Forensic Justice And Socio-Legal Research Journal
LEXFORENSICA

Vol. 2, No. 1, pp. 84-91 | 2025
CFORSJ Journal

DIGITAL FORENSICS AND THE ADMISSIBILITY OF ELECTRONIC EVIDENCE IN MALAYSIAN SYARIAH COURTS: TOWARDS A STANDARDISED LEGAL FRAMEWORK

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

[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 March 2025
Received in revised form: 15 June 2025
Acceptance date: 8 July 2025
Available online: 31 July 2025

Keywords:
Digital forensics, evidence, admissibility, electronic evidence, Malaysian Syariah courts, legal framework

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., Hashim, H., & Tuan Ibrahim, T. M. F. H. (2025). 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. https://doi.org/10.33102/6grx4619

SDG Elements:
Peace, Justice and Strong Institutions

ABSTRACT

The advancement of digital technology has introduced significant challenges to evidentiary processes, particularly within the Syariah judiciary in Malaysia. Electronic evidence—including mobile application messages, closed-circuit television (CCTV) recordings, emails, and online transactions—is increasingly tendered in Syariah proceedings. However, the absence of a legal framework under the Syariah Court Evidence (Federal Territories) Act 1997 [Act 561] has created substantial uncertainty, especially in relation to authentication and integrity. In contrast, the Civil Courts operate under the Evidence Act 1950 [Act 56], which provides comprehensive provisions governing the admissibility of electronic evidence. This study aims to analyse the existing legal framework governing electronic documents in Malaysia, explore the role of digital forensics in strengthening evidentiary reliability, and identify the issues and challenges faced by the Syariah judiciary in applying such methods. It further proposes legal and institutional reforms to enhance the effective management of electronic evidence in the future. The study employs a qualitative approach grounded in doctrinal analysis of statutes, case law, and scholarly literature, which are subsequently organised into thematic subcategories. The findings demonstrate that digital forensic tools—such as cryptographic hashing, digital signatures, metadata analysis, and blockchain play a crucial role in safeguarding the authenticity, integrity, and probative value of electronic documents. These mechanisms are also consistent with the objectives of the *maqāṣid al-sharīʿah*, particularly the protection of rights (*ḥifẓ al-ḥuqūq*), property (*ḥifẓ al-māl*), and dignity (*ḥifẓ al-ʿirḍ*). The study concludes that integrating digital forensics into Syariah evidentiary practice is vital to reinforce justice, enhance legal certainty, and safeguard the credibility of judicial outcomes in the digital era.

Introduction

The rapid development of information and communication technology has profoundly transformed evidentiary systems across the world, including within the Malaysian judiciary. In both civil and criminal proceedings, electronic documents such as emails, WhatsApp messages, CCTV footage, digital financial records, and metadata have increasingly been submitted to substantiate or refute claims (Radhakrishna et al., 2013). Their probative value lies in their ability to provide direct, immediate, and often highly detailed proof that conventional written or oral evidence cannot always offer. This trend signifies a paradigm shift in which electronic documents are no longer peripheral but have become central to the administration of justice (Goodison et al., 2012). In the context of Syariah courts, which adjudicate sensitive matters relating to family, morality, and religious obligations, the credibility of such evidence is especially critical in upholding justice, protecting rights, and ensuring procedural fairness (Wan Ismail et al., 2021).

Nevertheless, the admissibility of electronic evidence continues to generate persistent challenges. In the civil courts, the Evidence Act 1950 [Act 56] prescribes detailed procedures under sections 90A–90C for the admissibility of computer-generated documents (Mohamad, 2019). By contrast, the Syariah Court Evidence (Federal Territories) Act 1997 [Act 561] defines "documents" only in general terms, without explicit reference to electronic forms or technical requirements for authentication (Alias et al., 2024). This legislative gap has produced inconsistencies in practice, as the admissibility of electronic documents often depends on judicial discretion rather than uniform statutory guidance. Furthermore, risks of manipulation, alteration, and forgery—compounded by emerging threats such as deepfake technology—have raised serious concerns regarding the authenticity and reliability of electronic submissions. These concerns are exacerbated by the limited technical expertise of Syariah judges, prosecutors, and religious enforcement officers.

