Syariah and Law Discourse

Vol. 6, No. 1, pp. 7-14 | 2025
Syariah and Law Discourse

DIGITAL FORENSICS AND THE AUTHENTICATION OF ELECTRONIC EVIDENCE: ENHANCING INTEGRITY, ADMISSIBILITY, AND LEGAL REFORM IN MALAYSIAN SYARIAH COURTS

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

[i]Faculty of Syariah and Law, Universiti Sains Islam Malaysia (USIM), 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: 15 January 2023
Received in revised form: 22 March 2025
Acceptance date: 25 April 2025
Available online: 30 June 2025

Keywords:
Electronic evidence, digital forensic, admissibility, legal reform, Malaysian Syariah courts

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 authentication of electronic evidence: enhancing integrity, admissibility, and legal reform in Malaysian Syariah courts. *Syariah and Law Discourse, 6*(1), 7-14.

ABSTRACT

The rapid development of digital technology has introduced a new dimension into evidentiary systems, including the Syariah judiciary in Malaysia. Digital evidence such as audio-visual recordings, mobile application messages, emails, and document metadata is increasingly submitted in court proceedings to either substantiate or refute claims made during litigation. However, the absence of a clear legal framework on the admissibility of electronic evidence in Malaysian Syariah Courts has indirectly resulted in heightened risks of data manipulation and privacy breaches, which pose serious challenges to the authentication and admissibility of such evidence. This article therefore aims to examine the concept and tools of digital forensics in the authentication of electronic documents, analyse the issues and challenges faced within the Syariah legal context, and propose possible legal reforms. The study adopts a qualitative approach through document analysis, which is subsequently organised into subthemes. The findings reveal that strengthening the authentication of digital evidence requires the promulgation of a standardised Standard Operating Procedure (SOP), continuous technical training, and strategic collaboration with industrial agencies such as CyberSecurity Malaysia, SIRIM QAS International, and the Malaysian Communications and Multimedia Commission (MCMC). The study affirms that the integration of digital forensics is not only consistent with the principles of *maqāṣid al-sharīʿah* and *fiqh al-wāqiʿ*, but also essential to reinforce justice while ensuring the integrity, reliability, and admissibility of electronic evidence in Syariah proceedings. The article further recommends that future research explore the development of a more comprehensive and sustainable Syariah digital forensic ecosystem.

Introduction

The rapid advancement of information and communication technology has profoundly influenced legal systems across the globe, including the Syariah judicial framework in Malaysia. The emergence of digital evidence—such as mobile application messages, closed-circuit television (CCTV) recordings, emails, electronic transactions, videos and social media data—has become increasingly prevalent in judicial proceedings as substantive proof in both civil and criminal cases (Ab Rahman, 2021; Yahya & Mohd Shariff, 2021). While this form of evidence holds great potential in strengthening both prosecutorial and defence claims, its inherent vulnerability to manipulation, alteration, and forgery renders it highly susceptible to legal challenges in the absence of a reliable mechanism of authentication (Mustapa Sa'di et al., 2015).

Digital forensics has thus emerged as a crucial tool to ensure that electronic evidence is properly acquired, preserved, analysed, and presented in a manner that upholds its integrity, reliability, and admissibility before a court of law. However, within the Malaysian Syariah Courts, several pressing gaps and limitations impede the optimal utilisation of such technology. Among these is the absence of a comprehensive Standard Operating Procedure (SOP) governing the handling of digital evidence. Unlike the Civil Courts, which benefit from detailed statutory provisions under the Evidence Act 1950 [Act 56], Syariah Courts currently lack an equivalent procedural framework to regulate electronic document collection, storage, and presentation (Alias et al., 2024a). In addition, the limited technical expertise among Syariah judges, prosecutors, and religious enforcement officers significantly constrains their ability to evaluate digital forensic findings critically and to determine the authenticity of electronic materials presented in court (Yahya et al., 2023). These legal and institutional deficiencies are further compounded by risks of data manipulation, privacy breaches, and broader ethical implications, all of which may undermine the credibility and effectiveness of the Syariah judicial process.

