqīq al-ʿadl* and the prevention of injustice (*dafʿ al-ẓulm*).

Suppose the foundational principle of proof is justice. In that case, the question then arises, why have Shariah Courts not systematically utilised digital forensics to establish criminal liability in Shariah cases, particularly when it can provide such a high level of certainty? An over-reliance on traditional *wasaʾil al-ithbāt*, such as confessions and witness testimony alone, risks undermining the evaluation of evidence in modern criminal cases, especially those involving digital transactions, online communications, or cybercrime.

As Ibn ʿĀshūr emphasised, punishment in Islam is not intended merely to penalise but to eliminate injustice and prevent societal harm (Ibn ʻAshur, 2001). Likewise, Ibn al-Qayyim stressed that if offenders are not punished because their guilt cannot be established through strong evidence, society becomes vulnerable to disorder and moral decay (Ibn al-Qayyim, n.d.). In the digital era, therefore, rejecting or neglecting digital forensic methods that have proven to be more objective and accurate runs contrary to the very principles of maqāṣid.

In other words, so long as digital forensics is employed in accordance with lawful and ethical procedures, it not only fulfils the requirements of *wasaʾil al-ithbāt* in Shariah but also stands as one of the most effective tools for achieving the ultimate purpose of proof, ensuring that justice is upheld and the objectives of *Maqāṣid al-Sharīʿah* are realised.

Conclusion and Recommendation

The rapid advancement of digital technology has fundamentally altered the evidentiary landscape in both civil and Shariah legal systems. While Shariah courts in Malaysia continue to rely predominantly on traditional *wasaʾil al-ithbāt*, the emergence of the *wasāʾil al-ithbāt al-muʿāṣirah* in the form of scientifically verifiable digital forensic evidence offers unprecedented potential to ensure that the higher objectives of Shariah (*maqāṣid al-sharīʿah*) are achieved. In essence, the ultimate aim of criminal proof is not the rigid application of procedural forms, but the realisation of justice (*al-ʿadl),* the protection of public welfare (*maṣlaḥah*) and the prevention of harm (*mafsadah*). The evidentiary mechanisms recognised under Shariah law are tools to achieve this aim, not ends in themselves.

In contemporary reality, many forms of criminal activity, particularly those involving cybercrime, leave their traces primarily in digital form. The intangible and easily alterable nature of such evidence demands rigorous adherence to forensic best practices, particularly the maintenance of an unbroken chain of custody. International standards such as ISO/IEC 27037:2012 provide comprehensive technical guidance on digital evidence identification, collection, preservation, and examination. However, the adaptation of these standards within the Shariah legal context remains minimal, resulting in inconsistent application and occasional judicial reluctance to rely on such evidence in criminal proceedings.

In light of these considerations, several recommendations arise. First, Shariah courts should formally recognise and integrate digital forensic evidence within the framework of *wasaʾil al-ithbāt* supported by specific statutory provisions in Shariah criminal procedure and evidence laws. Second, standard operating procedures (SOPs) for handling digital evidence should be developed in alignment with international forensic standards while ensuring full compliance with Shariah principles, particularly in preserving the chain of custody. Third, capacity building and specialised training should be provided to Shariah judges, prosecutors, and religious enforcement officers to enhance their competence in assessing and managing digital forensic evidence. Finally, greater collaboration between Shariah legal institutions and forensic science experts should be encouraged to ensure that the application of digital forensics in Shariah criminal cases meets both technical and juristic requirements.

By embracing digital forensics as a legitimate and highly effective means of proof, Shariah courts can better fulfil their mandate to deliver justice, protect societal welfare, and uphold the principles of maqāṣid al-sharīʿah in the face of increasingly sophisticated digital-age crimes. Such an approach strengthens the credibility and resilience of the Shariah justice system and reaffirms its capacity to address contemporary challenges while remaining faithful to its divine objectives.

References

Alias, M. A. A., Wan Ismail, W. A. F., Baharuddin, A. S., Hasnizam, H., & Tuan Ibrahim, T. M. F. H. (2024). Evaluating electronic evidence in Malaysian civil courts: Current admissibility and future legal directions. *International Conference on Syariah, Law and Science (CFORSJ I-CONF), 2*(1), 13-21.

Baharuddin, A. S. (2017). *The integration of forensic science fundamentals and al-qarinah towards achieving maqasid al-shari'ah* (Doctor of Philosophy, Universiti Teknologi Malaysia).

Corrales, M., Fenwick, M., & Haapio, H. (2019). Digital technologies, legal design and the future of the legal profession. In *Legal Tech, Smart Contracts And Blockchain* (Pp. 1–15). Springer. https://doi.org/10.1007/978-981-13-6086-2_1

Hafiz Deandra, F., Sherly, & Muda, I. (2025). Advancing digital forensic investigations: Addressing challenges and enhancing cybercrime solutions-upubscience publisher. *Upubscience.Com*, *3*(1), 10–15.

Ibn ʻAshur, M. T. M. (2001). *Maqasid Al-Shariʻah Al- Islamiyyah.* Dar Al-Nafais.

Ibn Al-Qayyim, S. Al-Din M. (N.D.). *Al-Turuq al-hukmiyyah*. Dar Al-Kutub Al-'Ilmiyyah.

Jakub, M. (2024). Certain aspects of criminal evidence and digital evidence. *Analytical and Comparative Jurisprudence,* 699-704.

Kallil, M. K., & Che Yaacob, A. (2019). The integration of digital forensics science and Islamic Evidence laws. *International Journal Of Law, Government And Communication*, *4*(17), 61–70. https://doi.org/10.35631/ijlgc.417006

Matijašević, J., Bingulac, N., & Marinković, D. (2024). Digital evidence in criminal proceedings: Challenges and solutions. *Pravo - Teorija I Praksa*, *41*(4), 18–33. https://doi.org/10.5937/ptp2404018m

Mohd Yusof, S. (2019). *Kebolehterimaan keterangan forensik di Mahkamah Syariah Malaysia* (Doctor of Philosophy). Universiti Kebangsaan Malaysia.

Nath, S., Summers, K., Baek, J., & Ahn, G.-J. (2024). Digital evidence chain of custody: Navigating new realities of digital forensics. *Ieee International Conference On Trust, Privacy And Security In Intelligent Systems And Applications (Tps-Isa)*, 11–20. https://doi.org/10.1109/tps-isa62245.2024.00012

Tuan Ibrahim, T. M. F. H. ., Faisal, M. S., & Baharuddin, A. S. (2024). Judi dalam talian: Analisis awal isu dan cabaran pendakwaan di bawah Enakmen Kesalahan Jenayah Syariah di Malaysia: E-Gambling: Preliminary analysis on issues and challenges in prosecution under Syariah Criminal Offences Enactment In Malaysia. *Al-Qanatir: International Journal of Islamic Studies*, *33*(4), 1–10.

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

Vaishali, C. V., Thirumalaiswamy, V., & Thillaichidambaram, M. (2024). Introduction to digital forensics. In *Ai And Emerging Technologies* (Pp. 27–35). Crc Press.

Wan Ismail, W. A. F. (2020). *Keterangan dokumentar menurut fiqh dan undang-undang keterangan Islam di Malaysia.* Dewan Bahasa dan Pustaka.

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