CFORSJ
Centre of Research for
Fiqh Forensics and Judiciary

Vol. 3, No. 1, pp. 229-237 | 2025
CFORSJ Procedia

THE ROLE OF RELIGIOUS ENFORCEMENT OFFICERS AS DIGITAL EVIDENCE FIRST RESPONDERS (DEFRs) IN SYARIAH CRIMINAL INVESTIGATIONS: A PRELIMINARY REVIEW

PERANAN PEGAWAI PENGUATKUASA AGAMA SEBAGAI *DIGITAL EVIDENCE FIRST RESPONDERS* (DEFRs) DALAM SIASATAN JENAYAH SYARIAH: SUATU TINJAUAN AWAL

[i,*]Tuan Muhammad Faris Hamzi Tuan Ibrahim, [i]Nasrul Hisyam Nor Muhamad, [ii,iii,iv]Ahmad Syukran Baharuddin, [ii]Mohamad Aniq Aiman Alias

[i]Islamic Civilization Academy, Faculty Sciences Social and Humanities, Universiti Teknologi Malaysia, 81310, Johor Bahru, Johor, Malaysia
[ii]Faculty of Syariah and Law, Universiti Sains Islam Malaysia, 71800 Nilai, Negeri Sembilan, Malaysia
[iii] Research Fellow, Maqasid Institute, United States of America.
[iv] Centre of Research for Fiqh Forensics and Judiciary (CFORSJ), Faculty of Syariah and Law, Universiti Sains Islam Malaysia, 71800, Nilai, Negeri Sembilan, Malaysia

*(Corresponding author) e-mail: tuan00@graduate.utm.my

ABSTRACT

The rapid development of digital technology has led to the emergence of cyber-based Syariah offences such as online gambling and the dissemination of deviant teachings, which increasingly rely on evidence derived from electronic devices and digital artefacts, including metadata, IP logs, and transaction records. This shift necessitates strict preservation of the chain of custody to ensure that digital evidence remains authentic, intact, and admissible in court. However, the study finds that the role of the Digital Evidence First Responder (DEFR), as outlined in international standards such as ISO/IEC 27037:2012, has not yet been fully institutionalised within Syariah enforcement in Malaysia. Religious Enforcement Officers (REOs), as the first individuals to interact with digital evidence, often operate without specialised guidelines, adequate technical training, or appropriate forensic infrastructure, creating risks of evidence contamination, incomplete documentation, and weaknesses in the chain of custody. From the Syariah perspective, the emphasis on precise documentation, the prohibition against falsifying testimony, and the obligations of amānah and ʿadl as articulated in the Qur'an reinforce the necessity of safeguarding the integrity of digital evidence. This study asserts the need for formal recognition of the DEFR role among REOs, the implementation of comprehensive forensic training, the establishment of dedicated digital evidence management units, and legal reforms to ensure that the Syariah criminal justice system is capable of addressing contemporary digital challenges effectively and with integrity.

Keywords: *Chain of Custody, Digital Forensics, Religious Enforcement Officers, Digital Evidence First Responders, Syariah Cybercrime, Evidentiary Integrity*

ABSTRAK

Perkembangan pesat teknologi digital telah menyebabkan kewujudan jenayah Syariah berasaskan siber seperti perjudian dalam talian dan penyebaran ajaran sesat yang semakin bergantung kepada keterangan yang melibatkan peranti elektronik dan artifak digital seperti metadata, log IP dan rekod transaksi. Perubahan ini memerlukan pemeliharaan ketat terhadap rantaian jagaan keterangan bagi memastikan bukti digital kekal tulen, lengkap dan boleh diterima di mahkamah. Namun, kajian mendapati bahawa peranan Digital Evidence First Responder (DEFR) sebagaimana digariskan oleh piawaian antarabangsa seperti ISO/IEC 27037:2012 masih belum diinstitusikan sepenuhnya dalam penguatkuasaan Syariah di Malaysia. Pegawai Penguatkuasa Agama (PPA) sebagai pihak pertama yang berinteraksi dengan bukti digital sering beroperasi tanpa garis panduan khusus, latihan teknikal mencukupi atau infrastruktur forensik yang sesuai sehingga boleh mewujudkan risiko pencemaran bukti, dokumentasi tidak lengkap dan kelemahan rantaian jagaan. Dari perspektif Syariah, tuntutan terhadap dokumentasi tepat, larangan memalsukan keterangan serta kewajipan *amānah* dan *ʿadl* sebagaimana ditegaskan dalam al-Qur'an memperkukuhkan keperluan pemeliharaan integriti bukti digital. Kajian ini menegaskan terdapat keperluan pengiktirafan rasmi peranan DEFR dalam kalangan PPA, pelaksanaan latihan forensik secara menyeluruh, penubuhan unit pengurusan bukti digital dan pembaharuan undang-undang bagi memastikan sistem keadilan jenayah Syariah mampu menangani cabaran digital kontemporari dengan berkesan dan berintegriti.

