33 (2) 2025 IIUMLJ 205 - 240

CHAIN OF CUSTODY PARAMETERS FOR DIGITAL FORENSIC EVIDENCE IN SHARIAH CRIMINAL COURT PROCEEDINGS

Tuan Muhammad Faris Hamzi Tuan Ibrahim*

Nasrul Hisyam Nur Muhamad**

Ahmad Syukran Baharuddin***

ABSTRACT

The growing prevalence of cyber-enabled Shariah offence has necessitated the integration of digital forensic procedures into Shariah criminal proceedings. However, the absence of an explicit legal framework for the chain of custody (CoC) in handling digital evidence within the Shariah courts creates a critical procedural vacuum. This omission exposes proceedings to dual risks: the exclusion of probative evidence due to doubts about authenticity and the potential for wrongful convictions based on improperly handled or contaminated digital evidence. This study examines the operational role of religious enforcement officers (PPA) as Digital Evidence First Responders (DEFR) under the Syariah Criminal Procedure (Federal Territories) Act 1997, and their compliance with technical protocols outlined in ISO/IEC 27037:2012 and the Standing Instruction of the Director of the State

*PhD Candidate in Fiqh Science and Technology, Islamic Civilisation Academy, Faculty of Social Sciences and Humanities, Universiti Teknologi Malaysia, 81310, Johor Bahru, Johor, Malaysia. Email: tuanfaris.tf@gmail.com

**Associate Professor, Islamic Civilisation Academy, Faculty of Social Sciences and Humanities, Universiti Teknologi Malaysia, 81310, Johor Bahru, Johor, Malaysia. Email: nasrul@utm.my

***Associate Professor, Faculty of Syariah and Law, Universiti Sains Islam Malaysia, 71800, Nilai, Negeri Sembilan, Malaysia. Research Fellow, Maqasid Institute, United States of America. Researcher, Centre of Research for Fiqh Forensics and Judiciary (CFORSJ), Faculty of Syariah and Law, Universiti Sains Islam Malaysia, 71800, Nilai, Negeri Sembilan, Malaysia. Email: ahmadsyukran@usim.edu.my (Corresponding Author)

[Received: 22 July 2025, Accepted: 30 October 2025, Published: 30 November 2025]

Islamic Religious Department (2007). Using a doctrinal and comparative legal method, the study further analyses 18 Malaysian civil criminal cases to extract recurring CoC deficiencies and judicial expectations. From this analysis, five core CoC parameters are distilled, documentation continuity, evidence integrity, authentication, expert verification and corroborative reliability. These elements are essential in ensuring evidentiary credibility from seizure to courtroom presentation. The findings demonstrate that while Shariah enforcement officers operationally adhere to the existing procedure, these COC practices remain unrecognized in Shariah jurisprudence. This paper proposes the systematic adoption of CoC parameters within the Shariah proceedings to enhance evidentiary reliability and judicial confidence. Institutionalizing such parameters aligns with the *maqāṣid al-sharīʿah* by advancing justice and procedural transparency in the adjudication of emerging digital crimes.

Keywords: Digital Forensic, Chain of Custody, Shariah Criminal Procedure, Shariah Criminal Offences.

PARAMETER RANTAIAN JAGAAN BAGI BUKTI FORENSIK DIGITAL DALAM PROSIDING JENAYAH MAHKAMAH SYARIAH

ABSTRAK

Peningkatan kesalahan Syariah berasaskan siber telah menuntut pengintegrasian prosedur forensik digital ke dalam prosiding jenayah Syariah. Walau bagaimanapun, ketiadaan kerangka undang-undang yang jelas berhubung rantaian jagaan (CoC) bagi pengendalian bukti digital di Mahkamah Syariah telah mewujudkan kelompangan prosedural yang kritikal. Kelemahan ini mendedahkan prosiding kepada dua risiko utama, penolakan bukti yang bersifat probatif disebabkan keraguan terhadap kesahihannya dan kemungkinan sabitan yang salah akibat bukti yang tidak dikendalikan dengan betul atau tercemar. Kajian ini meneliti peranan pegawai penguatkuasaan agama (PPA) sebagai *Digital Evidence First Responders (DEFR)* di bawah Akta Tatacara Jenayah Syariah (Wilayah-Wilayah Persekutuan) 1997, serta pematuhan terhadap protokol teknikal yang digariskan dalam ISO/IEC 27037:2012 dan Arahan Tetap Pengarah Jabatan Agama Islam Negeri (2007). Melalui pendekatan metode doktrinal, kajian ini turut menganalisis 18 kes jenayah sivil di Malaysia bagi mengenal pasti kelemahan berulang dalam rantaian jagaan serta keputusan kehakiman terhadap pengendalian bukti. Hasil analisis ini mendapati lima parameter teras CoC iaitu,

kesinambungan dokumentasi, integriti bukti, autentikasi, pengesahan pakar, dan kebolehpercayaan sokongan. Kesemua elemen ini penting bagi memastikan kredibiliti bukti daripada proses penyitaan hingga kepada pembentangan di mahkamah. Dapatan kajian menunjukkan bahawa walaupun pegawai penguatkuasaan Syariah mematuhi prosedur sedia ada, amalan CoC masih belum diiktiraf secara jelas dalam kerangka perundangan Syariah. Oleh itu, kajian ini mencadangkan pengiktirafan parameter CoC secara sistematik dalam prosiding jenayah Syariah untuk meningkatkan kebolehpercayaan bukti serta keyakinan kehakiman. Pemantapan parameter ini sejajar dengan *maqāṣid al-sharīʿah* melalui usaha menegakkan keadilan dan ketelusan prosedural dalam pengadilan jenayah digital yang semakin kompleks.

Kata Kunci: Forensik Digital, Rantaian Jagaan, Tatacara Jenayah Syariah, Kesalahan Jenayah Syariah.

INTRODUCTION

The emergence of cyber-enabled Syariah criminal offences in Malaysia, including online gambling (*al-maysir*) or false doctrine via social media platforms poses serious challenges to the established evidentiary mechanisms within the Syariah judicial system.[1] These offences, while rooted in Syariah Criminal Offences (Federal Territories) Act 1997 have evolved into complex and technologically mediated forms that transcend jurisdictional boundaries and exploit the anonymity of the digital environment. Minister of Communications and Digital, Fahmi Fadzil, stated, according to records from the Royal Malaysia Police (PDRM), the number of various cybercrime cases in 2024 rose to 35,368, involving total losses of RM1.5 billion. This marks an increase from 34,495 cases in 2023, which recorded losses amounting to RM1.22 billion.[2] This technological shift has resulted in

[1]Tuan Muhammad Faris Hamzi Tuan Ibrahim et al., "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, no. 2 (July 31, 2025): 263–82, https://doi.org/10.37052/kanun.37(2)no4.

[2]Radhi, Mohamed. "Fahmi: Malaysia Lost RM1.2b to Online Crimes This Year." NST Online. New Straits Times, December 9, 2024. https://www.nst.com.my/news/nation/2024/12/1145948/fahmi-malaysia-lost-rm12b-online-crimes-year.

a significant evidentiary gap within the Shariah courts, which have long relied on traditional methods of proof such as *shahādah* (eyewitness testimony) and *iqrār* (confession) to substantiate criminal liability.[3,4]

Cybercrime often occurs covertly and is difficult to detect by authorities due to no physical traces or the difficulty in having human witnesses. Unlike conventional crimes which usually leave physical traces or have direct witnesses.[5,6,7] Cybercriminals commonly use disguise tools such as virtual private networks (VPNs), end-to-end encrypted applications, making the process of identity verification difficult and weakening the effectiveness of conventional testimonial evidence.[8] In cases involving *taʿzīr* offences, where the evidentiary threshold is based on *ẓann ghālib* (dominant probability),[9] the need for

[3]Mohamad Aniq Aiman Alias et al., "Wasa'il Ithbat Dalam Undang-Undang Keterangan Islam: Analisis Perundangan Terhadap Keabsahan Dokumen Elektronik Di Mahkamah Syariah Malaysia," *Malaysian Journal of Syariah and Law* 12, no. 3 (December 31, 2024): 689–700, https://doi.org/10.33102/mjsl.vol12no3.792.

[4]Tuan Muhammad Faris Hamzi Tuan Ibrahim et al., "Fiqh al-Waqi': Teras revolusi keterangan forensik digital dalam membendung jenayah Syariah siber." *Jurnal 'Ulwan* 10, no. 1 (2025): 28-46.

[5]Poongodi Thangamuthu et al., "Encyclopedia of Criminal Activities and the Deep Web," in *IGI Global EBooks* (IGI Global, 2020), 1–22, https://doi.org/10.4018/978-1-5225-9715-5.ch001.

[6]Tuan Muhammad Faris Hamzi Tuan Ibrahim et al., "Pembuktian Forensik Digital Di Mahkamah Syariah: Kerangka Kebolehterimaan Dan Integriti Dalam Jenayah Syariah," *Journal of Muwafaqat* 8, no. 2 (October 31, 2025): 78–100, https://doi.org/10.53840/muwafaqat.v8i2.197.