Given these challenges, there is a clear and urgent need for scholarly engagement that integrates the normative principles of Syariah—particularly those rooted in maqāṣid al-sharīʿah—with contemporary forensic and technological methodologies. Accordingly, this article examines the conceptual and legal dimensions of digital forensics and evidence authentication, evaluates the role and application of digital forensic tools in authenticating electronic documents within the Syariah Court system, and analyses the prevailing challenges, institutional gaps, and potential reforms necessary to enhance the admissibility and reliability of digital evidence in Syariah legal proceedings.

Forensic Science Foundations and the Role of Digital Forensics in Evidence Authentication

The concept of forensics originates from the Latin word "*forensis*", which refers to the forum or court—a reference to the Roman practice of conducting public trials in communal spaces (TG Team, 2015). Over time, the term evolved to denote the application of scientific methods and techniques in addressing legal questions, particularly in the evaluation of evidence and litigation processes (Baharuddin, 2017). Metwally (2009) defines forensic science as the systematic application of scientific and technical methods to identify, collect, evaluate, and interpret evidence in civil, criminal, and administrative contexts.

As illustrated in Figure 1, forensic science comprises multiple specialised disciplines, including forensic chemistry, forensic biology, forensic anthropology, forensic psychology, forensic engineering, and digital and cyber forensics, among others (Kapoor et al., 2023). One of the most significant emerging branches is digital forensics, which has become indispensable in contemporary evidentiary practice. Digital forensics systematically applies technological and scientific methodologies to identify, recover, analyse, and present electronic evidence in legal proceedings (Nelson et al., 2019). Scholars have further recognised that digital forensics now stands on par with more established forensic disciplines due to its unique capacity to extract concealed information from diverse digital platforms and electronic devices (Carrier & Spafford, 2003).