Kata Kunci: *Rantaian Jagaan, Forensik Digital, Pegawai Penguatkuasa Agama, Digital Evidence First Responders, Jenayah Siber Syariah, Integriti Keterangan*

Introduction

The exponential growth of digital technology has fundamentally redefined the character of modern criminality, giving rise to two major categories of offences: cyber-dependent and cyber-enabled crimes (Whitty & Young, 2025). Cyber-dependent crimes such as hacking, malware attacks and unauthorised system access exist solely because of the internet and cannot occur without it. In contrast, cyber-enabled crimes represent conventional offences that have been reconfigured through digital means, including fraud, gambling, pornography, and the dissemination of deviant religious teachings. Within Malaysia's Syariah legal context, this digital convergence has expanded the domain of al-maysir (gambling) and adeviation into online environments which make them more complex, transboundary, and less visible to traditional enforcement mechanisms (Tuan Ibrahim et al., 2025b).

This transformation challenges the classical evidentiary model of Islamic criminal law, which primarily relies on iqrār (confession), shahādah (eyewitness testimony), and qarīnah (circumstantial evidence). In the digital domain, such evidence is often replaced by intangible artefacts like metadata, IP logs, chat histories, encrypted messages, and transaction records that are volatile and susceptible to manipulation. Ensuring the authenticity, continuity and reliability of these artefacts depends upon an unbroken Chain of Custody (CoC), which serves as the backbone of evidentiary integrity in both civil and Syariah proceedings (Tuan Ibrahim et al., 2025d; ISO/IEC 27037:2012).

However, in the enforcement of Syariah criminal law in Malaysia, the Religious Enforcement Officers (REOs) tasked with carrying out raids, seizures and initial evidence preservation often lack specialised training in digital-forensic practices (Yahya et al., 2023; Tuan Ibrahim et al., 2025a). As the first responders at the scene, they are responsible for recognising digital devices, isolating volatile data, and documenting every action in accordance with forensic standards. Yet, in many instances, the absence of clear procedural guidance leads to ad hoc evidence handling, officers may switch on confiscated devices, browse contents, or fail to record serial numbers and timestamps.

Existing legal frameworks have not sufficiently addressed this technological evolution. The Syariah Court Evidence Act 1997 (Act 561) and the Syariah Criminal Procedure Act 1997 were drafted before the digital era and remain silent on electronic forensics. The Standing Instruction of the Director of the State Islamic Religious Department (2007) focuses on tangible exhibits, while the Practice Direction on the Acceptance of Forensic Evidence (2020) merely acknowledges forensic materials without prescribing operational standards. Consequently, inconsistencies arise between states, and evidence handling depends largely on individual discretion rather than uniform forensic procedure.

This procedural gap poses serious implications for justice delivery. In Syariah jurisprudence, the principles of ḥaqq (truth), amānah (trust) and ʿadl (justice) constitute the ethical pillars of adjudication. Any disruption in the evidentiary process undermines these values, risking not only technical invalidation of proof but also moral erosion of judicial credibility. The integrity of digital evidence, therefore, is not merely a procedural concern but a manifestation of maqāṣid al-sharīʿah. Against this background, this study examines the role of Religious Enforcement Officers (REOs) as Digital Evidence First Responders (DEFRs) in strengthening the CoC within Syariah cybercrime investigations.

The Importance of the Chain of Custody (CoC) in Syariah Criminal Investigation

The Chain of Custody (CoC) is the evidentiary framework that ensures every piece of evidence is accounted for from the moment it is discovered until its presentation in court. It records the chronology of evidence handling such as identification, seizure, storagetransfer, and analysis to guarantee authenticity and prevent allegations of tampering (Casey, 2011; Nath et al., 2024). In digital forensics, the CoC functions as the backbone of admissibility since electronic data can be altered, duplicated, or deleted without leaving visible traces (ISO/IEC 27037:2012).