[7]Alketbi, Anoud Sultan Saqer, and Osama Kanaker. " Dawr al-iʻlām al-raqamī fī tashkīl al-huwiyya al-waṭaniyya: dirāsah muqāranah bayna al-Imārāt wa Mālīziyā fī ḍaw' al-siyāsāt al-ʻlāmiyyah: The Role of Digital Media in Shaping National Identity: A Comparative Study between The United Arab Emirates and Malaysia in Light of Media Policies." *Law, Policy, and Social Science* 4, no. 1 (2025): 132-153.

[8]A.S. Awate et al., "Unmasking Attacker Identity behind the VPN," in *Advances in AI for Biomedical Instrumentation, Electronics and Computing* (London: CRC Press, 2024), 316–21,

[9]Suhaizad Saifuddin, "Analisis Pemakaian Darjah Pembuktian Bagi Kesalahan Hudud Di Bawah Enakmen Jenayah Syariah Di Malaysia: Analysis of Applied the Standard of Proof for Hudud Offences Under the Shariah Criminal Enactment in Malaysia," *Journal of Shariah Law Research* 6, No. 1 (2021): 89–108,

alternative forms of reliable proof has become increasingly urgent. Forensic digital evidence capable of fulfilling this function. However, its admissibility and probative strength in the Shariah courts depend heavily on its authenticity and legal integrity elements which, in practice, are preserved through the implementation of a transparent chain of custody.

The principle of chain of custody (CoC) refers to the continuous, chronological documentation that records every point of contact with the evidence, such as clear log of acquisition, handling, transfer, storage, and analysis from the moment of its collection to its final presentation in court.[10] International legal systems, including those in the United States under the Federal Rules of Evidence and the United Kingdom under the Police and Criminal Evidence Act 1984 (PACE), treat CoC as a legal safeguard to prevent contamination or fabrication of evidence. In Malaysia, civil courts have adopted this principle strictly, particularly in cases involving narcotics, corruption, and cybercrime as demonstrated in *Public Prosecutor v Lee Yau Ket [2008] 4 MLJ 223* and *Dato' Seri Anwar Ibrahim v Public Prosecutor [2015]*, where evidence was excluded due to gaps in the CoC that rendered it unreliable or susceptible to tampering.

Despite its significance in civil and criminal proceedings, the application of the chain of custody within the Shariah courts remains largely underdeveloped.[11] Most Syariah Criminal Procedure Enactments across the states of Malaysia are silent on the collection and preservation of digital evidence and there exists no standardised protocol or parameters for validating the integrity of such materials. In the absence of clear procedural guidance, judges in the Shariah courts are compelled to rely on personal interpretation, which risks inconsistency and undermines procedural fairness.

[10]Premanand Narasimhan and N. Kala, "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, no. 6 (December 12, 2024): 2438–50, https://doi.org/10.32628/CSEIT2410612443.

[11]Ahmad Azam Mohd Shariff et al., "Prinsip Rantaian Jagaan Dan Rantaian Keterangan: Keperluan Kepada Pengiktirafan Dan Pengaplikasian Dalam Perbicaraan Kes Syariah di Malaysia" *Journal of Muwafaqat* 5, no. 1 (April 30, 2022): 17–32, https://doi.org/10.53840/muwafaqat.v5i1.106.

This is further complicated by the lack of training within the Shariah legal framework and the limited technical infrastructure available to religious enforcement bodies.[12,13] Consequently, digital evidence that could potentially establish guilt in cyber-enabled offences such as online *zinā* (illicit sexual conduct through digital platforms), *qazf* (false online accusations of *zinā*), *or al-maysir* (online gambling) may be rendered inadmissible due to concerns over its credibility or mishandling during the investigation phase.

In response to these challenges, this article seeks to define and propose a coherent framework for the application of the chain of custody in the handling of digital forensic evidence within the context of Shariah criminal offences in Malaysia. The objective is to formulate parameters that are both technically sound and jurisprudentially legitimate, drawing from best practices in digital forensics, established legal doctrines in the civil judiciary, and principles rooted in Islamic evidentiary theory. By establishing clear parameters for the admissibility and integrity of digital evidence in Shariah courts, this study aims to bridge the evidentiary gap that has emerged in the wake of digital criminality and ensure that the administration of justice remains consistent with both technological developments and the ethical imperatives of the *Sharīʿah*.

DIGITAL FORENSICS AND CHAIN OF CUSTODY IN CRIMINAL PROCEEDINGS

Digital forensics is an evolving discipline dedicated to systematically identifying, collecting, preserving, and analysing digital evidence derived from electronic devices such as computers, smartphones,

[12]Mohamad Azhan Yahya, Ahmad Azam Mohd Shariff, and Nurul Nisa Khalid, Proses Pengumpulan Keterangan Dokumen Elektronik (Penerbit UKM, 2024).

[13]Mohamad Aniq Aiman Alias et al., "Digital Forensics and the Admissibility of Electronic Evidence in Malaysian Syariah Courts: Towards A Standardised Legal Framework," *LexForensica: Journal of Forensic Justice and Socio-Legal Research* 2, no. 1 (2025): 84–91, https://doi.org/10.33102/6grx4619.

storage drives, and networks.[14,15] This evidence, typically stored in binary form and is crucial in investigating and prosecuting electronic and cyber-enabled crimes. The core objective of digital forensic practices is to recover and examine digital artifacts in a manner that maintains their reliability and integrity to ensure they remain admissible in court.[16] Central to this evidentiary integrity is the principle known as the chain of custody (CoC). CoC refers to a meticulous documentation procedure that tracks evidence chronologically from the initial point of collection through storage, analysis, and eventual courtroom presentation. This rigorous process encompasses recording detailed information about who handled the evidence, the date and time of each interaction, and the circumstances surrounding each transfer.[17] By preserving a clear, traceable record, the CoC protects digital evidence from contamination, tampering, and unauthorised alterations, thereby enhancing its credibility and reliability. As Casey explains, meticulous CoC documentation ensures that each transfer of evidence is accounted for, which is critical to maintain judicial confidence in its integrity.[18] For example, in *Public Prosecutor v Ahmad Rizal bin Umar* [2017] 6 MLJ 279, the court rejected DNA evidence because of a break in the chain of custody,

[14]Jaydevsinh B Vala and Vipul M Vekariya, "The Role and Importance of Digital Forensics and Digital Evidence in Cyber Crime Detection," *International Journal of Life Sciences, Biotechnology and Pharma Research* 13, no. 6 (July 1, 2024): 413–20, https://doi.org/10.69605/ijlbpr_13.6.2024.80.

[15]Tuan Muhammad Faris Hamzi Tuan Ibrahim, Mohamad Aniq Aiman Alias, and Ahmad Syukran Baharuddin, "A Preliminary Review of Digital Forensics as A Means of Proof in Modern Syariah Criminal Offences from A Maqasid Al-Shari'ah Perspective," *Syariah and Law Discourse | Diskusi Syariah dan Undang-Undang* 6, no. 1 (2025): 1–6, https://fsuproceedings.usim.edu.my/index.php/dsl/article/view/33.

[16]R. Parkavi, K. Divya, and V Sherry Ruth, "Digital Crime Evidence," in *Critical Concepts, Standards, and Techniques in Cyber Forensics* (IGI Global, 2020), https://doi.org/10.4018/978-1-7998-1558-7.ch008.

[17]Souradip Nath et al., "Digital Evidence Chain of Custody: Navigating New Realities of Digital Forensics," in *IEEE 6th International Conference on Trust, Privacy and Security in Intelligent Systems, and Applications*, 2024, 11–20, https://doi.org/10.1109/tps-isa62245.2024.00012.

[18]Eoghan Casey, Digital Evidence and Computer Crime: Forensic Science, Computers, and the Internet (Academic Press, Inc.6277 Sea Harbor Drive Orlando, FL United States, 2011).

demonstrating how lapses in record-keeping can render crucial forensic material inadmissible.

CoC is not simply a theoretical concept but serves as a fundamental requirement for determining the admissibility of digital forensic evidence in judicial proceedings. Malaysian civil courts have consistently emphasised the CoC, as demonstrated in the landmark decision of *Public Prosecutor v Lee Yau Ket [2008] 4 MLJ 223*. In this case, the prosecution's inability to provide adequate documentation between seizure and chemical analysis raised substantial doubts regarding possible contamination or substitution, leading to the exclusion of the drug exhibits and resulting in acquittal. Similar judicial scrutiny has occurred in subsequent cases involving highly sensitive evidence like DNA samples, toxicological materials, and digital records, reinforcing the necessity for rigorous adherence to CoC protocols to protect evidence integrity throughout its lifecycle. For instance, in *Dato' Seri Anwar bin Ibrahim v Public Prosecutor and another appeal* [2015] 2 MLJ 293, the Federal Court emphasised that any gap in the custody of DNA samples could cast serious doubt on their admissibility.

