Vol. 3, No. 1, pp. 128-135 | 2025
CFORSJ Procedia

STRENGTHENING THE INTEGRITY OF DIGITAL EVIDENCE IN SYARIAH CRIMINAL PROCEEDINGS: A FORENSIC–LEGAL ANALYSIS OF THE CHAIN OF CUSTODY (CoC)

[i,*]Mohamad Aniq Aiman Alias, [i,ii]Wan Abdul Fattah Wan Ismail, [i,ii,iii]Ahmad Syukran Baharuddin, [i,ii]Hasnizam Hashim & [iv]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]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
[iii]Research Fellow, Maqasid Institute, United States of America (USA)
[iv]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

ABSTRACT

The rapid development of digital technology has significantly transformed the methods of collecting, managing, and evaluating evidence in Syariah criminal proceedings in Malaysia. Electronic evidence—such as messages, digital images, CCTV recordings, metadata, and communication logs—has become an increasingly primary source in the investigation and prosecution of Syariah offences. However, its volatile, easily altered, and highly manipulable nature raises serious concerns regarding authenticity, reliability, and overall evidentiary integrity. The absence of specific statutory provisions on digital evidence under the Syariah Court Evidence Act 1997 [Act 561] further creates a regulatory gap that heightens the potential for *shubuhāt* (doubt) during the evidentiary process. This article examines how the Chain of Custody (CoC) for digital evidence can serve as an effective forensic–legal framework to enhance the integrity of electronic evidence in Syariah criminal proceedings. Employing a qualitative approach through doctrinal analysis of legal documents and related literature, the study organises its findings according to key analytical themes. The results indicate that the CoC provides a robust scientific and procedural foundation to ensure that digital evidence is handled transparently, accountably, and free from risks of manipulation. The principles underpinning the CoC also align with the Syariah requirements of *thubut* (certainty of proof), *amanah* (proper preservation and stewardship of evidence), and *'adl* (justice), thereby making it a relevant mechanism for enhancing the admissibility and probative strength of digital evidence before the Syariah courts. This study contributes to strengthening the evidentiary framework in Syariah law by offering a scientific, forensic, and legal basis for more organised, consistent, and integrity-focused management of digital evidence. The findings further open avenues for the development of Syariah Digital Evidence Guidelines, capacity-building in digital forensic skills among enforcement officers and prosecutors, and further research into automated evidence management mechanisms within the Syariah judicial ecosystem.

Keywords: *Digital evidence, syariah criminal proceedings, forensic, chain of custody (CoC), integrity*

Introduction

Digital transformation has significantly reshaped the landscape of criminal justice worldwide, including within the Malaysian Syariah legal system (Alias et al., 2021). As communication, social interaction, and daily activities increasingly depend on digital platforms, electronic information has become a crucial source of proof in criminal cases. Digital materials—including text messages, call logs, metadata, CCTV recordings, and mobile device extractions—now form an integral part of investigations involving offences such as *khalwat*, *zinā*, falsification of marriage-related documents, cyber-related misconduct, and other Syariah criminal matters (Tuan Ibrahim et al., 2025). Given this growing reliance on electronic material, understanding the nature, vulnerabilities, and legal implications of digital evidence has become critically important.

Digital evidence differs fundamentally from physical evidence, presenting unique challenges to the integrity of evidence (Nath et al., 2024). Its volatility, susceptibility to alteration, and ease of duplication increase the risk of manipulation—whether intentional or accidental—thereby raising serious concerns about authenticity, reliability, and forensic soundness. Within Syariah criminal proceedings, these concerns are compounded by the absence of explicit statutory provisions governing electronic evidence under the Syariah Court Evidence Act 1997 [Act 561]. As a result, the probative reliability of screenshots, digital documents, device artefacts, and electronic communications is frequently scrutinised. Without proper procedural safeguards, digital evidence becomes vulnerable to *shubuhāt* (doubt), undermining its evidentiary value and threatening the standard of *thubut* (certainty) required for criminal adjudication.

Against this backdrop, this article examines the application of the chain of custody (CoC) as a forensic–legal framework for safeguarding the integrity of digital evidence in Syariah criminal proceedings. Specifically, it analyses the conceptual foundations and operational significance of the CoC, outlines five forensic stages through which the digital CoC may be implemented, and assesses the extent to which international standards—such as ISO/IEC 27037, the NIST guidelines, the ACPO Principles, and SWGDE best practices—can be meaningfully adapted to the Syariah context. The article then proposes practical recommendations for strengthening digital evidence governance and identifies key avenues for future research. Through this approach, the study aims to contribute to a more credible, consistent, and principled framework for managing digital evidence within Malaysia's Syariah criminal justice system.