International standards such as ISO/IEC 27037:2012 and NIST SP 800-101 Rev.1 emphasise that the CoC must include verifiable documentation at every stage. These procedures demonstrate that the evidence presented in court is identical to what was originally collected. Any break, omission, or undocumented access in the CoC can render digital evidence inadmissible, as illustrated in Public Prosecutor v Mohd Ezri Azmar Pavel & Anor [2015] MLJU 2112, where failure to verify data continuity undermined the reliability of proof.

Within the Syariah enforcement framework, the integrity of the Chain of Custody is fundamentally tied to the epistemological foundations of Islamic evidence law, which emphasise precision, certainty and the faithful preservation of all forms of bayyinah. The Qur'an provides a clear directive on the importance of accurate documentation and meticulous record-keeping. This is most explicitly articulated in al-Baqarah 2:282, where believers are instructed that whenever a matter involving rights or liabilities is transacted, it must be recorded in writing, and the scribe must write with complete accuracy. Classical jurists regard this verse as establishing a universal legal principle that documentation is required in any context where the protection of rights, the prevention of dispute or the avoidance of doubt is necessary. By analogy, the procedural requirement to record every step of evidence handling, from seizure to storage, reflects this Qur'anic emphasis on precise and reliable documentation.

The Qur'an further reinforces this obligation through the command in al-Baqarah 2:283 which warns against concealing testimony and affirms that whoever hides or manipulates evidence commits a moral and legal wrong. This verse directly supports the modern requirement that evidence must be preserved in its original state and must not be altered, contaminated or misrepresented. In the context of digital forensic evidence, this principle becomes even more significant because electronic data can be easily modified without proper safeguards, and the failure to preserve its authenticity would contravene the Qur'anic prohibition against concealing or distorting truth.

In addition to these specific evidentiary commands, the Qur'an also provides a broader ethical foundation for Chain of Custody obligations. Al-Nisāʾ 4:58 instructs believers to return trusts to their rightful owners, which jurists interpret as an obligation to safeguard all items and responsibilities entrusted to a person, including evidentiary material seized during investigations. The handling of evidence, whether physical or digital, is therefore an amānah that must be protected from loss, negligence or manipulation. Similarly, al-Nisāʾ 4:135 emphasises the duty to uphold justice with unwavering impartiality, even when it conflicts with personal interests. This verse supports the principle that evidence must be managed through transparent, traceable and accountable procedures, so that its reliability is not compromised by personal bias, institutional inconsistency or procedural gaps.

This foundational emphasis naturally leads to the role of the Digital Evidence First Responder. The concept of the DEFR emerges from the need to protect evidentiary integrity at the earliest point of contact. As defined in ISO/IEC 27037:2012, the DEFR is the first individual to identify, collect, or handle digital evidence in a way that preserves its authenticity. In Syariah enforcement operations, this responsibility typically falls upon religious enforcement officers, whose initial actions determine whether subsequent evidentiary procedures can proceed in a manner that aligns with both forensic best practices and Sharīʿah requirements.

The Role of Religious Enforcement Officers as Digital Evidence First Responders

The concept of the Digital Evidence First Responder (DEFR) emerged from the need to safeguard the integrity of electronic evidence at the earliest point of contact. ISO/IEC 27037:2012 defines a DEFR as the first individual who identifies, collects, acquires, or handles digital evidence in a manner that preserves its authenticity and integrity. This role is preventive in nature: most evidentiary contamination occurs at the scene rather than in the laboratory. Consequently, the DEFR bears a critical responsibility to ensure that no action intentional or accidental alters, damages, or destroys data that may later function as bayyinah (proof) in judicial proceedings.

International forensic frameworks such as NIST SP 800-86 and ISO/IEC 27037 emphasise that DEFR procedures must include immediate device isolation, prevention of remote access, photographic documentation, comprehensive seizure logs, and the use of tamper-evident packaging (Horsman, 2021; Faizal & Luthfi, 2024). These procedures maintain a verifiable and uninterrupted Chain of Custody (CoC) from the moment of seizure through subsequent forensic analysis.