The legal framework supporting CoC in Malaysia can be found indirectly in the *Evidence Act 1950*. Section 60 requires direct oral evidence to prove the contents of documents, unless exceptions apply. Section 73A allows for the admissibility of documents produced by computers, while Sections 90A and 90B explicitly govern the admissibility of electronic records and computer output, stipulating that such records must be generated through regular, secure, and verifiable processes**.** Although the Act does not use the term "chain of custody", the requirements of integrity, reliability, and authenticity embedded in these provisions functionally demand a CoC-compliant approach. Indeed, these sections establish a functional equivalence between physical and digital records which treat both as potentially probative if properly preserved and documented.

Critically, however, these statutory safeguards and the jurisprudence that supports them are exclusive to the civil and criminal courts and not binding on Shariah courts, which operate under a separate legal system. Shariah courts in Malaysia derive their jurisdiction from state-level legislation, and their evidentiary procedures are governed by enactments such as the *Syariah Court Evidence (Federal Territories) Act 1997* and their counterparts in other

states. A key limitation is that these enactments are largely silent on the procedural handling of digital or electronic evidence post-seizure. There is no explicit requirement for documentation of custody, no mention of forensic handling procedures and no statutory incorporation of best practices.[19]

This legislative gap creates a doctrinal vacuum. While Shariah judges may rely on *ijtihād* and discretion, the absence of codified CoC principles has led to inconsistent evidentiary practice. For instance, in *Pendakwa Syarie Negeri Sabah v Rosli bin Abdul Japar* [1428H] JH XXIII (II), DNA evidence was admitted proving *zinā* and in *Mohammad Ismail bin Hj Abu Bakar v Hajah Rosita @ Nurul Asyiqin* [2009] 3 ShLR, DNA was used in a paternity dispute. Yet in both cases, reliance on expert reports and forensic findings was not accompanied by any reference to CoC, reflecting its absence as a doctrinal parameter in the Shariah courts. Islamic law places a high emphasis on certainty (*yaqīn*) and the minimisation of doubt (*syak*), as preserved in the legal maxim *al-yaqīn lā yazūlu bi al-syak* (certainty is not overruled by doubt). Yet without a proper CoC framework, the evidentiary process in Shariah courts risks violating this maxim by allowing the possibility of doubt to contaminate the reliability of evidence. This problem is well illustrated in civil cases such as *PP v Ahmad Rizal bin Umar* [2017] 6 MLJ 279 and *PP v Saiful Bahari bin Mohamad* [2020] MLJU 2237, where DNA and drug evidence were excluded due to breaks in the CoC.

Thus, a critical re-examination of the CoC from the standpoint of legal harmonisation is warranted. The CoC is not inherently secular nor incompatible with Islamic jurisprudence. Rather, it is a manifestation of procedural justice (which resonates with the Qurʾānic command to uphold fairness and integrity in adjudication that complements the *maqāṣid*-based commitment to fairness, transparency, and protection of rights.

[19]Yahya, Shariff, and Khalid, Proses Pengumpulan Keterangan Dokumen Elektronik

EVIDENTIARY METHODS IN SHARIAH CRIMINAL LAW

The Shariah criminal legal tradition, as codified in various *madhāhib* and reflected in contemporary legal enactments, employs a structured and hierarchical framework for evidence admission. This framework encompasses *al-shahādah* (eyewitness testimony), *al-iqrār*, *al-yamīn*, *al-kitābah* (documentation), *al-qarīnah* (circumstantial evidence), *ʿilm al-qāḍī* (the judge's personal knowledge), and *al-khibrah* (expert opinion).[20] Each category carries varying degrees of probative weight, often calibrated according to the classification of the offence whether it pertains to *ḥudūd* (fixed penalties), *qiṣāṣ* (retaliatory punishments), or *taʿzīr* (discretionary punishments).[21,22] For *ḥudūd* and *qiṣāṣ* offences, the evidentiary threshold is exceptionally high, requiring *yaqīn* (absolute certainty) as embodied in the legal maxim *idrāʾū al-ḥudūd bi al-shubhāt* (avoid the ḥudūd punishments in cases of doubt). However, in *taʿzīr* offences which are discretionary in both definition and punishment, the evidentiary threshold is more flexible, often operating based on *ẓann ghālib* (dominant probability).[23] Within this category, the use of *qarīnah* contextual or circumstantial evidence has been widely acknowledged, particularly by classical jurists who viewed it as a legitimate means of establishing criminal liability when primary evidence is absent or inaccessible.

Among the most notable proponents of *qarīnah* as admissible proof in Islamic criminal jurisprudence are Ibn Taymiyyah and his student Ibn Qayyim al-Jawziyyah**.** Both scholars expanded the evidentiary scope of *taʿzīr* by recognising the validity of strong

[20]Muhammad Musṭafā Al-Zuḥaylī, *Wasāil Al-Ithbāt Fī Sharī'ah Islamiyyah.* (Damsyiq: Maktabah Dār Al-Bayān., 1982).

[21]Al-Zuḥaylī, Wasāʾil al-Ithbāt

[22]Wan Ismail, Wan Abdul Fattah, Hasnizam Hashim, Zulfaqar Mamat, Lukman Abdul Mutalib, Ahmad Syukran Baharuddin, and Norma Jusof. 2021. "Sumpah Nafy Al-'Ilmi Menurut Undang-Undang Keterangan Islam Di Malaysia: Nafy Al-'Ilmi Oath According to Islamic Law of Evidence in Malaysia". *AL-MAQASID: The International Journal of Maqasid Studies and Advanced Islamic Research* 2 (2). :25-37. https://doi.org/10.55265/almaqasid.v2i2.11.

[23]Ahmad Syarbaini, "Konsep Ta'zir Menurut Perspektif Hukum Pidana Islam," *Jurnal Tahqiqa: Jurnal Ilmiah Pemikiran Hukum Islam* 17, no. 2 (July 31, 2023): 37–48, https://doi.org/10.61393/tahqiqa.v17i2.167.

contextual indicators, provided such evidence does not contradict *naṣṣ qatʿī* (definitive legal texts) or lead to injustice. Ibn Qayyim, in *Iʿlām al-Muwaqqiʿīn*, offered numerous examples of prophetic practice and early judicial decisions in which judges relied on circumstantial signs to issue rulings, particularly in criminal and matrimonial contexts.[24] His legal philosophy also rooted in the preservation of *ʿadl* (justice) and *ḥifẓ al-ḥuqūq* (protection of rights), which justifies the use of *qarīnah* when it aligns with the objectives of the *Sharīʿah*.

Although Shariah criminal law identifies offences such such as *zinā, qazf*, and *shurb al-khamr* (consumption of intoxicants) as part of the classical *ḥudūd* framework, all state-level Shariah Criminal Offences Enactments currently classify and prosecute these acts under *taʿzīr*. This is due to the jurisdictional limitations imposed by the Syariah Courts (Criminal Jurisdiction) Act 1965 (Act 355), which restricts the scope of punishment to *taʿzīr*-based penalties. Despite various initiatives to expand Shariah criminal jurisdiction, including proposed amendments to Act 355, the administration of Islamic criminal justice in Malaysia remains within the *taʿzīr* framework as defined by federal law and the Syariah Criminal Offences (Federal Territories) Act 1997.

In the context of *taʿzīr* offences, the evidentiary threshold does not require absolute certainty (*yaqīn*) as in *ḥudūd* cases. It is generally sufficient for the evidence to establish guilt beyond reasonable doubt (*ghalabat al-ẓann)*. In fact, classical and contemporary scholars have debated the precise meaning of *yaqīn*, recognising that even with *shahādah* (eyewitness testimony) or *iqrār* (confession), there remains the possibility of deceit or error.[25] As a result, some jurists argue that *yaqīn* need not signify 100% certainty; rather, a high degree of confidence such as 95% may suffice, so long as it clearly exceeds mere *ghalabat al-ẓann* and supports a just conviction.[26] Therefore, the failure to incorporate contemporary technological methods of proof represents a significant disadvantage for the Shariah court system

[24]Shams Al-Din Muhammad Ibn Qayyim, *Iʿlām Al-Muwaqqiʿīn ʿan Rabb Al-ʿĀlamīn* (Darul Ibn Hazm, n.d.).

[25]Lukman Abdul Mutalib, Wan Abdul Fattah Wan Ismail, and Abd Hamid Abdul Murad, *Al-Qarinah Dalam Hukum Hudud*, *Jendela DBP* (Dewan Bahasa dan Pustaka Kuala Lumpur, 2017),

[26]Mutalib et al., Al-Qarinah dalam Hukum Hudud

Several preliminary studies have addressed the role of forensic evidence within the Shariah courts. Baharuddin[27] and Mohd Yusof[28] examined the admissibility of forensic evidence through the lens of *maqāṣid al-sharīʿah*. However, these studies did not specifically address the role of digital forensics. Khalil[29] also explored the potential of digital forensics as a means of proof in the Shariah context particularly in the form of *kitābah* (written evidence), *qarīnah* (circumstantial evidence), and expert opinion but did not foreground the procedural dimensions of digital forensic evidence, particularly the chain of custody, as a core issue. This omission constitutes a critical lacuna in Shariah evidentiary discourse. The admissibility of any forensic evidence begins with the establishment of an unbroken and verifiable chain of custody. Without it, such evidence no matter how scientifically valid cannot be accepted in court. Hence, addressing the procedural foundation of digital forensics is essential to ensure its integration into the Shariah legal process.