Digital Evidence in Syariah Criminal Proceedings: Nature, Characteristics, and Key Evidentiary Challenges

Digital evidence refers to any information of probative value that is stored, transmitted, or generated in digital form (Stoykova, 2021). It encompasses a wide range of materials, including text messages, call logs, social media communications, CCTV recordings, digital photographs, device-generated metadata, geolocation information, and files extracted from computers, mobile phones, and other networked devices (Alias et al., 2024). Unlike conventional physical evidence, digital evidence is encoded in electronic signals and binary data structures, making it heavily dependent on technological processes for its identification, extraction, preservation, and interpretation. In contemporary Syariah criminal proceedings—particularly in cases involving *khalwat*, *zina*, falsification of marriage-related documents, child-related disputes, and cyber-enabled offences—digital evidence increasingly constitutes a key component of investigative and prosecutorial strategies.

The inherent characteristics of digital evidence pose distinctive challenges to evidentiary integrity. First, digital evidence is volatile, meaning that electronic data can be altered, overwritten, or destroyed through routine device operations, system shutdowns, automatic background processes, or environmental factors (Watson & Jones, 2013). Second, it is highly susceptible to alteration, either unintentionally—through syncing, software updates, cloud backup processes, or user interaction—or intentionally through tampering, fabrication, or deletion (Aubin, 2025). Third, digital evidence is infinitely duplicable, making it difficult to distinguish between original and duplicate copies without the application of forensic validation mechanisms such as hashing, metadata comparison, and auditable verification processes (Narasimhan & Kala, 2024). These characteristics necessitate the use of

scientifically recognised forensic procedures in acquiring, preserving, analysing, and presenting digital evidence to ensure its reliability and admissibility.

Given these vulnerabilities, Syariah courts require stricter integrity controls compared to traditional physical evidence. The absence of inherent physical uniqueness, combined with the ease of manipulation, means that digital evidence cannot be authenticated solely through visual inspection or testimonial assertion. Its probative value depends heavily on the consistent application of forensic procedures—such as bit-stream imaging, hash verification, secure storage environments, and controlled access protocols—at every stage from identification to presentation in court. Failure to adhere to these procedures increases the risk of *shubuhāt* (doubt), thereby undermining the evidentiary weight of digital materials and jeopardising the administration of justice.

Strengthening digital evidence management within the Syariah legal framework is, therefore, both essential and unavoidable. Implementing a forensic-informed CoC ensures that electronic materials presented in court possess a verifiable lineage, remain demonstrably unaltered, and can withstand judicial scrutiny. Such a degree of integrity aligns closely with foundational Islamic evidentiary principles, including *thubut* (certainty), *amanah* (trustworthiness), and *ḥaqq* (truth), thereby supporting fair, accurate, and just adjudication in Syariah criminal cases (Alias et al., 2024b). The next section will elaborate on the concept, function, and legal significance of the CoC as the principal mechanism for safeguarding the integrity of digital evidence.

Chain of Custody (CoC) for Digital Evidence: Concepts, Legal Foundations, and Its Significance in Syariah Evidentiary Practice

The CoC serves as a procedural regulatory mechanism that ensures electronic evidence remains protected from contamination, alteration, manipulation, or unauthorised access throughout the processes of collection, storage, analysis, and presentation in court (Yahya et al., 2023). In the context of digital evidence, this requirement is increasingly critical due to the inherently volatile nature of electronic data, which can be easily modified, duplicated, or destroyed without detection. Accordingly, the CoC requires that each stage of evidence handling be recorded meticulously, systematically, and continuously to preserve its integrity and probative value.

The need for comprehensive documentation is consistent with the general principles of the chain of custody and the chain of evidence that have long been applied within civil evidentiary law. As explained by Ahmad Azam et al. (2022), the chain of custody is an evidentiary principle that requires strict control over access to and movement of evidence—whether physical or electronic—from the moment it is first obtained until it is tendered in court. This approach is essential to ensure that the integrity and evidential strength of the material remain intact throughout its handling.