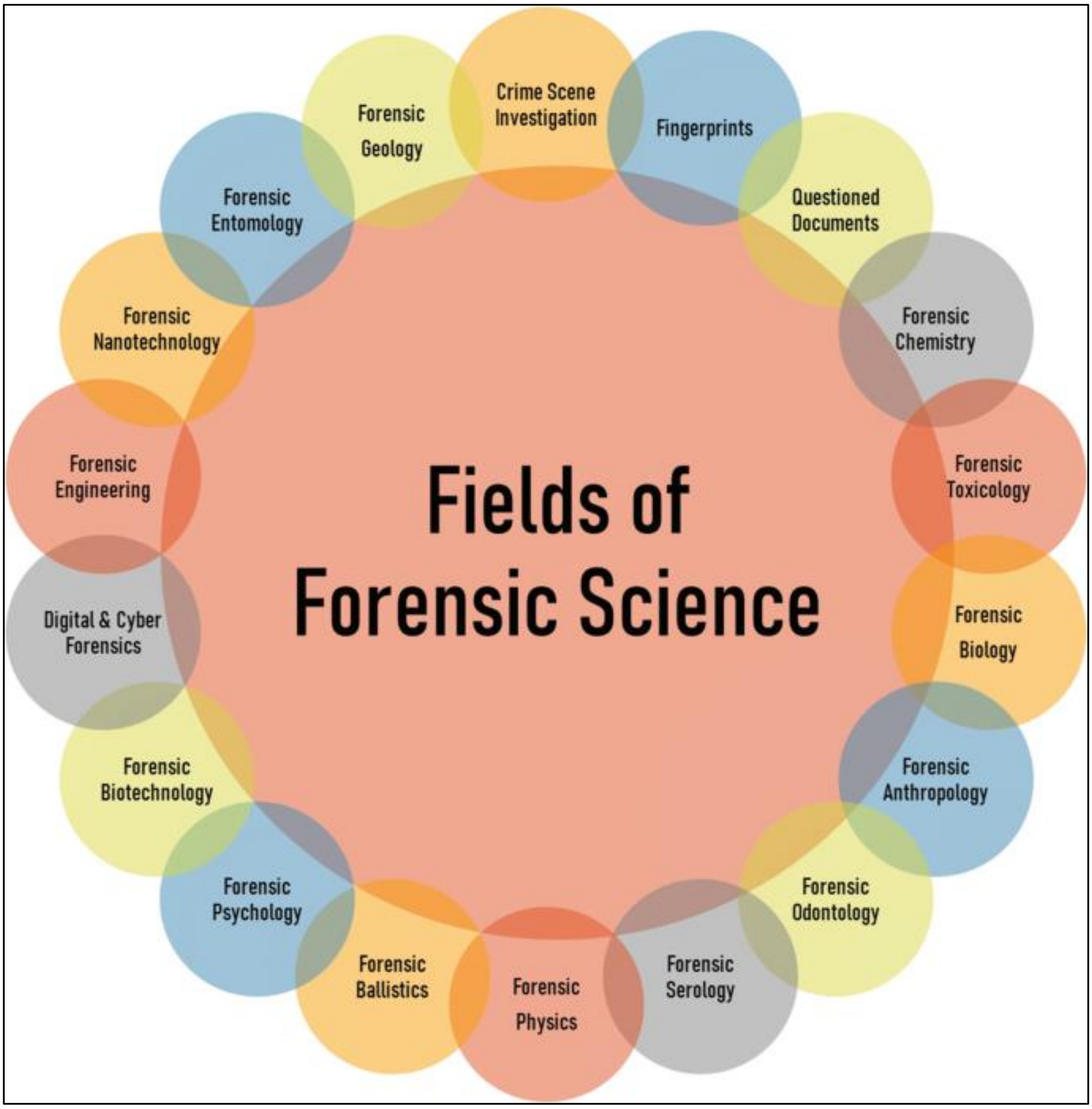

Figure 1. Fields of Forensic Science (Kapoor et al., 2023)

Given the inherent vulnerability of digital evidence to alteration, tampering, or deletion, the authentication of such evidence is of paramount importance. The admissibility of digital evidence in court must rest upon three fundamental principles: authenticity, integrity, and reliability (Yahya et al., 2023; Mohamad, 2019). Authenticity requires that electronic material genuinely originates from its purported source and remains unaltered. This may be demonstrated through metadata analysis embedded in communications such as WhatsApp messages or emails, where timestamps and sender identities can be verified (Maras & Miranda, 2014). Integrity refers to the assurance that digital content remains unmodified throughout its lifecycle, including storage, transfer, and forensic analysis. This principle is typically safeguarded through cryptographic techniques such as SHA-256 hashing, which generates a unique digital fingerprint for each file; even the smallest change produces a distinct hash value, signalling potential compromise (Casey, 2011). Reliability underscores the requirement that digital evidence be handled with transparency and scientific rigour, with every stage documented through a comprehensive and auditable chain of custody (Alias et al., 2024).

Thus, the chain of custody is a critical safeguard in preserving the evidentiary value of digital materials. It provides chronological documentation of the acquisition, transfer, handling, and analysis of evidence until its presentation in court. Any ambiguity in this chain risks undermining admissibility, as questions may arise regarding authenticity and integrity. Recent technological advances have further strengthened authentication mechanisms. Metadata analysis, for example, enables investigators to confirm creation dates, geographic locations, and user interactions with electronic documents. Similarly, blockchain technology introduces an innovative mechanism for ensuring secure and immutable preservation of digital records. Through its decentralised and tamper-evident ledger, blockchain offers a promising tool for enhancing the credibility and transparency of digital evidence in judicial contexts (Tuan Ibrahim et al., 2025).

Crucially, these scientific innovations do not conflict with Islamic legal theory (Alias et al., 2024b). The application of digital forensic technology aligns with the principles of *fiqh al-wāqiʿ*, which emphasise the necessity of Islamic legal rulings remaining responsive to contemporary realities. Provided that the conditions of authenticity and integrity are satisfied, digital evidence may be admissible as *qarinah* (circumstantial or corroborative evidence) within the Syariah judicial framework (Yahya et al., 2023; Wan Ismail et al., 2020). This alignment underscores the compatibility of forensic methodologies with the objectives of *maqāṣid al-sharīʿah*, particularly in upholding justice (*al-ʿadl*) and safeguarding individual rights (*ḥifẓ al-ḥuqūq*).

In light of these considerations, the following section discusses the technical tools and forensic methodologies employed in authenticating electronic documents submitted as evidence in Syariah court proceedings. These tools not only enhance evidentiary reliability but also operationalise the legal framework for the admissibility of electronic evidence in accordance with both statutory and Syariah requirements.