Within Malaysia's Syariah enforcement ecosystem, Religious Enforcement Officers (REOs) are not currently designated as Digital Evidence First Responders (DEFRs) under any Syariah statute, practice direction, or administrative circular. Nevertheless, their statutory investigative powers under the Syariah Criminal Procedure Act 1997 and corresponding state enactments position them as the earliest officers to identify, seize, and secure devices containing potential digital evidence. This makes REOs operationally analogous to DEFRs, insofar as they occupy the initial evidentiary interface where contamination, alteration, or destruction of electronic data is most likely to occur. Accordingly, while REOs are not DEFRs in a formal sense, their frontline functions highlight the institutional need to equip them with DEFR-level competencies as part of a coherent digital evidence framework for Syariah criminal enforcement.

Table 1. Functional Mapping Between Statutory Powers of Religious Enforcement Officers and DEFR Responsibilities

No.	Functional Responsibilities (DEFR-Equivalent)	Relevant Legal Provisions (Syariah Criminal Procedure Act 1997)
1	Receiving initial reports and documenting digital-related information	Section 54(1)–(2)
2	Determining the category of the case (seizable / non-seizable)	Section 2(1)
3	Initiating investigations and acting as the first responder at the scene (physical or digital)	Section 55, 57(1)
4	Securing the crime scene and stabilising digital devices (phones, laptops, routers, applications)	Sections 46, 49, 63
5	Conducting searches of premises and digital devices	Sections 44–53, 63(1)–(4)
6	Seizing and collecting digital evidence (mobile phones, USB drives, digital documents, app records)	Sections 46, 52, 53
7	Maintaining the chain of custody for digital evidence	Sections 52–53, 65
8	Conducting arrests to prevent destruction or alteration of digital evidence	Sections 18, 32–38
9	Conducting body searches for digital storage media (SIM cards, memory cards, USB drives)	Sections 12, 15, 16
10	Recording witness and suspect statements, including digital elements	Sections 58, 59, 61, 62
11	Ordering the production of digital documents (screenshots, e-transactions, metadata)	Section 42
12	Documenting all investigative actions (audit trail / chain of custody)	Sections 65, 66
13	Submitting reports to the Syariah Prosecutor	Section 66

The table presented is not intended to imply that Syariah legislation formally recognises or codifies the position of Digital Evidence First Responders (DEFRs). Instead, it functions as a conceptual and functional mapping between the statutory investigative powers articulated in the legislation and the operational roles required for contemporary digital evidence management. Through this analytical alignment, it becomes evident that Religious Enforcement Officers (PPA) effectively discharge DEFR responsibilities by virtue of the powers vested in them under the law. This observation underscores the imperative to enhance their digital and forensic capacities to ensure that the handling, preservation, and transfer of digital evidence adhere rigorously to established chain of custody standards.

Therefore, as frontline personnel during raids and investigative operations, they routinely encounter mobile devices, laptops, external storage media, CCTV units, and online transaction records connected to online gambling, digital fraud, or dissemination of deviant teachings (Tuan Ibrahim et al., 2025b). Although REOs possess statutory authority under the Syariah Criminal Procedure Act 1997 and corresponding state enactments, their operational framework remains predominantly grounded in procedures designed for physical evidence. The Standing Instruction of the Director of the State Islamic Religious Department (2007) prescribes documentation and storage procedures for physical exhibits; however, it provides no corresponding guidance for the handling of electronic evidence. This gap is further corroborated by Yahya and Shariff (2022), whose interviews with religious enforcement officers, pendakwa syarie, and hakim syarie across Negeri Sembilan, Selangor, Melaka, Johor, Perak, Pulau Pinang, and Terengganu revealed that there are no specific procedures governing the search and seizure of electronic documentary evidence in Syariah criminal cases.

This absence of digital-specific protocols has resulted in the widespread use of ad hoc, manual practices such as handwritten seizure lists, non-standardised labelling, and unsecured storage. Without standardised digital evidence forms or tamper-evident packaging, critical identifiers—IMEI numbers, serial numbers, MAC addresses, hash values and metadata are frequently omitted. These omissions weaken the CoC and make it difficult for prosecutors to demonstrate that the device presented in court is the same device seized during the operation. Furthermore, common field practices such as switching on devices to "check" their contents, browsing chat logs, unplugging cables without precaution, or transporting devices in non-secured conditions can alter timestamps, trigger remote wiping, or corrupt volatile data (Vanini et al., 2024). Such actions create opportunities for defence counsel to challenge evidentiary authenticity and admissibility.