Against this backdrop, digital forensics emerges as a vital means of bridging the divide between Islamic legal principles and contemporary technological realities. By employing tools such as cryptographic hashing, digital signatures, and blockchain, digital forensics provides a scientific foundation for authenticating, preserving, and presenting electronic evidence in a manner consistent with both statutory requirements and Syariah principles. Accordingly, this article pursues four interrelated objectives: first, to analyse the legal framework governing electronic documents in Malaysia; second, to examine the role of digital forensics in strengthening evidentiary reliability; third, to identify issues and challenges in the Syariah judiciary relating to the application of digital forensics; and finally, to propose legal and institutional reforms for the effective management of electronic evidence.

Legal Framework Governing Electronic Documents in Malaysia

The Malaysian legal framework governing the admissibility of electronic documents operates under two parallel systems: the Evidence Act 1950 [Act 56], which applies to the Civil Courts, and the Syariah Court Evidence (Federal Territories) Act 1997 [Act 561] (taken here as a representative sample for Syariah courts nationwide) (Rajamanickam et al., 2022; Alias et al., 2021). Although both statutes recognise documents as admissible evidence, their treatment of electronic documents diverges significantly, particularly with respect to mechanisms of authentication, admissibility standards, and technical guidelines.

Under Act 56, explicit provisions regulate electronic documents. Mohamad (2019) observes that sections 90A, 90B, and 90C govern admissibility in the Civil Courts, with particular emphasis on authenticity. Section 90A permits the admission of computer-generated documents provided that they are produced in the ordinary course of the computer's use. Section 90B requires an authentication certificate verifying that a reliable system generated the document. Section 90C provides further technical guidance on computer operations and data integrity. These provisions have enabled the Civil Courts to admit a wide range of electronic materials—including emails, digital banking records, and forensic computer reports—while maintaining high standards of reliability.

For example, in *Glenn Whittle v. The Commissioner for Her Majesty's Revenue & Customs* [2014] UKFTT 254 (TC), evidence tendered during prosecution included computer printouts of bank account statements, taxi meter records, and other digital records maintained by the appellant for tax purposes. Similarly, section 90A(2) requires the production of a certificate from the person responsible for the computer system. Failure to provide such certification renders the evidence inadmissible due to a lack of authenticity. In *Bank Bumiputra Malaysia Berhad v. Emas Bestari Sdn Bhd & Anor* [2014] 1 CLJ 316, a bank statement generated by computer was rejected because it was not accompanied by a certificate from the officer who prepared it. These precedents illustrate the Civil Courts' strict reliance upon authenticity as a threshold requirement for electronic evidence.

By contrast, the Syariah Court Evidence (Federal Territories) Act 1997 [Act 561]does not expressly define "electronic document". Section 3 offers only a general definition of "document," encompassing anything expressed or described in any form, including matter contained in discs, tapes, films, soundtracks, or other devices—an implicit rather than explicit recognition of electronic formats (Yahya et al., 2017). Section 33 permits reliance on expert testimony to establish a document's authenticity, which may be extended to digital evidence through verification by forensic experts. Section 49 acknowledges computers as sources of evidence, but without prescribing detailed technical mechanisms.

Judicial practice shows that Syariah courts have admitted electronic evidence in several cases. For instance, in *Pendakwa Syarie v. Zulkifli bin Othman* [2013] 4 SHLR 92, digital photographs from a khalwat operation were admitted as primary evidence. In *Pendakwa Syarie v. A Mohad A/L Sahab bin Husin* [2013] 3 SHLR 33, digital images of a gambling premise were accepted. More recently, in *SM Faisal SM Nasimuddin v. Maria Chin Abdullah* [2023] 7 MLJ 485, online articles were admitted in contempt proceedings. However, such acceptance has largely depended on judicial discretion and expert testimony, rather than uniform statutory guidance.