Digital Forensic Tools and Their Role in the Authentication of Electronic Documents in the Syariah Court

Building upon the conceptual foundations of digital forensics and the principles of evidence authentication, examining the technological tools that operationalise these concepts within the legal framework is imperative. In contemporary evidentiary practice, digital forensic tools form the technological backbone for verifying the authenticity and reliability of electronic documents. These tools include specialised software, cryptographic algorithms, and scientific methodologies designed to detect, collect, preserve, and analyse digital data in a forensically sound and legally admissible manner. Their utilisation complements expert testimony; in the absence of standardised and scientifically validated tools, forensic expert opinions risk being challenged or disregarded. Thus, properly deploying such tools is crucial for establishing the admissibility of electronic documents as *qarīnah* (corroborative evidence) in Syariah court proceedings.

One of the most fundamental tools in digital forensics is the cryptographic hashing algorithm, particularly MD5, SHA-1, and SHA-256. These algorithms convert electronic data into a unique hash value that functions as a digital fingerprint of a file’s content. Any alteration, however minimal, produces a drastically different hash output, thereby enabling tampering detection. This ensures that electronic documents—such as WhatsApp messages, emails, or PDF files—can be verified as unchanged from the time of acquisition until their presentation in court (Casey, 2011). Such mechanisms align with the Syariah principle of *aṣālah* (authenticity), since any modification or uncertainty directly undermines evidence’s probative value and admissibility.

Equally significant are digital signatures and the Public Key Infrastructure (PKI) framework, which enable the verification of the origin and authorship of electronic documents. In cases involving matrimonial disputes, financial claims, or inheritance documentation, digital signatures serve as legally recognised tools to confirm that the rightful individual or institution issued a document. This is critical in preventing impersonation, identity fraud, and document forgery—concerns that directly engage the *maqāṣid al-sharīʿah*, particularly the preservation of lineage (*ḥifẓ al-nasl*) and property (*ḥifẓ al-māl*) (Yahya et al., 2023).

Blockchain technology has also emerged as an innovative tool for ensuring the integrity and traceability of digital records. By maintaining a decentralised and immutable ledger, blockchain systems create an auditable and virtually tamper-proof trail. Its application is particularly relevant in contexts such as *waqf* management, *hibah*, and digital contractual arrangements, where unauthorised modifications could compromise document validity. In such circumstances, blockchain reinforces the principles of *al-ʿadl* (justice) and *amānah* (trust), while advancing the objectives of the *maqāṣid al-sharīʿah* by safeguarding wealth (*ḥifẓ al-māl*) and ensuring procedural fairness (Mohaiyadin et al., 2022; Aljamos et al., 2022; Alsadi, 2025).

Forensic practitioners also employ advanced software such as EnCase, Forensic Toolkit (FTK), and X-Ways Forensics to conduct detailed examinations. These tools enable comprehensive metadata analysis, allowing investigators to trace document creation dates, access logs, modification histories, and user activity. Metadata analysis is particularly valuable in Syariah contexts, such as verifying timelines in *ṭalāq* proceedings, establishing account ownership in cyber-defamation cases involving religious figures, and substantiating financial records in *muʿāmalāt*-related disputes (Nelson et al., 2019). Without such tools, validating the credibility and provenance of digital submissions in court would be extremely difficult.

Despite their critical role, the integration of these tools in the Malaysian Syariah Court remains limited. Persistent challenges include the high cost of licensed forensic software, the absence of standardised operating procedures (SOPs), and the limited technical expertise of Syariah prosecutors and religious enforcement officers (Alias et al., 2024a). These shortcomings were evident in cases such as *Pendakwa Syarie Negeri Selangor v Khalid bin Abdul Samad* [2019] 3 ShLR 39, where a video recording failed to substantiate a criminal charge due to unresolved questions regarding its authenticity. Similarly, in *Hisham Halim v Maya Ahmad Fuaad* [2018] 3 LNS 15, expert intervention by CyberSecurity Malaysia was pivotal in authenticating an audio recording submitted as evidence. These precedents illustrate the pressing need for systematic reforms to embed digital forensic tools within Syariah evidentiary practice.

In summary, digital forensic tools are indispensable in authenticating electronic documents within the Syariah judicial system. They bridge the divide between technological innovation and the normative framework of Islamic legal reasoning, ensuring that evidence is both scientifically valid and legally sound. While practical limitations—such as costs, procedural gaps, and technical training—remain obstacles, these tools must be institutionalised within the evidentiary framework of Syariah law. This can be achieved through the adoption of formal guidelines, capacity-building initiatives for judges, prosecutors, and enforcement officers, and strategic partnerships with expert institutions such as CyberSecurity Malaysia, SIRIM QAS International, and the Malaysian Communications and Multimedia Commission (MCMC). Such measures would significantly enhance electronic evidence's credibility, transparency, and probative value in Syariah proceedings.