INSTITUTIONAL GAPS IN SHARIAH LEGAL FRAMEWORK

Although forensic evidence is becoming increasingly relevant in the prosecution of Shariah criminal offences, the procedural and legislative frameworks within Malaysia's Shariah legal system remain largely unprepared to accommodate it.[30] Most Syariah Criminal Procedure Enactments across the states do not contain any express provisions that govern the chain of custody or admissibility of electronic or digital

[27]Ahmad Syukran Baharuddin, "The Integration of Forensic Science Fundamentals and Al-Qarinah towards Achieving Maqasid Al-Shari'ah" (Doctor of Philosophy, Universiti Teknologi Malaysia, 2017).

[28]Syazwan Mohd Yusof, "Kebolehterimaan Keterangan Forensik Di Mahkamah Syariah Di Malaysia" (Sarjana Falsafah, 2019)

[29]Mohamad Khairudin Kallil and Ahmad Che Yaacob, "The Integration of Digital Forensics Science and Islamic Evidence Laws," *International Journal of Law, Government and Communication* 4, no. 17 (December 15, 2019): 61–70, https://doi.org/10.35631/ijlgc.417006.

[30]Mohamad Azhan Yahya, Ahmad Azam Mohd Shariff, and Suhaizad Saifuddin, "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, no. S1 (November 10, 2023): 143–64, https://doi.org/10.31436/iiumlj.v31iS1.874.

evidence. There exists an enforcement practice observed by religious enforcement officers (PPA), namely the Standing Instruction of the Director of the State Islamic Religious Department 2007, particularly Instructions 20 to 22 that provide for the process of handling objects seized. Although these procedures were initially designed for the seizure of physical evidence especially items requiring submission to the Department of Chemistry, they have also been applied in the handling of digital evidence. This lack of clear rules creates an institutional gap that affects both the consistency of judicial decisions and the reliability of digital forensic evidence in Shariah courts.

Unlike civil courts that operate under the Evidence Act 1950 which provides detailed rules for the admissibility of electronic records and implicitly demands a strict chain of custody. Shariah courts are governed by fragmented state-level laws. This law tends to emphasise classical categories of evidence such as *shahādah* or *iqrār*, with little or no provision for *qarīnah* in its modern digital form. For instance, the Syariah Court Evidence (Federal Territories) Act 1997 (Act 561) enumerates seven categories of admissible evidence but makes no mention of digital artefacts or forensic handling procedures. However, Section 33 Act 561 acknowledges the role of expert opinion in assisting the court when dealing with matters requiring scientific or technical expertise. This is crucial for digital forensics, as such evidence cannot be understood without specialist interpretation. Section 39 further underscores that when an opinion is treated as *qarīnah,* the grounds or tests upon which the opinion is based are also *qarīnah*. For example, a forensic expert may testify not only about his conclusions but also about the laboratory tests or digital analyses performed, which themselves carry evidentiary weight.

In 2020, the Syariah Judiciary issued Practice Direction No. 4 of 2020 on the submission of forensic evidence in Shariah court proceedings. This directive recognises the admissibility of forensic evidence but remains general, not prescribing how digital evidence should be preserved or chain of custody requirements implemented.

This inconsistency stems from the lack of clear procedures or adequate training among the PPA responsible for investigating Shariah criminal offences.[31] It should be emphasised that the admissibility of

[31]Mohamad Azhan Yahya and Ahmad Azam Mohd Shariff, "Proses Penggeledahan Keterangan Dokumen Elektronik Dalam Kes Jenayah

evidence in the Shariah criminal proceedings is highly dependent on the level of competence of the PPA in ensuring the integrity of digital devices or digital evidence is preserved throughout the process of storage and forensic examination at the investigation stage. These officers must ensure that the chain of custody remains unbroken throughout both processes as this aspect is an important basis to support the admissibility of evidence in court. Weakness in this aspect not only raises questions about technical competence but also challenges the fundamental principles of procedural justice and legal certainty that are at the core of civil and Shariah legal philosophies. Although reported Shariah cases rarely address digital evidence or chain of custody explicitly, lessons can be drawn from Malaysian civil criminal jurisprudence where such issues have been tested. For instance, in *Public Prosecutor v Lee Yau Ket* [2008] 4 MLJ 223, narcotics were rejected because the officer responsible during transfer was not identified which creating a fatal gap in custody.

The resulting absence of a codified chain of custody within the Shariah criminal procedure generates two major risks. On one hand, valuable digital evidence may be excluded from proceedings due to questions about its authenticity or reliability, thereby weakening the prosecution's case and potentially allowing offenders of serious moral and religious offences to go unpunished. On the other hand, improperly handled or contaminated digital evidence may be admitted and relied upon, raising the possibility of wrongful conviction based on flawed or manipulated information.

METHODOLOGY

This study adopts a qualitative doctrinal approach to examine the applicability of the CoC principles in the Shariah criminal proceedings involving digital forensic evidence. It involves critical analysis of statutory instruments such as the Evidence Act 1950, state-level Syariah Criminal Offences and Evidence Enactments, and relevant procedural laws to identify gaps and potential for integration. Key

Syariah: Searching Process in the Syariah Criminal Cases: Analysis the Admissibility of Electronic Document Evidence," *Journal of Muwafaqat* 5, no. 2 (October 31, 2022): 153–63, https://doi.org/10.53840/muwafaqat.v5i2.122.

Malaysian civil court decisions are reviewed to distil established CoC principles, with 18 purposively selected cases drawn from Lexis Nexis, CLJ Law, and MLJ databases. The selection focused on judgments that explicitly addressed CoC and offered substantive judicial reasoning on evidentiary continuity and integrity within the Malaysian jurisdiction, ensuring their relevance and adaptability to the Shariah context. Through thematic synthesis and comparative legal reasoning, the study evaluates how civil evidentiary parameters particularly regarding the CoC can be aligned with Islamic legal concepts thereby proposing a principled model for the procedural handling of digital evidence in Shariah courts.

FINDINGS AND DISCUSSION

Operational Continuity in the Chain of Custody: Technical Procedures for Forensic Digital Evidence in The Shariah Criminal Proceeding

It is widely recognised that digital forensic procedures typically follow five main phases: identification, collection, preservation, analysis, and presentation.[32] Some scholars have proposed models comprising four or even six phases, such variations do not reflect any fundamental or conceptual differences.[33] Rather, they differ only in how the frameworks organise and describe specific activities, without altering the core principles underpinning the forensic process.[34]

One of these core principles is the chain of custody which is rooted throughout all phases from the initial investigation to the final presentation of evidence in court. The chain of custody is an interactional process involving five principal entities: the first responder, the investigator, the prosecutor, the defence, and the court.

[32]Hamza Azam et al., "Cybercrime Unmasked: Investigating Cases and Digital Evidence," *International Journal of Emerging Multidisciplinaries: Computer Science & Artificial Intelligence* 2, no. 1 (November 25, 2023), https://doi.org/10.54938/ijemdcsai.2023.02.1.255.

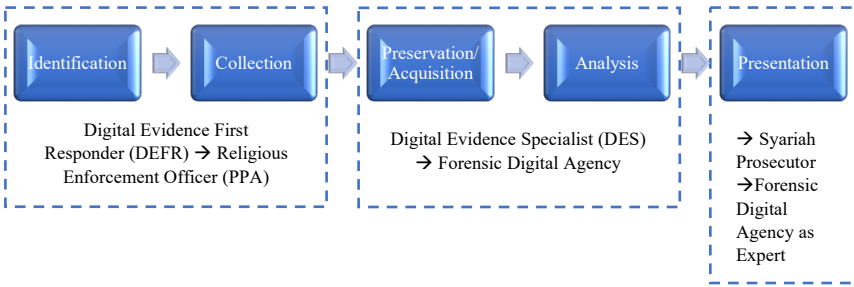
[33]Talib M. Jawad Abbas and Ahmed Salem Abdulmajeed, "Identifying Digital Forensic Frameworks Based on Processes Models," *Iraqi Journal of Science Special Issue* (January 14, 2021): 249–58, https://doi.org/10.24996/ijs.2021.si.1.35.

[34]Abbas and Abdulmajeed, "Identifying Digital Forensic Frameworks," 249.

The structure and interaction of these entities may vary depending on a country's legal framework.[35] Each phase of the digital forensic process may be conducted by a single individual or by multiple actors, depending on institutional capacities and jurisdictional arrangements. In Malaysia, particularly within the Shariah enforcement framework, the PPA typically serves as the Digital Evidence First Responder (DEFR) which the first to arrive at the scene of the incident.