Although the principle is widely recognised and applied in civil and criminal proceedings in Malaysia's civil courts, Syariah legal provisions in Malaysia have yet to expressly recognise the CoC under the Syariah Court Evidence Enactments (Yahya et al., 2024). This legislative gap necessitates greater diligence in maintaining a strict and coherent CoC, particularly for digital evidence such as messages, images, metadata, audio-visual recordings, and other electronic documents. Failure to establish a complete and unbroken CoC may give rise to *shubuhāt* (doubt), weaken the evidentiary value of *qarīnah*, and allow the defence to challenge the authenticity or integrity of the evidence (Alias et al., 2024a).

A robust CoC must, at a minimum, document:

i. The identity of each individual who handled the evidence;

ii. The date, time, and location of each action involving the evidence;

iii. The forensic methods or software used;

iv. The physical or digital storage locations;

v. The cryptographic hash values verifying the evidence remain unchanged; and

vi. A complete record of every transfer, access, or analysis performed.

In Syariah evidentiary practice, the CoC is not merely a technical requirement but has a firm grounding in Islamic principles of proof. Tuan Ibrahim et al., (2025) emphasise that the chain of custody and the chain of evidence do not conflict with Syariah but instead align with its core demands of justice, trustworthiness, and evidentiary certainty. The principle of *thubut* (certainty) requires that evidence be free from doubt; *amanah* (trustworthiness) necessitates integrity and transparency in evidence management; while *'adl* (justice) obligates judges and prosecutors to ensure that evidence presented is untainted, as compromised evidence may result in unjust or erroneous judgments.

Moreover, the maintenance of an unbroken evidentiary chain is also recognised within the classical fiqh tradition as a form of *qarīnah qawiyyah* (strong circumstantial indication) supporting the credibility of information, as elaborated by scholars such as Ibn Qayyim. This cautious approach is consistent with the Qur'anic injunction to verify information from uncertain sources. Allah the Almighty says:

> Translation: O believers, if an evildoer brings you any news, verify it, lest you harm people unknowingly and become regretful for what you have done.
>
> (Surah al-Hujurāt, 49:6)

Ibn Kathīr interprets this verse as a command to verify reports from a *fāsiq* (unreliable source) thoroughly, exercising caution to avoid falsehood and confusion. Early exegetes note that this verse was revealed concerning al-Walīd ibn 'Uqbah, who was sent as an emissary by the Prophet to collect *zakāt* from Banu Mustaliq (Tafsīr al-Qur'ān al-'Azīm, 4/264). Imām al-Shawkānī adds that *tabayyun* refers to careful verification. At the same time, *tasabbut* denotes deliberate caution and the avoidance of haste, requiring deep reflection on information until it becomes clear and certain.

This verse indirectly illustrates that the CoC not only fulfils modern procedural requirements but is also deeply consistent with the *fiqhī* and ethical foundations of Syariah. Mohd Kamil et al., (2024) further assert that the chain of custody and chain of evidence should be recognised as legitimate components of Syariah evidentiary practice and applied consistently across Syariah court proceedings to ensure that *qarīnah* presented is credible and aligned with the principle of justice.

In essence, the chain of custody represents an essential foundation for ensuring that digital evidence remains intact, authentic, and evidentially reliable. Its implementation closes avenues for manipulation or doubt, strengthens the integrity of electronic evidence, and guarantees that the evidentiary process in Syariah courts adheres to the overarching principles of justice, trustworthiness, and certainty.

The Forensic Stages for Operationalising the Digital Chain of Custody in Syariah Criminal Proceedings: A Preliminary Proposal

Grounded in the conceptual foundations of the CoC and the Syariah principles of *thubut* (certainty), *amanah* (trustworthiness), and *'adl* (justice), the operationalisation of the digital CoC in Syariah criminal proceedings must be structured through clearly defined forensic stages. Although these technical frameworks originate from international standards, their underlying principles—integrity, transparency, traceability, and preservation—are entirely consistent with Islamic legal thought and the requirement that evidence be free from *shubuhāt* (doubt).

Internationally recognised standards, such as ISO/IEC 27037, NIST SP 800-86, NIST SP 800-101, the ACPO Principles, and SWGDE Best Practices, provide a reliable technical foundation for constructing a model of digital evidence management that ensures authenticity, reliability, and admissibility in line with Syariah evidentiary requirements. Contemporary digital forensic literature also emphasises that the CoC must be comprehensive, unbroken, and verifiable throughout the entire lifecycle of digital evidence.