Issues, Challenges, and Recommendations for Strengthening Digital Forensics in the Authentication of Electronic Documents in the Syariah Court

As previously discussed, the application of digital forensics plays a vital role in ensuring the authenticity and reliability of electronic evidence. Nevertheless, several critical issues and challenges hinder its effective implementation within the Syariah legal framework.

The first major challenge lies in the absence of a Standard Operating Procedure (SOP) specifically designed for handling digital evidence. Unlike the Civil Courts, which operate under established provisions in the Evidence Act 1950 [Act 56]—particularly Sections 90A to 90C—the Syariah Courts lack a unified procedural reference governing the collection, storage, and presentation of electronic evidence. This deficiency has resulted in inconsistent practices across different states and has opened the door for defence counsel to contest the authenticity and integrity of submitted evidence (Wan Ismail et al., 2023).

Secondly, Syariah judges, prosecutors, and religious enforcement officers face a significant lack of technical expertise (Tuan Ibrahim et al., 2025; Yahya et al., 2024). Most of these legal actors are trained primarily in Syariah or law and are seldom exposed to digital forensics or computer science complexities. This knowledge gap makes it difficult for them to fully comprehend technical reports, such as metadata analyses or cryptographic hash results, thereby limiting the courts' ability to accurately evaluate electronic evidence's probative value. This limitation is particularly evident in cybercrime cases involving online gambling, the dissemination of deviant teachings through digital platforms, and religious defamation committed via social media.

The third challenge concerns the risks of data manipulation, privacy breaches, and ethical issues. Electronic documents can be altered using editing software or deepfake technology without leaving obvious traces. In some circumstances, litigants' personal data may also be exposed if robust data protection mechanisms are not implemented. Such vulnerabilities not only compromise evidentiary integrity but also risk infringing upon fundamental rights protected under the *maqāṣid al-sharīʿah*, particularly the preservation of dignity (*ḥifẓ al-ʿirḍ*) and the protection of information (*ḥifẓ al-maʿlūmāt*).

Recommendations for Legal Reform

In response to these challenges, several reform measures are proposed. First, a dedicated SOP on digital evidence should be developed for the Syariah Courts. This SOP should be formalised as a Practice Direction issued by the Department of Syariah Judiciary Malaysia (JKSM) to ensure consistent nationwide application. It should prescribe clear procedures for collecting digital evidence, documentation of the chain of custody, and authentication methods using scientific tools such as cryptographic hash functions and blockchain systems.

Second, capacity-building initiatives through structured technical training are indispensable. Judges, prosecutors, and religious enforcement officers must be equipped with digital forensics fundamentals to interpret technical reports accurately. Such training should be carried out in collaboration with expert agencies, including CyberSecurity Malaysia, SIRIM QAS International, and the Malaysian Communications and Multimedia Commission (MCMC). These collaborations would strengthen technical competency and align Syariah Courts with international best practices in digital evidence management.

Third, data protection and ethical safeguards must be given priority. The Syariah judiciary could adopt established international standards, such as ISO/IEC 27001 on information security, to safeguard litigants' personal data strictly. The SOP or Practice Direction should also incorporate specific privacy provisions to prevent data leaks during investigation and trial.

Finally, a long-term strategic measure involves the establishment of a dedicated Syariah digital forensics ecosystem. This may include creating specialised forensic units within State Islamic Religious Departments (JAIN) and the development of accredited digital forensic laboratories for Syariah-related cases. Such infrastructure would reduce overreliance on external agencies while equipping the Syariah judiciary with in-house scientific capacity to authenticate digital evidence with greater credibility.

Taken together, these reforms will not only address existing gaps in the management of electronic evidence but also ensure that the Syariah judiciary evolves in step with technological advancements. Ultimately, the institutionalisation of digital forensics within the Syariah legal framework will reinforce judicial outcomes' credibility, integrity, and transparency in an increasingly digital era.