Similarly, Practice Direction No. 4 of 2020 on the Submission of Forensic Evidence in Syariah Court Proceedings merely states that "forensic evidence shall be recognised and adopted as one of the forms of proof that may be heard, considered, evaluated and admitted in Syariah Courts for both civil and criminal matters." However, the directive provides no further elaboration on the evidentiary standards, procedural safeguards, or technical requirements applicable to forensic evidence particularly digital forensic evidence. The absence of detailed standards invites inconsistent interpretations and discretionary practices across jurisdictions, creating a risk that critical forensic evidence may be excluded on grounds that are neither legally sound nor forensically justified.

The broader institutional landscape also contributes to forensic unreadiness. Unlike civil enforcement bodies that maintain established digital forensic laboratories and standard acquisition protocols, Syariah enforcement agencies lack a dedicated technological infrastructure for evidence processing, imaging, hashing, and analysis. This absence places a disproportionate burden on REOs, who are expected to preserve digital integrity without the support of specialised facilities or personnel. In effect, the system demands a level of forensic precision that it does not structurally equip officers to achieve.

Addressing these gaps requires the institutional recognition of REOs as Digital Evidence First Responders and equipping them with foundational digital forensic competencies. Training in device isolation, identification of volatile data, digital documentation, and the generation of hash values would enable REOs to protect electronic evidence in accordance with global best practices. Ensuring DEFR-level competence at the earliest stage is crucial because any weakness in the initial handling of evidence cannot be remedied by downstream forensic processes.

These operational, procedural, and institutional weaknesses carry ethical consequences from the perspective of maqāṣid al-sharīʿah. Digital evidence integrity is directly connected to ḥaqq (truth), ʿadl (justice), and amānah (responsibility). Mishandling evidence can lead to wrongful acquittals, compromised prosecutions, or unjust convictions. Thus, improving forensic readiness is not only a technical necessity but a Sharīʿah imperative. Taken together, these challenges demonstrate that the existing Syariah enforcement structure is not yet equipped to meet the evidentiary demands of cyber-enabled offences. Strengthening DEFR competencies among REOs is therefore essential to ensuring accurate, trustworthy, and legally defensible digital evidence handling.

Recommendations for Strengthening Digital Evidence Handling and the Role of DEFRs in Syariah Enforcement

The findings of this study show that the current system for handling digital evidence in Syariah criminal cases is still not strong enough to meet the needs of today's digital environment. Existing rules focus mainly on physical items, while digital devices such as mobile phones, laptops, online accounts and cloud-based data are becoming the main sources of evidence in many modern Syariah offences, including online gambling, digital fraud and various forms of online misconduct. Because Religious Enforcement Officers (REOs) are usually the first to encounter digital devices during raids or investigations, their role as Digital Evidence First Responders (DEFRs) is extremely important for ensuring that evidence remains clean, authentic and usable in court. To improve this situation, several practical steps can be taken at the administrative, operational and legal levels.

Improving and Clarifying Existing Guidelines for Digital Evidence Handling

One of the main weaknesses in the current system is the lack of clear and detailed guidelines that Religious Enforcement Officers can rely on when handling digital evidence. Although Practice Direction No. 4 of 2020 acknowledges that forensic evidence may be admitted in Syariah courts, it does not set out the basic steps required. This creates inconsistency and increases the risk that important evidence may later be challenged in court. Strengthening the guidelines with clearer explanations, practical steps, sample forms and easy-to-follow checklists would ensure that all states apply the same standards. A more complete and consistent set of guidelines would make digital evidence handling more reliable, transparent and defensible in Syariah proceedings.

Establishing a Dedicated Digital Evidence Unit within Religious Enforcement Agencies

Given the rapid digitalisation of society, Syariah offences are increasingly linked to technological platforms. The traditional structure of religious enforcement agencies, which focuses mainly on physical inspections and on-ground surveillance, is no longer sufficient to manage digital forms of wrongdoing. A dedicated digital evidence unit would serve as a central point for managing electronic devices from the moment they are seized until they are safely stored. Such a unit would coordinate with external forensic laboratories, maintain updated knowledge on digital threats and assist other officers in ensuring that devices are handled properly. This kind of structural improvement reflects current global enforcement trends and ensures that Syariah agencies are organisationally prepared to deal with crimes conducted through smartphones, apps, cloud platforms and emerging technologies.