The role of the PPA as DEFR is explicitly specified by the Syariah Criminal Procedure (Federal Territories) Act 1997 [Act 560]. Under Part IV, Section 63, PPAs are authorised to conduct searches and seizures with or without a warrant, subject to situational requirements. Section 15 further empowers them to search the body of a person suspected of committing a Shariah offence and to seize any item believed to be involved in the commission of that offence. These provisions provide the statutory mandate for PPA to act during the early investigative phase, particularly in identifying and securing digital devices or electronic materials that may constitute key evidence, thus fulfilling their legal role in upholding the integrity of digital forensic procedures.

In digital forensic practice, the phases of identification and collection are foundational steps that directly affect the reliability and admissibility of digital evidence. As the first responder in Shariah criminal investigations, the PPA plays the role of the DEFR with identifying and collecting potential digital evidence at the scene of the incident. Figure 1: Entities that involve all phases from the initial investigation to the final presentation of evidence in court.



[35]Giuliano Giova, "Improving Chain of Custody in Forensic Investigation of Electronic Digital Systems," *International Journal of Computer Science and Network Security* 11, no. 1 (2011): 1–9.

Figure 1 above illustrates the five interrelated phases of digital forensic practice, identification, collection, preservation/acquisition, analysis and presentation together with the entities responsible at each stage.

Based on ISO/IEC 27037:2012, in identification phase, the PPA must recognise both the physical form (e.g., mobile phones, laptops, USB drives) and the logical form (e.g., stored files, metadata, communication logs) of digital evidence. This phase involves conducting a thorough and systematic search, distinguishing potential sources of data and documenting all items and their relevance to the offence. Priority should be given to more volatile forms of data to prevent loss. The PPA must also account for possible hidden or remote sources of evidence such as cloud storage or network-attached systems, which may not be readily visible at the scene. All findings should be carefully documented, including the condition of the device, its location and whoever had access to it.

The collection phase involves physically securing and removing the identified devices to a laboratory and controlled environment for further analysis. Depending on whether a device is powered on or off, different tools and procedures must be used to avoid compromising the data. Supporting items such as password notes or power adaptors should also be collected. All actions must be documented, including labelling, photographing, and packaging of devices in a manner that preserves evidentiary integrity. Instruction 20 of the Standing Instruction of the Director of the State Islamic Religious Department 2007[36] also outlines the procedures for handling seized objects, including electronic document evidence, as follows:

1) All seized items must be registered and labeled with the item number, date, time, incident address, and case file number;
2) Officers must verify that the seized items correspond exactly with the list or confiscation form; (3) Perishable items must be photographed individually during the removal process;
3) A note must be made indicating the exact time each photograph was taken; and

[36]Standing Instruction of the Director of the State Islamic Religious Department 2007

4) Every transaction involving the submission or receipt of confiscated items must be recorded and accompanied by the receiver's signed declaration.

Critically, embedded within both these phases is the principle of the chain of custody, as outlined in ISO/IEC 27037:2012. The PPA as DEFR must be able to account for all data and devices while they are under their custody. A chain of custody records must be initiated at the point of collection and maintained throughout the lifecycle of the evidence. This record should trace the chronological handling, movement, and access to each item capturing details such as the unique evidence identifier, names of individuals accessing or transferring the evidence, times and locations of transfer, purposes of each movement, and any changes made to the evidence, including justifications and responsible personnel. In the context of Malaysian Shariah investigations as the Standing Instruction of the Director of the State Islamic Religious Department 2007, this responsibility rests with the PPA, who must ensure that every interaction with the digital evidence is fully documented and justified, thereby safeguarding the admissibility and probative value of the evidence in court.

Once collected, the evidence is transferred to certified digital forensic specialists (DES) such as those from the Royal Malaysia Police Forensics Department, the Malaysian Communications and Multimedia Commission or CyberSecurity Malaysia who carry out the preservation and analysis phases in accordance with technical standards and legal protocols. Upon completion, a forensic report is generated and returned to the PPA, who then bears the responsibility of presenting the evidence in the Shariah court, often in coordination with the Shariah prosecutor.

Once the forensic analysis is complete, the digital evidence along with the official forensic report is returned to the PPA under formal handover which requiring documented acknowledgements and signatures. The item is resealed and stored in the evidence room until the prosecution presentation phase. During trial, the digital evidence is presented by the shariah prosecutor, and the forensic digital expert may be called as an expert witness to explain technical findings, hash verifications and evidentiary relevance. Any inconsistency in the chain of custody, such as undocumented transfers or tampered seals, may render the evidence inadmissible. Therefore, strict adherence to these

procedures is paramount from the moment of seizure through to courtroom admission.

While the technical implementation of digital forensic procedures and chain of custody within Shariah criminal investigations through the operational role of the PPA illustrates the emerging procedural readiness at the enforcement level, there remains a significant gap in legal articulation and judicial reasoning concerning digital evidence within the Shariah court system. This is especially evident in the absence of explicit recognition or application of the chain of custody concept in Syariah legal instruments or reported case law.[37,38] To address this lacuna, the following section turns to the more developed evidentiary jurisprudence of Malaysian civil criminal courts. Although originating outside the Shariah legal framework, civil court precedents provide substantive guidance on how CoC is judicially interpreted, the consequences of its breach, and the evidentiary standards required for admissibility. These precedents provide important reference points that can be used to shape CoC principles suitable for the Shariah legal framework. Lessons from civil court cases, particularly on documentation, integrity of evidence, and expert verification, show how CoC can ensure that digital evidence remains reliable and trustworthy. Adapting these principles to Shariah courts is necessary as they now deal more frequently with offences involving technology, such as online gambling and cyber-enabled crimes. In this way, civil court experience offers a practical guide to strengthen evidentiary processes in Shariah courts and to secure the credibility of digital evidence presented in trials.

Principle From Civil Court Precedents Analysis as Benchmarks

In the context of Shariah criminal proceedings in Malaysia, the application of CoC principles has thus far been practiced in a limited

[37]Ahmad Azam Mohd Shariff et al., "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, no. 1 (April 30, 2022): 17–32, https://doi.org/10.53840/muwafaqat.v5i1.106.

[38]Yahya, Shariff, and Saifuddin, "Application of Principles of Chain of Evidence," 143.

and indirect manner. While procedures for handling seized items such as the registration, labeling, and documentation of electronic evidence are followed by religious enforcement authorities, these practices are not formally recognised under the term "chain of custody" within Shariah legal instruments or judicial reasoning. A survey of reported Shariah cases confirms the absence of any direct reference to CoC indicate either the lack of digital evidence-related prosecutions or a procedural gap in terminology and legal framework. However, this does not weaken the urgency of addressing the issue. As Shariah courts increasingly face crimes facilitated by digital platforms, they must proactively adapt to ensure that evidence integrity is preserved from seizure to adjudication. For example, online gambling cases, where digital devices such as mobile phones or laptops may contain betting applications, transaction records, and communication logs that are central to proving the offence. If these devices are not handled with proper documentation and transfer records, the defence may raise doubts about their authenticity and reliability. By adapting chain of custody principles, Shariah courts can ensure that such evidence remains credible and admissible, thereby strengthening the overall process of proof in technology-related offences.

Given the limitations in Shariah case law, this study refers to the jurisprudence of Malaysian civil courts, which offer a more developed foundation in dealing with CoC, particularly in criminal cases involving drug offences, electronic records, and biometric data. Although the evidentiary focus in these cases often centers around narcotics, the underlying judicial reasoning concerning the safeguarding, transmission, and authentication of evidence remains highly relevant. These civil court precedents provide essential procedural benchmarks for understanding how CoC is operationalised, the implications of any breach, and the parameters required for admissibility. Thus, this section draws on selected civil criminal cases to extract recurring CoC themes and formulate principles that may be adapted within the Shariah evidentiary structure to enhance procedural consistency and reliability.

Table 1. Shows Summary of 18 Selected Cases That Involve with Chain of Custody Issue

No.	Case	Chain of Custody Issue	Judicial Decision
1	*Public Prosecutor v Saiful Bahari* [2020] MLJU 2237	Failure to comply with laboratory certification and documentation requirements under Sections 31A(1A) and 37(k) of the Dangerous Drugs Act 1952	Evidence rejected due to incomplete CoC and unmitigated risk of manipulation
2	*Public Prosecutor v Ahmad Rizal* [2017] 6 MLJ 279	Break in transfer records; no explanation regarding who handled the sample between scene and lab	Evidence rejected; CoC interrupted and integrity compromised
3	*Public Prosecutor v Syed Mohd Faysal* [2004] 6 MLJ 303	Lack of proof of the specimen's origin; reliant solely on expert opinion without chain verification	Evidence inadmissible without complete CoC documentation
4	*Public Prosecutor v Lee Yau Ket* [2008] 4 MLJ 223	Absence of documentation identifying the officer responsible during transfer	Gap in CoC resulted in exclusion of evidence
5	*Anwar Ibrahim v Public Prosecutor* [2015] 2 MLJ 293	Suspected contamination and questionable documentation	Court scrutinised CoC thoroughly and emphasised the need for full documentation
6	*Gunalan v Public Prosecutor* [2004] 4 MLJ 489	Minor lapses in CoC did not affect the identity of the exhibit	Evidence accepted; deficiencies not fatal to evidentiary authenticity
7	*Public Prosecutor v Ngoforo* [2024] MLJU 3619	No fingerprint analysis, no clear photographic record, and unidentified owner	Accused acquitted; CoC weakness created reasonable doubt