The comparative analysis highlights several significant gaps in the Syariah Court Evidence (Federal Territories) Act 1997 [Act 561] when measured against the Evidence Act 1950 [Act 56]. First, there is no requirement for an authentication certificate equivalent to section 90B, leaving authenticity uncertain. Second, the broad definition of "document" under section 3 allows for varying judicial interpretations, undermining consistency in admissibility rulings. Third, unlike the Evidence Act 1950 [Act 56], which provides detailed procedural standards under sections 90A–90C, the Syariah Court Evidence (Federal Territories) Act 1997 [Act 561] contains no explicit guidance on handling electronic documents, thereby leaving matters largely to judicial discretion. Fourth, the absence of an express provision on the chain of custody further weakens safeguards against tampering or manipulation. Finally, while the Civil Courts benefit from provisions aligned with modern forensic standards, Syariah courts remain limited, relying heavily on expert interpretation without statutory support.

This analysis demonstrates that while both Acts recognise electronic documents, the Civil Courts operate under a more robust statutory regime. In contrast, the Syariah Courts remain dependent on general provisions open to broad interpretation. The findings underscore the pressing need for reform within the Syariah legal framework, particularly in developing clearer mechanisms of authentication and reliability.

In this respect, digital forensics may serve as a viable means of bridging the gap. Cryptographic hashing can secure the integrity of digital files from collection to presentation. Metadata analysis can verify timestamps and authorship, while digital signatures may confirm the authenticity of electronic contracts, digital divorce pronouncements, or marriage registrations. Blockchain technology could also be employed to record family law transactions in an immutable and transparent manner. Accordingly, the subsequent discussion focuses on the role of digital forensics in enhancing evidentiary reliability.

The Role of Digital Forensics in Strengthening Evidentiary Reliability

Digital forensics constitutes a specialised branch of forensic science. It applies scientific methods and technological tools to identify, acquire, analyse, and present digital information within a legal context (Tuan Ibrahim et al., 2025). In essence, it is a discipline designed to ensure that electronic documents are handled carefully, systematically, and in an auditable manner, thereby preserving their probative value before the courts. Its scope extends across multiple forms of data, including mobile application messages, electronic transaction records, emails, document metadata, audiovisual materials, and social media content. The primary strength of digital forensics lies in its ability to extract hidden information and detect even subtle alterations to data, rendering it a critical instrument for enhancing evidentiary reliability (Mohamad Nasir, 2023).

At the heart of digital forensics are three foundational principles of digital evidence: authenticity (Maras & Miranda, 2014), integrity (Casey, 2011), and reliability (Yahya et al., 2023). Authenticity requires that a document genuinely originates from its purported source, which can be verified through metadata analysis, such as timestamps and IP addresses, that confirm the creator's identity. Integrity ensures that the content remains unaltered throughout its lifecycle. Cryptographic hashing algorithms (e.g., SHA-256) generate unique digital "fingerprints" that change even with the smallest alteration, thereby ensuring tamper resistance. Ultimately, reliability relies on maintaining a comprehensive chain of custody that documents every stage of the handling process, thereby ensuring transparency and accountability in the preservation of digital evidence.

On the other hand, various forensic tools operationalise these principles. Digital signatures and the Public Key Infrastructure (PKI), for example, authenticate authorship and prevent document forgery, particularly in disputes involving matrimonial property claims or electronic contracts (Uzunay et al., 2007). Metadata analysis aids in verifying timelines and user activity, which is crucial in cases such as confirming a divorce pronouncement (ṭalāq) via messaging platforms or establishing account ownership in online defamation cases (Sgaras et al., 2016). Blockchain technology further provides a decentralised and immutable record, offering transparent and tamper-resistant mechanisms applicable to areas such as waqf management, hibah, or digital marriage registration, thereby reinforcing the principles of justice (*al-ʿadl*) and trust (*amānah*) (Akand et al., 2022).