In line with these principles, the following five stages form a suitable operational model for implementing the digital CoC within Syariah criminal proceedings:

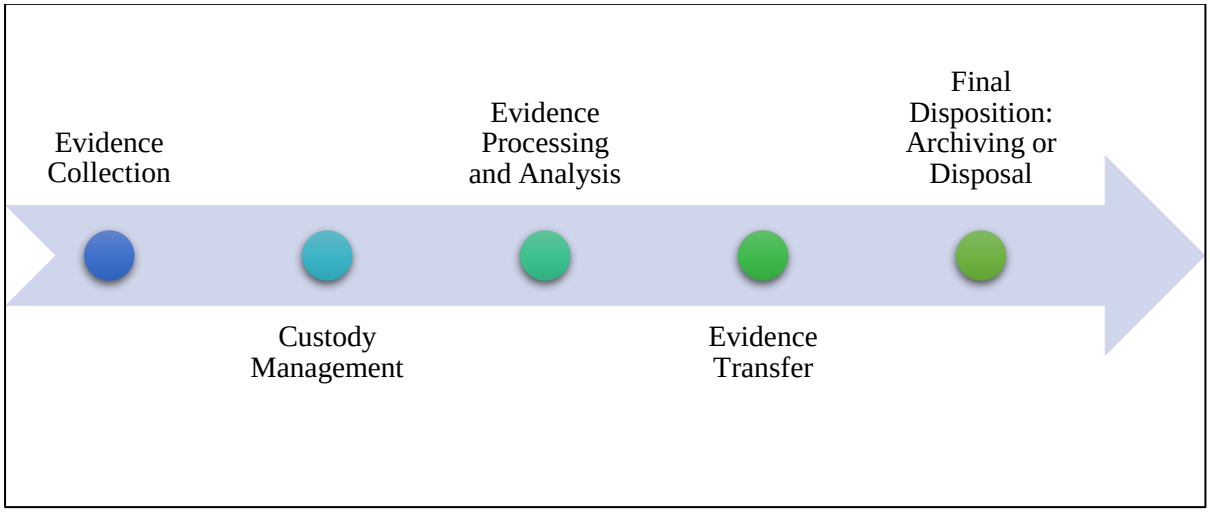

Figure 1. Proposed Forensic Stages for Operationalising the Digital Chain of Custody in Syariah Criminal Proceedings

Evidence Collection

The first stage involves identifying, collecting, and acquiring digital data using scientifically validated techniques, including bit-stream imaging, cryptographic hashing (e.g., SHA-256/SHA-512), and metadata preservation. ISO/IEC 27037 underscores that acquisition must be performed without altering the original data, while cryptographic hash values serve as technical proof that no modification has occurred. In the Syariah context, adherence to these procedures fulfils the requirement of *thubut*, ensuring the authenticity of evidence from the very beginning of its lifecycle.

Custody Management

Following the acquisition, digital evidence must be secured through a structured storage and handling system. The ACPO Principles and SWGDE guidelines emphasise the need for complete documentation detailing who handled the evidence, when it was accessed, for what purpose, and under what storage conditions. Security mechanisms—such as encryption, controlled access, and non-erasable audit logs—further reinforce evidentiary integrity. From a Syariah perspective, this stage reflects the principle of *amanah*, ensuring that evidence is not compromised or mismanaged at any point.

Evidence Processing and Analysis

This stage involves examining and analysing digital artefacts using validated forensic tools, such as EnCase, FTK, and Autopsy. All analysis must be conducted on forensic copies rather than on the original media to prevent inadvertent alteration. International standards require detailed documentation of each analytical step, including the technical parameters used, software versions, changes in hash values, and the resulting artefacts identified. This level of documentation reduces *shubuhāt* and strengthens the probative value of the evidence before the Syariah court.

Evidence Transfer

Any transfer of digital evidence—whether to another investigator, a forensic examiner, the prosecution, or court officials—must be strictly recorded. Records must include the time of transfer, the personnel involved, the reason for the transfer, and the method used for the transfer. Careful control over this process prevents breaks in the evidentiary chain and ensures that evidence reaches the court in a valid and uncontaminated condition. This corresponds to the principle of *'adl*, guaranteeing fairness and transparency in evidentiary procedures.

Final Disposition: Archiving or Disposal

The final stage concerns either the long-term preservation of digital evidence for appeal or review purposes or its secure disposal. Standards such as NIST SP 800-86 recommend monitored long-term storage, periodic verification of hash integrity, and secure disposal methods, including cryptographic

erasure. From the perspective of *maqāṣid al-sharī'ah*, the preservation of evidence for judicial review aligns with *ḥifẓ al-ḥuqūq*—the protection of rights and justice.

