

## EVALUATING ELECTRONIC EVIDENCE IN MALAYSIAN CIVIL COURTS: CURRENT ADMISSIBILITY AND FUTURE LEGAL DIRECTIONS

i,ii,\*Mohamad Aniq Aiman Alias, <sup>i,ii</sup>Wan Abdul Fattah Wan Ismail, <sup>i,ii,iii,iv</sup>Ahmad Syukran Baharuddin, <sup>i,ii</sup>Hasnizam Hashim & <sup>v</sup>Tuan Muhammad Faris Hamzi Tuan Ibrahim

<sup>i</sup> Faculty of Syariah and Law, Universiti Sains Islam Malaysia (USIM), 71800, Nilai, Negeri Sembilan, Malaysia

<sup>ii</sup> Centre of Research for Fiqh Forensics and Judiciary (CFORSJ), Faculty of Syariah and Law, Universiti Sains Islam Malaysia (USIM), 71800, Nilai, Negeri Sembilan, Malaysia

<sup>iii</sup> International Advisory Board Member, Mejellat Al-Afaq wa Al-Maarif (JSKP), Faculty of Humanities, Islamic Sciences and Civilization, University Amar Telidji of Laghouat, BP 37G, Road of Gharadaia, 03000 Laghouat, Algeria

<sup>iv</sup> Associate Editor, Journal of Contemporary Maqasid Studies, Maqasid Institute, United States of America (USA)

<sup>v</sup> Faculty of Social Sciences and Humanities, Universiti Teknologi Malaysia (UTM), 81310, Skudai, Johor, Malaysia

\*(Corresponding author) e-mail: [aniqalias@usim.edu.my](mailto:aniqalias@usim.edu.my)

### ABSTRACT

In the digital age, various forms of new evidence have emerged, including the use of electronic documents. Within the context of Malaysian civil law, the scope and clarity of the admissibility of electronic documents have expanded, covering criminal, commercial, and various other cases. Against this backdrop, this study aims to analyze the rules governing the admissibility of electronic documents in Malaysian civil courts, explore their practical application, and address the associated challenges and technological implications. A qualitative approach was employed, using document analysis of books, theses, case reports, legal provisions, journal articles, websites, and other relevant materials. The data collected was then analyzed and categorized into subthemes. The findings reveal that there are specific provisions for the admissibility of electronic documents. Section 3 of the Evidence Act 1950 [Act 56] generally recognizes electronic documents as admissible evidence, while Sections 90A, 90B, and 90C further clarify the conditions for their acceptance in civil court. Despite this legal framework, key challenges remain, particularly concerning the authenticity, integrity, and reliability of electronic documents. Given these challenges, this study is significant in evaluating the adequacy of the current legal framework governing the admissibility of electronic documents in Malaysian civil courts. It highlights the need to assess whether the existing provisions sufficiently address the complexities introduced by technological advancements. In conclusion, while electronic evidence is broadly accepted in civil courts, the rapid pace of technological development continues to introduce new challenges. These evolving challenges underscore the importance of ongoing research and legal reforms to ensure that the framework for electronic evidence remains robust and adaptable.

**Keywords:** *electronic document, electronic evidence, Malaysian Civil court, admissibility, legal framework*

## Introduction

In the digital era, the role of e-documents or electronic documents in judicial processes has become increasingly central, necessitating a closer examination of legal frameworks globally (Stoykova, 2023). Like many other jurisdictions, Malaysia has faced the challenge of integrating electronic documents into its legal system, prompting amendments to its laws to accommodate this new form of evidence, especially under the Malaysian Syariah court (Wan Ismail et al., 2023; Alias et al., 2021). The Evidence Act 1950 [Act 56], particularly through Sections 90A, 90B, and 90C, is the cornerstone for the admissibility of electronic documents in civil proceedings (Kallil & Che Yaacob, 2019). This legislative evolution underscores an essential shift towards recognizing and standardizing digital evidence in courtrooms.

However, integrating electronic documents into the legal system has not been without challenges. Significant gaps exist in how electronic documents are handled, authenticated, and integrated into the legal framework (Abdul Hadi & Paino, 2016). These gaps include verifying the authenticity and integrity of electronic documents, training legal professionals to understand technological intricacies, and aligning legal practices with rapid technological advancements (Mohamad, 2019). These issues highlight the need for a detailed study to assess the current legislative measures and their efficacy in dealing with electronic documents.

This study, therefore, aims to achieve the following objectives: critically analyze the current legal framework governing electronic documents in Malaysia, examine the legal rules on the admissibility of electronic documents in Malaysian civil courts, explore the admissibility of electronic documents in these courts and addressing the practical challenges and technological implications. By exploring these aspects, the study seeks to offer insights into best practices and potential areas for improvement in Malaysian law.