Case law demonstrates the significance of digital forensics in Syariah contexts. In *Hisham Halim v. Maya Ahmad Fuaad* [2018] 3 LNS 15, expert intervention from CyberSecurity Malaysia was essential in authenticating an audio recording as admissible evidence. Conversely, in *Pendakwa Syarie Negeri Selangor v. Khalid bin Abdul Samad* [2019] 3 ShLR 39, a video recording was rejected due to unresolved doubts about its authenticity. These cases illustrate that without standardised forensic analysis, the admissibility of electronic evidence is easily challenged.

Conceptually, digital forensics aligns with Syariah principles. *Al-kitābah* (documentation) is embodied in the preservation of authentic electronic records, while *al-qarīnah* (corroborative evidence) is reinforced through metadata and digital traces. *Al-ra'yu al-khabīr* (expert opinion) is institutionalised through the involvement of digital forensic specialists in evaluating evidence authenticity. Collectively, these principles align with the objectives of the *maqāṣid al-sharīʿah*, particularly the preservation of justice (*ḥifẓ al-ʿadl*), property (*ḥifẓ al-māl*), lineage (*ḥifẓ al-nasl*), and dignity (*ḥifẓ al-ʿirḍ*).

Despite its potential, persistent challenges remain in the Syariah judiciary, including the absence of specific Standard Operating Procedures (SOPs), limited technical expertise among judges and prosecutors, and the prohibitive cost of forensic software. Reform is therefore necessary through the issuance of Practice Directions on digital evidence, continuous technical training for religious enforcement officers and judges, and strategic collaboration with expert agencies such as CyberSecurity Malaysia, SIRIM QAS International, and the Malaysian Communications and Multimedia Commission (MCMC). Through these measures, digital forensics can be institutionalised as a core mechanism for authenticating electronic documents, thereby strengthening the reliability, integrity, and probative value of evidence in Syariah court proceedings.

While digital forensics promises to enhance the credibility of electronic documents, the reality remains that its implementation in Syariah courts faces procedural, technical, and infrastructural limitations, alongside the risks of data manipulation. The subsequent section will therefore examine the key issues and challenges that impede the effective application of digital forensics within the Syariah judicial system, before moving on to possible reforms and proposed frameworks for improvement.

Issues and Challenges in the Application of Digital Forensics to Electronic Evidence in the Syariah Judiciary

Although digital forensics holds significant potential in strengthening the reliability of electronic documents, several issues and challenges have been identified in its implementation within the Syariah judiciary. Three principal challenges may be highlighted: the absence of specific Standard Operating Procedures (SOPs), the lack of technical expertise among Syariah judicial actors, and the risks of data manipulation and privacy breaches.

Absence of Specific SOPs for the Management of Digital Evidence

The most pressing challenge is the absence of standardised SOPs governing the collection, preservation, and authentication of electronic documents in Syariah courts. Unlike the Civil Courts, which are guided by explicit provisions under the Evidence Act 1950 [Act 56], particularly sections 90A to 90C, Syariah courts continue to rely on general statutory interpretations without concrete technical guidelines. This deficiency results in inconsistent practices across different states and creates opportunities for the defence to contest the authenticity and integrity of evidence. Wan Ismail et al., (2023) emphasise that the absence of SOPs complicates procedural standardisation and undermines judicial authority in cases involving electronic evidence.

Limited Technical Expertise among Judges, Prosecutors, and Religious Enforcement Officers

Beyond procedural shortcomings, human resource limitations also pose a significant obstacle. The majority of Syariah judges, prosecutors, and religious enforcement officers are trained in law or Islamic jurisprudence but lack adequate exposure to computer science and digital forensics (Yahya et al., 2024). This gap impedes their ability to comprehend technical reports such as metadata analyses or the results of cryptographic hashing, both of which are crucial for determining the authenticity of electronic documents. Tuan Ibrahim et al., (2025) observe that this expertise gap compromises the courts' capacity to critically evaluate electronic evidence, particularly in cybercrime cases such as online gambling, the dissemination of deviant digital teachings, or religious defamation on social media.