Conclusion

In conclusion, integrating digital forensics into Syariah court proceedings is critical to ensure that electronic evidence is lawfully admissible, credible, and resistant to manipulation. Despite existing gaps—such as the absence of standardised SOPs, limited technical expertise, and unresolved data integrity and privacy concerns—digital forensics offers a scientifically grounded mechanism capable of safeguarding the authenticity and reliability of electronic documents. By developing specific guidelines, providing continuous technical training, and establishing institutional partnerships with relevant agencies, the Syariah Court is well-positioned to enhance the credibility of its judicial determinations. These efforts are consistent with the higher objectives of *maqāṣid al-sharīʿah*, which emphasise justice, the protection of rights, and legal certainty in an increasingly digitalised world.

References

Ab Rahman, R. (2021, February 26). *“Beza tandatangan digital dengan elektronik dalam menentusahkan identiti penandatangan dokumen”.* Astro Awani. https://www.astroawani.com/berita-malaysia/beza-tandatangan-digital-dengan-elektronik-dalam-menentusahkan-identiti-penandatangan-dokumen-284822

Alias, M. A. A., Mohd Jailani, M. R., Wan Ismail, W. A. F., & Baharuddin, A. S. (2024b). The integration of five main goals of Shariah in the production of science and technology for human well-being. *AL-MAQASID: The International Journal of Maqasid Studies and Advanced Islamic Research, 5*(1), 1–16. https://doi.org/10.55265/al-maqasid.v5i1.79

Alias, M. A. A., Wan Ismail, W. A. F., Baharuddin, A. S., & Mallow, M. S.(2024a). 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.

Alias, M. A. A., Wan Ismail, W. A. F., Baharuddin, A. S., Hashim, H., & Tuan Ibrahim, T. M. F. H. (2024). Evaluating electronic evidence in Malaysian Civil Courts: Current admissibility and future legal directions. In Proceeding of *the International Conference on Syariah, Law and Science (CFORSJ I-CONF),* (pp. 13-21).

Aljamos, Y. M., Mohd Noor, A., Mohd Aswadi, M. S., & Baharuddin, A. S. (2022). *The blockchain technology from maqasid shari’ah perspective*. *Journal of Current Media Studies (JCMS)*, 1(2), 59–82. https://doi.org/10.52100/jcms.v1i2.54

Alsadi, N. (2025). *“The convergence of blockchain technology and Islamic economics: Decentralized solutions for Shariah-compliant finance”*. arXiv. https://doi.org/10.48550/arXiv.2501.02263

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

Carrier, B., & Spafford, E. H. (2003). Getting physical with the digital investigation process. *International Journal of Digital Evidence*, 2(2), 1–20.

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

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

Metwally, M. (2019). Forensic organizational psychology: Shedding light on the positive repercussions of ethical leadership in forensic medicine. *Egyptian Journal of Forensic Sciences, 9*(1), 1-8.

Mohaiyadin, N. M. H., Aman, A., Palil, M. R., & Said, S. M. (2022). Addressing accountability and transparency challenges in waqf management using blockchain technology. *Journal of Islamic Monetary Economics and Finance, 8*, 53–80. https://doi.org/10.21098/jimf.v8i0.1413

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. https://doi.org/10.35631/ijlgc.4150013

Mustapa Sa’di, M., Kamarudin, A. R., Mohamed, D., & Ramlee, Z. (2015). Authentication of electronic evidence in cybercrime cases based on Malaysian laws. *Pertanika Journals Social Sciences and Humanities, 23*(S), 153-168.

Nelson, B., Phillips, A., & Steuart, C. (2019). *Guide to Computer Forensics and Investigations* (6th ed.). Cengage Learning.

TG Team. (2015). *“Meaning of word forensic/forensic science & origin”*. Tax Guru. https://taxguru.in/chartered-accountant/meaning-word-forensicforensicscience-

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.

Wan Ismail, W. A. F., Abdul Mutalib, L., Baharuddin , A. S., Abdullah Kahar, N. S., & Alias, M. A. A. (2023). Keperluan Prosedur operasi standard dalam penerimaan dokumen digital di mahkamah sivil Malaysia. *UUM Journal of Legal Studies, 14*(1), 365–390. https://doi.org/10.32890/uumjls2023.14.1.14

Yahya, A., M. 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. (2021). Kebolehterimaan keterangan dokumen elektronik di mahkamah syariah: Analisis permasalahan dan penyelesaiannya. In *Proceedings of the International Conference on Syariah & Law 2021 (ICONSYAL 2021) – Online Conference* (pp. 704–713). Universiti Sains Islam Malaysia.

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