8	*Yee Chien Hwee v Public Prosecutor* [2023] MLJU 2623	Alleged lack of CCTV and incomplete sealing	CoC proven complete; evidence admitted
9	*Public Prosecutor v Padmanathan* [2023] MLJU 1979	Missing physical urine bottle and slight weight discrepancy	No manipulation proven; evidence accepted
10	*Public Prosecutor v Jeffery Wong* [2023] MLJU 2843	Drugs not securely stored; discrepancies in registration dates	Evidence rejected; damaged CoC and no proven link between exhibit and accused
11	*Public Prosecutor v Hasamuddin* [1995] MLJU 206	Discrepancies in registration dates	Clerical error deemed non-fatal; evidence accepted as seal was intact
12	*Public Prosecutor v Mohd Ezri* [2015] MLJU 2112	DVD copy unreadable; integrity of third copy questionable	Evidence rejected; digital CoC found lacking
13	*Public Prosecutor v Jamal Md Yunos* [2022] MLJU 3752	No device, IP address, or forensic witness presented; primary evidence missing	Evidence rejected; digital CoC failed, charge not prima facie
14	*Mesnayo v Public Prosecutor* [2016] 2 MLJ 264	Absence of Section 90A certificate; lack of formal documentation challenged	Oral expert testimony accepted; evidence admitted under Section 90A(4)
15	*MMEA v Nyuyen Van Dai* [2020] MLJU 410	Edited video, suspicious metadata, and unverified camera	Evidence rejected; lack of digital integrity and weak CoC

16	*Mohd Asri v Public Prosecutor* [2024] MLJU 3493	No formal handover form; issues with exhibit labeling	Evidence accepted; forensic expert provided convincing explanation
17	*Public Prosecutor v Mohd Razef* [2023] MLJU 3027	Incomplete analytical report; critical evidence not printed	Evidence rejected; digital CoC deemed insufficient
18	*Azilah v Public Prosecutor* [2013] MLJU 802	Altered data, missing Section 90A certificate, and technical errors	Evidence rejected; CoC deemed weak and data manipulation occurred

Table 1 summarises 18 selected criminal cases in Malaysian courts that involved issues of CoC. The summary demonstrates how weaknesses in documentation, transfer records, and evidentiary authentication had a direct impact on judicial decisions, whether evidence was admitted or excluded. The CoC issues identified in these cases will subsequently be examined in greater depth and organised into key thematic categories, which are systematically presented in Table 2 as the foundation for establishing robust CoC parameters.

Table 2. Shows Analysis of 18 Selected Cases That Involve with Chain of Custody Issue

Case	**Code (Issue)**	**Theme**
PP v Ahmad Rizal [2017] 6 MLJ 279	Break in transfer records	Documentation and Continuity
PP v Lee Yau Ket [2008] 4 MLJ 223	Absence of documentation of officer in charge	
PP v Jeffery Wong [2023] MLJU 2843	Discrepancies in registration dates	
PP v Hasamuddin [1995] MLJU 206	Registration discrepancies (clerical error)	
Mohd Asri v PP [2024] MLJU 3493	No formal handover form; exhibit labelling issues	

PP v Saiful Bahari [2020] MLJU 2237	Non-compliance with lab certification & documentation (DDA 1952)	Integrity and Security of Evidence
Azilah v PP [2013] MLJU 802	Altered data; missing Section 90A certificate	
PP v Mohd Ezri [2015] MLJU 2112	DVD copy unreadable; integrity of copy questionable	
MMEA v Nyuyen Van Dai [2020] MLJU 410	Edited video; suspicious metadata	
PP v Jeffery Wong [2023] MLJU 2843	Drugs not securely stored	
PP v Mohd Razef [2023] MLJU 3027	Incomplete analytical report (digital)	
PP v Syed Mohd Faysal [2004] 6 MLJ 303	Origin of specimen not proven; reliance only on expert	Authentication and Provenance
Anwar Ibrahim v PP [2015] 2 MLJ 293	Suspected contamination; questionable documentation	
Mesnayo v PP [2016] 2 MLJ 264	Absence of Section 90A certificate; documentation challenged	
PP v Jamal Md Yunos [2022] MLJU 3752	No forensic witness; device/IP missing	Expert Verification and Support
PP v Padmanathan [2023] MLJU 1979	Expert explanation upheld urine evidence despite flaws	
Mohd Asri v PP [2024] MLJU 3493	Expert explanation compensating documentation gap	
Gunalan v PP [2004] 4 MLJ 489	Minor lapses in CoC not fatal	Corroboration and Judicial Discretion

Yee Chien Hwee v PP [2023] MLJU 2623	CoC proven complete despite sealing challenge	
PP v Hasamuddin [1995] MLJU 206	Registration error overlooked as seal intact	
PP v Ngoforo [2024] MLJU 3619	CoC weakness created reasonable doubt	

Table 2 summarises the findings from eighteen Malaysian court cases involving issues of CoC and organises them into five main themes. Analysis of these cases shows that the challenges are not random but instead recur around several common aspects: weaknesses in documentation, concerns over the integrity and security of the evidence, difficulties in verifying the provenance of evidence, the strength of expert testimony, and the role of judicial discretion.

This thematic organisation provides a more comprehensive view of how courts have assessed CoC weaknesses and the principles that guided their decisions. More significantly, it establishes a conceptual foundation for developing CoC parameters that are more appropriately tailored to digital forensic evidence in the Shariah courts.

Documentation and Continuity

Documentation and continuity are fundamental to the reliability of digital forensic evidence.[39] Any break or omission in the recording process undermines the CoC. Cases such as *PP v Ahmad Rizal* [2017] and *PP v Lee Yau Ket* [2008] highlight the consequences of poor documentation practices. In *Ahmad Rizal*, the failure to account for who handled the specimen between the crime scene and the laboratory resulted in the rejection of evidence. Similarly, in *Lee Yau Ket*, the absence of clear documentation identifying the officer in charge during transfer created a fatal gap.

[39]Gilbert Gilibrays Ocen et al., "Multi-Platform Process Flow Models and Algorithms for Extraction and Documentation of Digital Forensic Evidence from Mobile Devices," *ArXiv* (Cornell University) 1, no. 1 (January 1, 2022), https://doi.org/10.48550/arxiv.2203.13258.

Minor errors such as clerical errors can also potentially affect the continuity of the chain of evidence. In *PP v Hasamuddin* [1995], the discrepancy in registration dates raised concerns. However, the court still accepted the evidence because the evidence seal was found to be intact, thus showing that the continuity of the chain of evidence can sometimes potentially be preserved despite procedural laxity. Meanwhile, *PP v Jeffery Wong* [2023] revealed discrepancies in registration dates, adding to doubts about whether the evidence was handled consistently. The case of *Mohd Asri v PP* [2024] underscored the importance of formal handover records and proper labelling. The absence of such documentation initially weakened the CoC, but expert clarification later restored some credibility.

These cases demonstrate that chain of custody documentation is an aspect that cannot be ignored by the courts. However, judges assess the degree of documentation weakness differently depending on whether the integrity of the evidence is still preserved. As *Ocean et al.* point out, detailed recording of each step of the forensic investigation is essential to verify findings and defend them against challenges in court.

Integrity and Security of Evidence

The integrity and security of evidence refer to ensuring that exhibits remain free from contamination, tampering or substitution. In *PP v Saiful Bahari* [2020], the prosecution's failure to comply with statutory laboratory certification and documentation requirements under the Dangerous Drugs Act 1952 led to the exclusion of evidence. *Azilah v PP* [2013] similarly shows that altered data and the absence of a Section 90A certificate fatally undermined the integrity of digital records.

When a case item fails to be stored securely or revealed technical inconsistencies, the court has taken a firm stance by excluding the evidence. According to the case of *PP v Jeffery Wong* [2023], drugs that were not securely stored, coupled with registration inconsistencies, prompted the court to reject the evidence. *PP v Mohd Ezri* [2015] illustrates the risks of digital fragility, where unreadable copies cast doubt on evidentiary reliability. Likewise, in *MMEA v Nyuyen Van Dai* [2020], edited video footage with suspicious metadata led the court to reject it as unreliable. Finally, *PP v Mohd Razef* [2023] highlights the

consequences of incomplete analytical reports, as the absence of essential documentation rendered the digital CoC insufficient.

All these decisions have emphasised that the physical and digital security of case materials is a key pillar of the chain of custody principle. The Court has consistently emphasised that evidence cannot be relied upon if it is not preserved in a manner that excludes all possibility of contamination, manipulation or damage. Therefore, digital evidence must be protected from any form of tampering through proper sealing, secure storage and limited access controls to ensure its integrity.