Risks of Data Manipulation and Privacy Breaches

A further challenge concerns the risk of data manipulation and privacy violations. Electronic documents can be easily altered using editing software or advanced technologies such as *deepfakes*, thereby raising doubts about the authenticity of the evidence presented. More concerning still is the potential for the personal data of litigants to be compromised if information security mechanisms are not rigorously implemented. Weak security controls not only diminish the integrity of evidence but may also undermine the objectives of the *maqāṣid al-sharīʿah*, particularly the protection of dignity (*ḥifẓ al-ʿirḍ*) and the safeguarding of information (*ḥifẓ al-maʿlūmāt*).

In summary, although the integration of digital forensics provides valuable tools for authenticating electronic documents submitted in court, its comprehensive application within the Syariah judiciary remains constrained by structural and technical barriers. The absence of SOPs, the shortage of technical expertise, and the persistent risks of data manipulation and privacy breaches collectively threaten the admissibility and credibility of electronic evidence. Accordingly, the next section of this study proposes several legal and institutional recommendations aimed at strengthening the integration of digital forensics, thereby enhancing the administration of justice in the Syariah courts.

Legal and Institutional Reform in the Management of Electronic Evidence

Based on the earlier discussion of the legal framework, the admissibility of electronic evidence in Malaysian Syariah courts requires substantive legal and institutional reform to address existing gaps between the civil and Syariah evidentiary regimes. Currently, the Evidence Act 1950 [Act 56] provides a structured legal framework for the admissibility of electronic documents, particularly under sections 90A–90C, which establish clear procedures for authentication, certification, and chain of custody. By contrast, the Syariah Court Evidence (Federal Territories) Act 1997 [Act 561] remains silent on specific procedures for handling digital documents, relying instead on general definitions and judicial discretion. This lacuna has resulted in inconsistent practices, leaving Syariah courts vulnerable to challenges concerning the integrity and admissibility of electronic materials. Reform is therefore necessary not only to strengthen the credibility of Syariah court judgments but also to ensure parity with civil court practices while remaining aligned with Islamic legal principles.

One key area of reform is the formulation of a comprehensive SOP on digital evidence. Such an SOP, ideally promulgated as a Practice Direction by the Department of Syariah Judiciary Malaysia (JKSM), would establish uniform procedures nationwide. It should cover protocols for data acquisition, forensic preservation, storage, authentication, and the documentation of a digital chain of custody. By institutionalising these processes, the courts can ensure that electronic evidence is treated with consistency, transparency, and scientific reliability. Importantly, the introduction of a Syariah-specific SOP would also reduce reliance on ad hoc judicial interpretation and shield proceedings from unnecessary disputes over authenticity.

Equally crucial is the strengthening of technical capacity among Syariah judges, prosecutors, and religious enforcement officers. While these officers are highly trained in Syariah jurisprudence, most have limited exposure to computer forensics and information technology. This knowledge gap constrains their ability to evaluate forensic reports, such as metadata analyses or hash verifications, and risks undermining the probative value of digital submissions. Structured training programmes, carried out in collaboration with expert agencies such as CyberSecurity Malaysia, SIRIM QAS International, and the Malaysian Communications and Multimedia Commission (MCMC), are therefore indispensable. Such collaborations would empower Syariah legal actors to critically assess forensic findings while aligning judicial practice with international evidentiary standards.

Reform must also extend to data protection and ethical safeguards. The vulnerability of electronic documents to tampering, *deepfake* technology, and unauthorised disclosure underscores the importance of embedding privacy protections within Syariah evidentiary practice. The adoption of international standards such as ISO/IEC 27001 on information security would serve as a benchmark for safeguarding litigants' personal data while ensuring procedural fairness. Embedding these safeguards would not only protect dignity (*ḥifẓ al-ʿirḍ*) and rights (*ḥifẓ al-ḥuqūq*) but also enhance public trust in the credibility of Syariah judicial determinations.

In the long term, Malaysia should consider establishing a dedicated Syariah digital forensic ecosystem. This initiative could include the creation of specialised forensic units within State Islamic Religious Departments (JAIN) as well as the development of accredited laboratories capable of handling Syariah-related cases. Such infrastructure would reduce dependence on external civil or private agencies while providing in-house scientific capacity tailored to the evidentiary requirements of Syariah law. More importantly, the existence of specialised units would operationalise the principles of *maqāṣid al-sharīʿah*, particularly justice (*al-ʿadl*), protection of property (*ḥifẓ al-māl*), and preservation of dignity (*ḥifẓ al-ʿirḍ*), within a digitalised legal context.