Enhancing Training for REOs as Digital Evidence First Responders

As technology evolves, Religious Enforcement Officers must be equipped with knowledge and skills that go beyond traditional enforcement training. Officers acting as Digital Evidence First Responders need to understand how to identify electronic devices, isolate them safely, prevent remote access, document relevant data and preserve volatile information. Modern training should also address technological challenges posed by artificial intelligence, such as deepfake images, manipulated videos, automated messaging and hidden online gambling applications. Up-to-date and continuous training will help officers avoid accidental damage, prevent data loss and maintain the integrity of the chain of custody. It will also strengthen their ability to give accurate and credible explanations in court, which is essential for supporting the principle of amānah and ensuring that evidence remains trustworthy.

Updating Syariah Evidence Legislation to Reflect Digital Realities

Even with better guidelines and improved officer training, digital evidence may still face legal challenges if the Syariah Court Evidence Act is not updated to reflect the realities of today’s digital environment. The Act currently lacks explicit provisions on digital evidence. Without legal definitions and statutory recognition, judges may struggle to evaluate digital records consistently, and prosecutors may face uncertainty in presenting them. Updating the Act to include clear definitions and rules on digital evidence will give the courts a stronger legal foundation and reduce reliance on broad interpretive principles. This modernisation is necessary to ensure that Syariah courts remain relevant and capable of dealing with digital forms of wrongdoing, especially as cyber-enabled offences continue to grow.

Conclusion

The emergence of cyber-dependent and cyber-enabled crimes has transformed the evidentiary landscape of Syariah criminal justice in Malaysia. Offences that once occurred in physical settings now unfold through digital platforms, leaving behind electronic footprints rather than human witnesses. This shift challenges the classical foundations of Islamic evidentiary law, which traditionally relies on iqrār, shahādah, and qarīnah. In digital environments, proof is increasingly embodied in metadata, log files, chat histories, online transactions, and AI-generated materials, all of which are volatile and easily manipulated. Ensuring their authenticity requires strict adherence to an unbroken Chain of Custody, a principle widely recognised in international forensic standards and fundamentally aligned with Islamic demands for accuracy, trustworthiness, and justice.

The study shows that the current Syariah enforcement system remains structurally unprepared to meet these demands. Religious Enforcement Officers, who serve as the earliest point of contact with digital evidence, play a decisive role in shaping its admissibility. Yet, in practice, they operate without specialised training, without dedicated digital-forensic infrastructure, and without clear procedural guidance. The Standing Instruction of 2007 was drafted for physical exhibits, while the 2020 Practice Direction acknowledges forensic evidence but offers no operational standards. As a result, digital devices are often handled inconsistently, documented incompletely, or exposed to contamination—problems further exacerbated by handwritten seizure lists, non-standard labelling, and unsecured storage. These weaknesses undermine the continuity and certainty required by both forensic science and the Sharīʿah.

At the normative level, the integrity of digital evidence is not merely a procedural expectation but an ethical imperative grounded in the Qur'an. Verses such as al-Baqarah 2:282 and 2:283 emphasise precise documentation and prohibit concealment or distortion of testimony, while al-Nisā' 4:58 and 4:135 establish the duties of amānah and ʿadl in all forms of public responsibility. These principles resonate strongly with the logic of the Chain of Custody, which requires transparent, traceable, and accountable handling of every item intended to serve as bayyinah. Any disruption to evidentiary integrity therefore represents not only a technical flaw but a deviation from core maqāṣid values of truth, justice, and trustworthiness.

Recognising Religious Enforcement Officers as Digital Evidence First Responders is essential for bridging this gap between traditional investigative practices and the demands of the digital age. Their position at the front lines of Syariah investigations places them in the most critical stage of evidence preservation, where contamination is most likely to occur and where proper handling can determine the fate of a case. Elevating REOs to DEFR-level competency requires clearer guidelines, institutional support, legal reform, and continuous professional development. Measures such as establishing dedicated digital evidence units, enhancing training to address AI-driven risks, standardising documentation and storage procedures, and updating the Syariah Court Evidence Act to explicitly recognise digital records are all necessary steps to ensure that Syariah enforcement remains relevant, reliable, and aligned with contemporary forensic standards.

Ultimately, strengthening the role of REOs as Digital Evidence First Responders is not only a technical necessity but a Sharīʿah imperative. As digital environments continue to reshape human behaviour and criminal activity, the Syariah justice system must evolve to protect the values it upholds. Ensuring that digital evidence is handled with accuracy, trustworthiness, and procedural justice affirms the maqāṣid al-sharīʿah and reinforces public confidence in the integrity of Syariah courts. This study demonstrates that the transformation of REOs into competent DEFRs is a critical pathway toward a more resilient, credible, and technologically responsive Syariah criminal justice system.