Authentication and Provenance

Authentication and provenance focus on verifying the origin, identity, and unbroken lineage of evidence. In *PP v Syed Mohd Faysal* [2004], the absence of proof regarding the specimen's origin and reliance solely on expert testimony proved fatal to the prosecution's case. This reflects the principle that expert opinion cannot substitute for proper authentication.

Anwar Ibrahim v PP [2015] demonstrated that suspected contamination and questionable documentation cast significant doubt on the provenance of DNA evidence, prompting intense judicial scrutiny. Similarly, *Mesnayo v PP* [2016] illustrates the risks of bypassing formal statutory requirements, where the absence of a Section 90A certificate weakened authentication. However, in this case, the court accepted oral testimony under Section 90A(4), signalling that provenance concerns can sometimes be mitigated through judicial discretion.

Across these cases, authentication emerges as the cornerstone of admissibility. Courts expect prosecutors to prove not only that evidence exists but also that it is the same item seized, unaltered, and untainted. Any weakness in demonstrating this provenance leads to evidentiary exclusion.

Expert Verification and Support

Expert verification plays a decisive role in sustaining the admissibility of evidence when documentary or procedural flaws exist. In *PP v Jamal Md Yunos* [2022], the absence of forensic witnesses, as well as

missing devices and IP data, meant that expert verification was lacking altogether. The result was that the prosecution's digital evidence failed.

By contrast, in *PP v Padmanathan* [2023], although a physical urine bottle was missing and a slight weight discrepancy existed, the expert's convincing testimony persuaded the court to admit the evidence. Similarly, *Mohd Asri v PP* [2024] demonstrates how forensic experts can rehabilitate otherwise weak documentation through credible explanation.

These cases show that experts serve as crucial guarantors of evidentiary trust. Courts lean heavily on expert testimony to confirm the integrity, reliability and forensic soundness of evidence. Where experts are absent, evidence often collapses and where experts are persuasive, courts may be willing to tolerate minor flaws in CoC.

Corroboration and Judicial Discretion

Courts also exercise discretion in admitting evidence when minor CoC lapses exist, provided overall reliability is maintained. *Gunalan v PP* [2004] is a landmark case where minor documentation lapses did not undermine the identity of the exhibit and the court admitted the evidence. Likewise, in *Yee Chien Hwee v PP* [2023], although challenges were raised regarding sealing, the CoC was ultimately proven complete and the evidence accepted.

PP v Hasamuddin [1995] illustrates judicial pragmatism, where clerical errors in registration were overlooked because the seal was intact, thus preserving integrity. Conversely, *PP v Ngoforo* [2024] shows the limits of discretion: the absence of fingerprint analysis, photographic records, and proof of ownership created reasonable doubt, leading to acquittal.

These cases reflect the balancing approach taken by the courts. While strict adherence to the chain of custody principle is the overriding norm, judges will sometimes accept evidence with minor flaws if it is supported by the reliability of other evidence. However, when weaknesses in the chain of custody raise substantial doubts, acquittal becomes an inevitable outcome.

The five core parameters distilled from these cases documentation continuity, evidence integrity, authentication, expert

verification, and corroborative reliability represent essential safeguards that ensure evidentiary credibility from seizure to adjudication.

Although these principles have developed within the civil criminal framework, their procedural logic and evidentiary parameters are highly transferable to the Shariah context. Given the increasing prevalence of cyber-enabled Shariah offences, there is a compelling need for Shariah courts to adopt and institutionalise these parameters to avoid evidentiary gaps and judicial uncertainty.

Proposed Integration of Chain of Custody Parameters in Shariah Criminal Proceedings

The principle of CoC is not explicitly codified within Malaysia's Shariah criminal procedure laws. Nevertheless, its foundational rationale is consistent with the Qurʾānic and Sunnah imperatives of justice, trustworthiness, and integrity.[40] The Qurʾān mandates the upholding of justice (al-Naḥl 16:90), stresses the necessity of careful verification prior to accepting information (al-Ḥujurāt 49:6), and highlights the obligation of fulfilling responsibilities with integrity (al-Nisāʾ 4:58). The narrative of Prophet Yusuf (peace be upon him) also illustrates the notion of evidentiary continuity, as his garment was presented as proof which an early reflection of the CoC philosophy requiring the preservation of unbroken evidence.[41]

In the contemporary context, maintaining the chain of custody from the stage of investigation through to trial is crucial to ensuring the admissibility of digital evidence in court. Although the Standing Instruction of the Director of the State Islamic Religious Department addresses procedures for handling forensic materials such as chemical evidence,[42] it does not provide a detailed mechanism for CoC, especially in relation to digital evidence. Similarly, Practice Direction

[40]Ahmad Azam Mohd Shariff et al., "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, no. 1 (April 30, 2022): 17–32, https://doi.org/10.53840/muwafaqat.v5i1.106.

[41]Shariff et al., "Prinsip Rantaian Jagaan," 17.

[42]Yahya, Shariff, and Khalid, Proses Pengumpulan Keterangan Dokumen Elektronik.

No. 4 of 2020 on the Submission of Forensic Evidence in Syariah Court Proceedings merely affirms, in general terms, the admissibility of forensic evidence, without specifying the procedures necessary to safeguard its integrity. This absence of precise guidelines poses significant risks when digital evidence is tendered, given its susceptibility to manipulation, alteration, or contamination without detection.

Accordingly, it is proposed that either a dedicated practice direction be introduced, or Practice Direction No. 4 of 2020 be strengthened, to explicitly recognise the principle of CoC in Shariah criminal proceedings. Such a directive should detail five essential parameters that have proven pivotal within civil court practice—documentation continuity, evidentiary integrity, authentication, expert verification, and corroborative reliability,and adapt them to Shariah categories of evidence such as *qarīnah* and *al-khibrah*. This initiative would provide clear guidance for the PPA as Digital Evidence First Responders, enhance the credibility of digital evidence, and reinforce judicial confidence in its evaluation. Ultimately, institutionalising the CoC principle would not only align with the *maqāṣid al-sharīʿah* in upholding justice and transparency but also strengthen the capacity of the Shariah courts to effectively address the growing challenges of digital crime.

CONCLUSION

The absence of explicit legal articulation and judicial application of the CoC in Shariah criminal proceedings presents a significant evidentiary vacuum. This gap generates two critical risks. On one hand, valid digital evidence may be excluded from trials due to perceived deficiencies in authenticity or procedural documentation, thereby weakening the prosecution's case. On the other hand, improperly handled, undocumented or tampered digital evidence may be admitted without adequate scrutiny, increasing the likelihood of wrongful convictions based on compromised or manipulated information.

This study demonstrates that such risks can be mitigated by integrating two essential components: (1) the operational role of the PPA as the DEFR who initiates the identification and collection phases, and (2) the evidentiary principles of CoC derived from the

jurisprudence of Malaysian civil criminal courts. While Shariah legal texts and judgments have yet to formally acknowledge the CoC concept, field practices such as item labelling, photographic documentation, evidence registration, and handover protocol but there are already being implemented by PPA under administrative directives like the Standing Instruction of the Director of the State Islamic Religious Department.

However, for these practices to meaningfully impact the evidentiary threshold in Shariah courts, they must be reinforced through the adaptation of tested judicial reasoning from civil criminal cases. The five core CoC parameters, documentation continuity, evidence integrity, authentication and provenance, expert verification, and corroborative reliability serve as essential procedural safeguards to ensure the reliability and admissibility of digital forensic evidence from the moment of seizure to its presentation in court. In the Shariah context, these parameters could be institutionalised and expanded through a dedicated Practice Direction, or by strengthening Practice Direction No. 4 of 2020 on the Submission of Forensic Evidence in Syariah Court Proceedings.

As Shariah courts increasingly confront cyber-enabled offences, operational coherence between enforcement and judicial becomes indispensable. Institutionalising these CoC benchmarks not only prevents evidence from being unjustly rejected or misused but also aligns digital evidence management with the higher *Sharīʿah* objectives of justice (*ʿadl*), truth-revealing and public protection (*ḥifẓ al-nafs, ḥifẓ al-dīn*). The convergence of technical procedures and principled jurisprudence thus forms the foundation for a more coherent, reliable, and ethically sound digital evidentiary model within the Shariah criminal justice framework.

REFERENCES

Alias, Mohamad Aniq Aiman, Wan Abdul Fattah Wan Ismail, Ahmad Syukran Baharuddin, Hasnizam Hashim, and Tuan Muhammad Faris Hamzi Tuan Ibrahim. "Digital Forensics and The Admissibility of Electronic Evidence in Malaysian Syariah Courts: Towards A Standardised Legal Framework." *LexForensica: Journal of Forensic Justice and Socio-Legal Research* 2, no. 1 (2025): 84–91. https://doi.org/10.33102/6grx4619.

Alias, Mohamad Aniq Aiman, Wan Abdul Fattah Wan Ismail, Ahmad Syukran Baharuddin, and Muzaffar Syah Mallow. "Wasa'il Ithbat Dalam Undang-Undang Keterangan Islam: Analisis Perundangan Terhadap Keabsahan Dokumen Elektronik di Mahkamah Syariah Malaysia." *Malaysian Journal of Syariah and Law* 12, no. 3 (December 31, 2024): 689–700. https://doi.org/10.33102/mjsl.vol12no3.792.