Beyond domestic reform, there is value in examining comparative experiences from other Muslim jurisdictions. Indonesia, for instance, has enacted the *Undang-Undang Informasi dan Transaksi Elektronik* (UU ITE), which explicitly recognises electronic documents and digital signatures as valid legal evidence (Law No. 11/2008 & its amendment Law No. 19/2016). Brunei has also introduced legislation facilitating the use of digital evidence in criminal proceedings, ensuring that electronic submissions are not excluded solely because of their digital format. Meanwhile, the United Arab Emirates (UAE) has gone further by embedding electronic evidence within its judicial system through comprehensive cybercrime laws and data protection legislation, including the Personal Data Protection Law (PDPL). While each of these jurisdictions operates within different legal and cultural contexts, their experiences demonstrate practical models for integrating digital evidence into judicial practice. By critically studying their approaches, Malaysia may adopt best practices while avoiding pitfalls, thereby ensuring that any adaptation remains consistent with the normative principles of Syariah.

Taken together, these reforms present a holistic pathway for enhancing the management of electronic evidence in Syariah courts. By institutionalising SOPs, building technical capacity, embedding ethical safeguards, and drawing insights from international experiences, Malaysia can develop a robust and credible framework that upholds both statutory requirements and Syariah principles. At the same time, further research should explore two important areas: the design of a comprehensive Syariah digital forensic ecosystem integrating law, technology, and institutional collaboration; and comparative studies with other Islamic jurisdictions to benchmark best practices. Such initiatives would ensure that the Syariah judiciary evolves in tandem with technological realities while remaining anchored in the higher objectives of *maqāṣid al-sharīʿah*.

Conclusion

This study has examined the admissibility and management of electronic evidence in Malaysian Syariah courts, highlighting the pressing need for a clearer and more consistent framework. The findings reveal that while electronic materials such as emails, mobile messages, and audiovisual recordings are increasingly common in litigation, Syariah courts remain constrained by legal ambiguities and procedural gaps when compared to the more structured provisions of the Evidence Act 1950 [Act 56]. The analysis shows that the Syariah Court Evidence Act 1997 [Act 561] provides only general references to documents, leaving the determination of authenticity and reliability largely to judicial discretion. This contrasts with the civil courts, which benefit from explicit statutory mechanisms under sections 90A–90C. At the same time, Syariah principles of evidence—*al-kitābah* (documentation), *al-qarīnah* (corroborative evidence), and *al-ra'yu al-khabīr* (expert opinion)—affirm the importance of authenticity, integrity, and reliability as values consistent with the *maqāṣid al-sharīʿah*.

The study further underscores the value of digital forensics in bridging this gap. Tools such as cryptographic hashing, digital signatures, metadata analysis, and blockchain strengthen the probative value of electronic submissions. Case law also demonstrates that expert intervention can determine whether electronic evidence is admitted or rejected, thereby reinforcing the importance of forensic expertise. Nevertheless, challenges persist. The absence of standard operating procedures (SOPs), limited technical expertise among Syariah judicial officers, and risks of data manipulation and privacy breaches threaten the credibility of electronic evidence. Addressing these shortcomings requires reform through the development of SOPs, capacity-building, data protection safeguards, and the gradual establishment of a Syariah digital forensic ecosystem. The contribution of this study lies in proposing practical reforms that integrate forensic science with Islamic legal principles. By strengthening procedures, building expertise, and safeguarding litigants' rights, the Syariah judiciary can ensure that its evidentiary framework evolves in step with technological realities while remaining faithful to the higher objectives of the *maqāṣid al-sharīʿah*.