Collectively, these five stages constitute a comprehensive operational model for the digital CoC that aligns with both contemporary forensic best practices and Syariah evidentiary doctrine. When systematically adapted and applied, this model ensures that all digital evidence submitted before the Syariah court is authentic, reliable, and free from doubt—thereby fulfilling the standard of *qarīnah qawiyyah* in Islamic law and strengthening the administration of justice in Syariah criminal proceedings.

Recommendations and Future Directions

Strengthening the governance of digital evidence within Malaysia's Syariah criminal justice system requires a series of coordinated and forward-looking reforms grounded in both forensic best practices and Islamic legal principles. A key priority is the development of comprehensive Syariah Digital Evidence Guidelines that can be applied uniformly across all states. These guidelines should draw upon internationally recognised digital forensic standards—such as ISO/IEC 27037, NIST SP 800-86, NIST SP 800-101, and the ACPO Good Practice Guide for Digital Evidence—while being adapted to the core evidentiary doctrines of *thubut* (certainty), *amanah* (trustworthiness), and *'adl* (justice). A clearly delineated guideline framework would outline scientifically sound procedures for the acquisition, preservation, analysis, transfer, and long-term storage of digital evidence. The establishment of such a framework would promote procedural uniformity, reduce inconsistencies between states, strengthen the reliability of electronic materials submitted in court, and provide an authoritative reference for Syariah enforcement officers, prosecutors, and judges.

Parallel to the need for standardised guidelines is the necessity of enhancing the technical competence of Syariah enforcement agencies. With digital evidence becoming increasingly central in modern investigations, enforcement officers must acquire both conceptual understanding and operational expertise in digital forensics. Training initiatives should therefore encompass the foundational principles of digital evidence handling, the practical implementation of the Chain of Custody (CoC), validated forensic acquisition methodologies, and the thorough documentation techniques required to establish authenticity and integrity. Collaboration with national technical and regulatory institutions such as CyberSecurity Malaysia, SIRIM, and the Malaysian Communications and Multimedia Commission (MCMC), as well as with academic institutions, would ensure that training modules reflect contemporary forensic advancements and regulatory expectations. Enhancing technical competence is crucial not only to ensure accurate and consistent implementation of CoC procedures but also to minimise *shubuhāt* (doubts) surrounding the reliability of evidence presented before Syariah courts.

Beyond capacity-building measures, the development of an automated CoC system represents an important structural reform in digital evidence management. Such a system should incorporate tamper-evident audit logs, secure documentation of hash values, authenticated records of evidence movement, and encrypted repositories with controlled access. The integration of emerging technologies—such as blockchain—has the potential to enhance traceability, immutability, and transparency, thereby providing judges and prosecutors with a verifiable and trustworthy evidentiary trail. By reducing the likelihood of human error, improving procedural clarity, and expediting investigative and judicial processes, an automated CoC system would support the Syariah judiciary's commitment to certainty, fairness, and evidentiary integrity.

Looking ahead, various opportunities for future research may enrich the development of a robust digital evidence framework for the Syariah criminal justice system. Empirical studies could examine the current implementation of CoC-related practices within Syariah enforcement agencies, identifying gaps, operational constraints, and variations in compliance across regions. Comparative legal studies may explore how other Muslim-majority jurisdictions—such as Indonesia, Brunei, Jordan, and the United Arab Emirates—regulate and evaluate digital evidence in Syariah judicial settings, offering potential models that may inform local reforms. Technical research, on the other hand, could investigate the feasibility of blockchain-based evidentiary registries, artificial intelligence-assisted authenticity verification tools, and immutable digital storage architectures as advanced mechanisms to support evidentiary certainty. Collectively, these avenues of inquiry would help harmonise technological innovation with the *maqāṣid al-sharī'ah*, particularly the preservation of truth, justice, and individual

rights, thereby contributing to a more credible, consistent, and future-ready digital evidence governance framework for the Syariah criminal justice system.