References

Casey, E. (2011). *Digital Evidence and Computer Crime : Forensic Science, Computers and the Internet* (3rd ed.). Academic Press.

Faizal, A., & Luthfi, A. (2024). Comparison Study of NIST SP 800-86 and ISO/IEC 27037 Standards as A Framework for Digital Forensic Evidence Analysis. *Journal of Information Systems and Informatics*, *6*(2), 701–718. https://doi.org/10.51519/journalisi.v6i2.717

Horsman, G. (2021). Decision support for first responders and digital device prioritisation. *Forensic Science International: Digital Investigation*, *38*, 301219. https://doi.org/10.1016/j.fsidi.2021.301219 https://unimel.edu.my/journal/index.php/julwan/article/view/1954/1514

Nath, S., Summers, K., Baek, J., & Ahn, G.-J. (2024). Digital Evidence Chain of Custody: Navigating New Realities of Digital Forensics. 11–20. https://doi.org/10.1109/tps-isa62245.2024.00012

Shariff, A. A. M., Yahya, M. A., Rajamanickam, R., Tzu-Hsin, M. H., Subki, M. M. M., Azahari, N. F., Raja, J., & Muhamad, S. S. (2022). Prinsip Rantaian Jagaan dan Rantaian Keterangan: Keperluan kepada Pengiktirafan dan Pengaplikasian dalam Perbicaraan Kes Syariah di Malaysia: Principles of Chain of Custody and Chain of Evidence: The Need for Recognition and Application in Malaysian Syariah Case. *Journal of Muwafaqat*, *5*(1), 17–32. https://doi.org/10.53840/muwafaqat.v5i1.106

Tuan Ibrahim, T. M. F. H., Alias, M. A. A., Nor Muhamad, N. H., & Baharuddin, A. S. (2025a). Pembuktian Forensik Digital di Mahkamah Syariah: Kerangka Kebolehterimaan dan Integriti Dalam Jenayah Syariah. *Journal of MUWAFAQAT*, *8*(2), 78–100. https://doi.org/10.53840/muwafaqat.v8i2.197

Tuan Ibrahim, T. M. F. H., Faisal, M. S., Alias, M. A. A., & Baharuddin, A. S. (2025b). Pemetaan Perundangan Seksyen 70 Akta Tatacara Jenayah Syariah (Wilayah-wilayah Persekutuan) 1997 [Akta 560]: Implikasi terhadap Kesalahan Jenayah Syariah di Alam Siber. *Kanun Jurnal Undang-Undang Malaysia*, *37*(2), 263–282. https://doi.org/10.37052/kanun.37(2)no4

Tuan Ibrahim, T. M. F. H., Nor Muhamad, N. H., Alias, M. A. A., & Baharuddin, A. S. (2025c). Fiqh Al-Waqi': Teras Revolusi Keterangan Forensik Digital Dalam Membendung Jenayah Syariah Siber. Jurnal 'Ulwan, 10(1), 28–46.

Tuan Ibrahim, T. M. F. H., Nur Muhamad, N. H., & Baharuddin, A. S. (2025d). Chain Of Custody Parameters For Digital Forensic Evidence in Shariah Criminal Court Proceedings. IIUM Law Journal, 33(2), 205–240. https://doi.org/10.31436/iiumlj.v33i2.1088

Vanini, C., Gruber, J., Hargreaves, C., Benenson, Z., Freiling, F., & Breitinger, F. (2024). Strategies and Challenges of Timestamp Tampering for Improved Digital Forensic Event Reconstruction (extended version). *ArXiv (Cornell University)*. https://doi.org/10.48550/arxiv.2501.00175

Whitty, Monica. T., & Young, G. (2025). Relational Cybercrimes: A New Way Forward in Classifying Cybercrimes. *IEEE Security & Privacy*, *23*(4), 80–90. https://doi.org/10.1109/msec.2025.3576909

Yahya, M. A., & Shariff, A. A. M. (2022). Proses Penggeledahan Keterangan Dokumen Elektronik dalam Kes Jenayah Syariah: Searching Process in the Syariah Criminal Cases: Analysis the Admissibility of Electronic Document Evidence. *Journal of Muwafaqat*, *5*(2), 153–163. https://doi.org/10.53840/muwafaqat.v5i2.122