References

Akand, M. A.-S., Reza, S. A., & Akhi, A. B. (2022). Blockchain-based Islamic marriage certification with the supremacy of Web 3.0. *Intelligent Control and Automation*, *13*(4), 39–53. https://doi.org/10.4236/ica.2022.13.4004

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: Analisis perundangan bagi undang-undang keterangan Mahkamah Syariah terhadap dokumen digital sebagai kaedah pembuktian dan kebolehterimaannya dalam prosiding mahkamah. *Journal of Management and Muamalah, 11*(2), 54–64.

Alias, M. A. A., Wan Ismail, W. A. F., Baharuddin, A. S., & Mallow, M. S. (2024). *Wasa'il ithbat* dalam undang-undang keterangan Islam: Analisis perundangan terhadap kebolehterimaan dokumen elektronik di Mahkamah Syariah Malaysia: Means of proof in Islamic law of evidence: A legal analysis of the admissibility of electronic documents in Malaysian Syariah courts. *Malaysian Journal of Syariah and Law, 12*(3), 689–700. https://doi.org/10.33102/mjsl.vol12no3.792

Callaghan, P. (n.d.). *"Why hash values are crucial in digital evidence authentication"*. Pagefreezer. https://blog.pagefreezer.com/importance-hash-values-evidence-collection-digital-forensics

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. (2012). *Digital evidence and the U.S. criminal justice system*. National Institute of Justice.

Maras, M.-H., & Miranda, M. (2014). *"Cybercrime module 4: Introduction to digital forensics"*. United Nations Office on Drugs and Crime (UNODC). https://www.unodc.org/e4j/en/cybercrime/module-4/index.html

Mohamad Nasir, H. (2023, December 15). *"Memperkasakan Bahagian Forensik Teknologi SPRM dalam jenayah siber"*. Suruhanjaya Pencegahan Rasuah Malaysia (SPRM). https://www.sprm.gov.my/index.php?id=21&page_id=103&contentid=3094&cat=BKH

Mohamad, A. M. (2019). Admissibility and authenticity of electronic evidence in the courts of Malaysia and United Kingdom. *International Journal of Law, Government and Communication, 4*(15), 121–129.

Radhakrishna, G., Zan, M., & Khong, D. W. K. (2013, January 30). *"Computer evidence in Malaysia: Where are we?"*. SSRN. https://doi.org/10.2139/ssrn.2208973

Rajamanickam, R., Mohamad Noh, N. I., & Harun, A. (2022). Kebolehterimaan keterangan elektronik di Malaysia. *Jurnal Undang-undang dan Masyarakat (JUUM), 31*, 111–125.

Sgaras, C., Kechadi, M.-T., & Le-Khac, N.-A. (2016). *"Forensics acquisition and analysis of instant messaging and VoIP applications"*. arXiv. https://arxiv.org/abs/1612.00204

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.

Uzunay, Y., Incebacak, D., & Bicakci, K. (2007). Towards trustable digital evidence with PKIDEV: PKI based digital evidence verification model. In J. Lopez, S. Furnell, & R. Pernul (Eds.), *Trust and privacy in digital business: Third international conference, TrustBus 2006, Kraków, Poland, September 4–6, 2006. Proceedings* (pp. 141–150). Springer. https://doi.org/10.1007/978-1-84628-750-3_11

Wan Ismail, W. A. F., Baharuddin, A. S., Mutalib, L. A., & Alias, M. A. A. (2021). A systematic analysis on the admissibility of digital documents as evidence in Malaysian Syariah courts. *Pertanika Journal of Social Sciences & Humanities, 29*(3), 1981–1996. https://doi.org/10.47836/pjssh.29.3.26

Yahya, A., Azam, A., & Hassan, A. (2017). Keterangan dokumen dalam bentuk digital di Mahkamah Syariah: Analisis berkaitan definisi serta kebolehterimaannya di sisi prinsip Syariah di Malaysia. *Current Legal Issue, 1*, 1–12.

Yahya, A., Mohd Shariff, A. A., & Saifuddin, S. (2023). Application of principles of chain of evidence and chain of custody during storage and forensic examination of electronic documentary evidence in Shariah criminal cases in Malaysia. *IIUM Law Journal, 31*(2), 145–166.

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