Conclusion

As a conclusion, this article has examined the nature of digital evidence and demonstrated why its distinctive characteristics—volatility, susceptibility to alteration, and infinite replicability—necessitate evidentiary safeguards far more stringent than those applied to conventional physical exhibits. Within Syariah criminal proceedings, these vulnerabilities heighten the risk of *shubuhāt* (doubt), making it insufficient for courts to rely solely on visual inspection, oral testimony, or traditional evidentiary presumptions. A structured, forensic-informed CoC is therefore indispensable to ensuring that digital evidence remains authentic, reliable, and legally admissible throughout its lifecycle. The analysis of the five proposed forensic stages—evidence collection, custody management, processing, transfer, and final disposition—demonstrates how internationally recognised standards, such as ISO/IEC 27037, the NIST guidelines, ACPO principles, and SWGDE best practices, can be meaningfully operationalised within the Syariah criminal justice framework. These standards not only reinforce the technical integrity of electronic evidence but also align with fundamental Islamic evidentiary doctrines: *thubut* (certainty of proof), *amanah* (trustworthiness), and *'adl* (justice). Their integration enhances procedural transparency, reduces the potential for evidentiary disputes, and promotes greater consistency across jurisdictions in the management of digital evidence.

This study contributes to closing the methodological gap between modern forensic science and Islamic legal principles by proposing a structured digital CoC model tailored for Syariah criminal cases. The findings underscore the pressing need for the development of national Syariah Digital Evidence Guidelines, the enhancement of technical competence among enforcement and prosecutorial personnel through specialised digital forensics training, and the establishment of automated CoC systems capable of producing tamper-evident and auditable records. Collectively, these measures form a practical, coherent, and future-oriented roadmap for strengthening evidentiary reliability and upholding the integrity of Syariah adjudication. Future research should examine the actual implementation of CoC-related practices within Syariah enforcement agencies, analyse comparative models from other Muslim-majority jurisdictions that have formalised digital evidence frameworks, and investigate emerging technological solutions—including blockchain-based audit trails, AI-assisted authenticity verification, and immutable evidence storage architectures. As digital evidence increasingly shapes modern investigations and prosecutions, establishing a robust, principled, and forensically sound regulatory framework is essential to safeguard rights, ensure justice, and reinforce public confidence in the Syariah criminal justice system.

References

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.(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., 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

Aubin, M. (2025, July 17). *"Types of digital evidence"*. https://srecon.com/types-of-digital-evidence/

Mohd Kamil, K. M., Yahya, M. A., Mohd Arif, M. I. A., Mohd Shariff, A. A., Hassan@Yahya, M. S., & Adenan, F. (2025). Application of qarinah and cyber document evidence in deviant teaching cases: Aplikasi qarinah dan keterangan dokumen siber dalam kes ajaran sesat. *Al-Qanatir:*

International Journal of Islamic Studies, *34*(04), 15–24. https://doi.org/10.64757/alqanatir.2025.3404/1234

Mohd Shariff, A. A., Yahya, M. A., Tzu-Hsin, M. H., Mohd Subki, M. M., Azahari, N. F., Raja, J., & Muhamad, S. S. (2022). Prinsip rantaian jagaan dan rantaian keterangan: Keperluan kepada pengiktirafan dan pengaplikasian dalam kes syariah di Malaysia. *Journal of Muwafaqat*, *5*(1), 17-32.

Narasimhan, P. & Kala, N. (2024). Ensuring the integrity of digital evidence: The role of the chain of custody in digital forensics. *International Journal of Scientific Research in Computer Science, Engineering and Information Technology*, *10*(6), 2438-2450.

Nath, S., Summers, K., Baek, J., & Ahn, G. J. (2024). Digital evidence chain of custody: Navigating new realities of digital forensics. In *Proceedings of IEEE International Conference on Trust, Privacy and Security in Intelligent Systems, and Applications*, (pp. 11-20).

Stoykova, R. (2021). Digital evidence: Unaddressed threats to fairness and the presumption of innocence. *Computer Law & Security Review*, *42*, 1–20. https://doi.org/10.1016/j.clsr.2021.105575

Tuan Ibrahim, T. M. F. H., Alias, M. A. A., Nor Muhamad, N. H., & Baharuddin, A. S. (2025). Pembuktian forensik digital di mahkamah syariah: Kerangka kebolehterimaan dan integriti dalam jenayah syariah: Digital forensics in the shariah court: Framework of evidentiary admissibility and integrity in syariah criminal law. *Journal of Muwafaqat*, *8*(2), 78–100. https://doi.org/10.53840/muwafaqat.v8i2.197

Watson, D., & Jones, A. (2013). *Digital forensics processing and procedures*. Elsevier.

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

Yahya, 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*, 145-166.