Awate, A.S., B.N. Nandwalkar, M.R. Shahade, D.B. Mali, H.V. Patil, H.R. Waghare, and H.R. Patil. "Unmasking Attacker Identity behind the VPN." In *Advances in AI for Biomedical Instrumentation, Electronics and Computing*, 316–21. London: CRC Press, 2024. https://doi.org/10.1201/9781032644752-59.

Azam, Hamza, Mohammad Irfan Dulloo, Muhammad Hassan Majeed, Janelle Phang Hui Wan, Lee Tong Xin, and Siva Raja Sindiramutty. "Cybercrime Unmasked: Investigating Cases and Digital Evidence." *International Journal of Emerging Multidisciplinaries: Computer Science & Artificial Intelligence* 2, no. 1 (November 25, 2023). https://doi.org/10.54938/ijemdcsai.2023.02.1.255.Ocen,

Baharuddin, Ahmad Syukran. "*The Integration of Forensic Science Fundamentals and Al-Qarinah towards Achieving Maqasid Al-Shari'ah*." Doctor of Philosophy, Universiti Teknologi Malaysia, 2017.

Casey, Eoghan. *Digital Evidence and Computer Crime: Forensic Science, Computers, and the Internet*. Academic Press, Inc.6277 Sea Harbor Drive Orlando, FLUnited States, 2011.

Gilbert Gilibrays, Ocident Bongomin, Gilbert Barasa Mugeni, Mutua Stephen Makau, and Twaibu Semwogerere. "Multi-Platform Process Flow Models and Algorithms for Extraction and Documentation of Digital Forensic Evidence from Mobile Devices." *ArXiv* (Cornell University) 1, no. 1 (January 1, 2022). https://doi.org/10.48550/arxiv.2203.13258.

Giova, Giuliano. "Improving Chain of Custody in Forensic Investigation of Electronic Digital Systems." *International Journal of Computer Science and Network Security* 11, no. 1 (2011): 1–9.

Jawad Abbas, Talib M., and Ahmed Salem Abdulmajeed. "Identifying Digital Forensic Frameworks Based on Processes Models." *Iraqi Journal of Science* Special Issue (January 14, 2021): 249–58. https://doi.org/10.24996/ijs.2021.si.1.35.

Kallil, Mohamad Khairudin, and Ahmad Che Yaacob. "The Integration of Digital Forensics Science and Islamic Evidence Laws." *International Journal of Law, Government and Communication* 4, no. 17 (December 15, 2019): 61–70. https://doi.org/10.35631/ijlgc.417006.

Mohd Yusof, Syazwan. "Kebolehterimaan Keterangan Forensik Di Mahkamah Syariah Di Malaysia." Sarjana Falsafah, 2019.

Narasimhan, Premanand, and N. Kala. "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, no. 6 (December 12, 2024): 2438–50. https://doi.org/10.32628/CSEIT2410612443.

Nath, Souradip, Keb Summers, Jaejong Baek, and Gail-Joon Ahn. "Digital Evidence Chain of Custody: Navigating New Realities of Digital Forensics." In *IEEE 6th International Conference on Trust, Privacy and Security in Intelligent Systems, and Applications*, 11–20, 2024. https://doi.org/10.1109/tps-isa62245.2024.00012.

Parkavi, R., K. Divya, and V Sherry Ruth. "Digital Crime Evidence." In *Critical Concepts, Standards, and Techniques in Cyber Forensics*. IGI Global, 2020. https://doi.org/10.4018/978-1-7998-1558-7.ch008.

Saifuddin, Suhaizad. "Analisis Pemakaian Darjah Pembuktian Bagi Kesalahan Hudud Di Bawah Enakmen Jenayah Syariah Di Malaysia: Analysis of Applied the Standard of Proof for Hudud Offences under the Shariah Criminal Enactment in Malaysia." *Journal of Shariah Law Research* 6, no. 1 (2021): 89–108. https://jati.um.edu.my/index.php/JSLR/article/view/30154.

Shariff, Ahmad Azam Mohd, Mohamad Azhan Yahya, Ramalinggam Rajamanickam, Melissa Hsu Tzu-Hsin, Muhammad Muhaimin Mohd Subki, Nurasyraf Fahmi Azahari, Jeevitha Raja, and Syaidatul Syaffiqa Muhamad. "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, no. 1 (April 30, 2022): 17–32. https://doi.org/10.53840/muwafaqat.v5i1.106.

Suara Keadilan. "Media Sosial: MCMC Minta Hampir 19,000 Kandungan Langgar Peraturan Diturunkan." Suara Keadilan, January 21, 2025. https://www.suarakeadilan.my/post/media-sosial-mcmc-minta-hampir-19-000-kandungan-langgar-peraturan-diturunkan.

Syarbaini, Ahmad. "Konsep Ta'zir Menurut Perspektif Hukum Pidana Islam." *Jurnal Tahqiqa: Jurnal Ilmiah Pemikiran Hukum Islam* 17, no. 2 (July 31, 2023): 37–48. https://doi.org/10.61393/tahqiqa.v17i2.167.

Radhi, Mohamed. "Fahmi: Malaysia Lost RM1.2b to Online Crimes This Year." NST Online. New Straits Times, December 9, 2024. https://www.nst.com.my/news/nation/2024/12/1145948/fahmi-malaysia-lost-rm12b-online-crimes-year.

Thangamuthu, Poongodi, Anu Rathee, Suresh Palanimuthu, and Balamurugan Balusamy. "Encyclopedia of Criminal Activities and the Deep Web." In *IGI Global EBooks*, 1–22. IGI Global, 2020. https://doi.org/10.4018/978-1-5225-9715-5.ch001.

Tuan Ibrahim, Tuan Muhammad Faris Hamzi, Mohamad Aniq Aiman Alias, Nasrul Hisyam nor Muhamad, and Ahmad Syukran Baharuddin. "Pembuktian Forensik Digital Di Mahkamah Syariah: Kerangka Kebolehterimaan Dan Integriti Dalam

Jenayah Syariah." *Journal of Muwafaqat* 8, no. 2 (October 31, 2025): 78–100. https://doi.org/10.53840/muwafaqat.v8i2.197.

Tuan Ibrahim, Tuan Muhammad Faris Hamzi, Nasrul Hisyam Nor Muhamad, Mohamad Aniq Aiman Alias, and Ahmad Syukran Baharuddin. "Fiqh al-Waqi': Teras revolusi keterangan forensik digital dalam membendung jenayah Syariah siber." *Jurnal 'Ulwan* 10, no. 1 (2025): 28-46.

Tuan Ibrahim, Tuan Muhammad Faris Hamzi, Muhammad Sobri Faisal, Mohamad Aniq Aiman Alias, and Ahmad Syukran Baharuddin. "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, no. 2 (July 31, 2025): 263–82. https://doi.org/10.37052/kanun.37(2)no4.

Tuan Ibrahim, Tuan Muhammad Faris Hamzi, Mohamad Aniq Aiman Alias, and Ahmad Syukran Baharuddin. "A Preliminary Review of Digital Forensics as A Means of Proof in Modern Syariah Criminal Offences from a Maqasid Al-Shari'ah Perspective." *Syariah and Law Discourse | Diskusi Syariah dan Undang-Undang* 6, no. 1 (2025): 1–6. https://fsuproceedings.usim.edu.my/index.php/dsl/article/view/33.

Vala, Jaydevsinh B, and Vipul M Vekariya. "The Role and Importance of Digital Forensics and Digital Evidence in Cyber Crime Detection." *International Journal of Life Sciences, Biotechnology and Pharma Research* 13, no. 6 (July 1, 2024): 413–20. https://doi.org/10.69605/ijlbpr_13.6.2024.80.

Yahya, Mohamad Azhan, Ahmad Azam Mohd Shariff, and Nurul Nisa Khalid. Proses Pengumpulan Keterangan Dokumen Elektronik. Penerbit UKM, 2024.

Yahya, Mohamad Azhan, Ahmad Azam Mohd Shariff, and Suhaizad Saifuddin. "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, no. S1 (November 10, 2023): 143–64. https://doi.org/10.31436/iiumlj.v31iS1.874.

Yahya, Mohamad Azhan, and Ahmad Azam Mohd Shariff. "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, no. 2 (October 31, 2022): 153–63. https://doi.org/10.53840/muwafaqat.v5i2.122.

Wan Ismail, Wan Abdul Fattah, Hasnizam Hashim, Zulfaqar Mamat, Lukman Abdul Mutalib, Ahmad Syukran Baharuddin, and Norma Jusof. 2021. "Sumpah Nafy Al-'Ilmi Menurut Undang-Undang Keterangan Islam Di Malaysia: Nafy Al-'Ilmi Oath According to Islamic Law of Evidence in Malaysia". *AL-MAQASID: The International Journal of Maqasid Studies and Advanced Islamic Research* 2 (2). :25-37. https://doi.org/ 10.55265/almaqasid.v2i2.11.