### The Current Legal Framework Governing Electronic Documents in Malaysia

The Evidence Act 1950 [Act 56] is the cornerstone of the legal framework for the admissibility of electronic documents in Malaysian courts. Since its inception, the Act has undergone several amendments to accommodate the complexities of electronic evidence, reflecting the evolving landscape of technology and its integration into the legal system (Abdullah Kahar et al., 2021; Lee, 2019). This discussion explores these amendments and the sections pertinent to electronic documents, clarifying the legal standards and procedures governing their admissibility.

According to Section 3 of the Evidence Act 1950 [Act 56]:

"document" means any matter expressed, described, or howsoever represented, upon any substance, material, thing or article, including any matter embodied in a disc, tape, film, sound track or other device whatsoever, by means of--

- (a) letters, figures, marks, symbols, signals, signs, or other forms of expression, description, or representation whatsoever;
- (b) any visual recording (whether of still or moving images);
- (c) any sound recording, or any electronic, magnetic, mechanical or other recording whatsoever and howsoever made, or any sounds, electronic impulses, or other data whatsoever;
- (d) a recording, or transmission, over a distance of any matter by any, or any combination, of the means mentioned in paragraph (a), (b) or (c), or by more than one of the means mentioned in paragraphs (a), (b), (c) and (d), intended to be used or which may be used for the purpose of expressing, describing, or howsoever representing, that matter;

From this section, the electronic document is generally accepted as court evidence. Section 90A, 90B and 90C of the Evidence Act 1950 [Act 56] further explain the admissibility of electronic documents as evidence in civil court.

One significant amendment to the Evidence Act 1950 [Act 56] came from the inclusion of Section 90A. Section 90A of the Evidence Act 1950 [Act 56], with seven subsections that contained the admissibility of documents produced by computers, stated:

**Section 90A.**

(1) In any criminal or civil proceeding a document produced by a computer, or a statement contained in such document, shall be admissible as evidence of any fact stated therein if the document was produced by the computer in the course of its ordinary use, whether or not the person tendering the same is the maker of such document or statement.

(2) For the purposes of this section it may be proved that a document was produced by a computer in the course of its ordinary use by tendering to the court a certificate signed by a person who either before or after the production of the document by the computer is responsible for the management of the operation of that computer, or for the conduct of the activities for which that computer was used.

(3) (a) It shall be sufficient, in a certificate given under subsection (2), for a matter to be stated to the best of the knowledge and belief of the person stating it.

(b) A certificate given under subsection (2) shall be admissible in evidence as prima facie proof of all matters stated in it without proof of signature of the person who gave the certificate.

(4) Where a certificate is given under subsection (2), it shall be presumed that the computer referred to in the certificate was in good working order and was operating properly in all respects throughout the material part of the period during which the document was produced.

(5) A document shall be deemed to have been produced by a computer whether it was produced by it directly or by means of any appropriate equipment, and whether or not there was any direct or indirect human intervention.

(6) A document produced by a computer, or a statement contained in such document, shall be admissible in evidence whether or not it was produced by the computer after the commencement of the criminal or civil proceeding or after the commencement of any investigation or inquiry in relation to the criminal or civil proceeding or such investigation or inquiry, and any document so produced by a computer shall be deemed to be produced by the computer in the course of its ordinary use.

(7) Notwithstanding anything contained in this section, a document produced by a computer, or a statement contained in such document, shall not be admissible in evidence in any criminal proceeding, where it is given in evidence by or on behalf of the person who is charged with an offence in such proceeding the person so charged with the offence being a person who was—

(a) responsible for the management of the operation of that computer or for the conduct of the activities for which that computer was used; or

(b) in any manner or to any extent involved, directly or indirectly, in the production of the document by the computer.

According to Section 90A, an electronic record produced by a computer is considered a document and admissible as evidence in court, provided certain criteria are met. These criteria focus on the regular use of the computer for certain activities, the computer's operation during the period in question, and how the data was generated, stored, or transmitted (Mohamed Arifin, 2020; Mohammad, 2019). In the case of *Lim Pang Cheong v. Tan Sri Dato' Dr. Rozali Ismail & Ors* [2012] 2 CLJ 849, text messages were deemed to meet the requirements of Section 90A (1) after being confirmed by the oral testimony of relevant witnesses.

Further to Section 90A, Sections 90B and 90C outline the conditions under which electronic records and digital signatures are considered secure. Section 90B of the Evidence Act 1950 [Act 56] regarding the weight to be attached to a document, or statement contained in the document, admitted by provide of section 90A, stated:

### **Section 90B**

In estimating the weight, if any, to be attached to a document, or a statement contained in a document, admitted by virtue of section 90A, the court—

(a) may draw any reasonable inference from circumstances relating to the document or the statement, including the manner and purpose of its creation, or its accuracy or otherwise:

(b) shall have regard to—

(i) the interval of time between the occurrence or existence of the facts stated in the document or statement, and the supply of the relevant information or matter into the computer; and

(ii) whether or not the person who supplies, or any person concerned with the supply of, such information or the custody of the document, or the document containing the statement, had any incentive to conceal or misrepresent all or any of the facts stated in the document or statement.

Section 90B deals with the authenticity of an electronic record, stipulating that a computer must produce the record during regular activities to provide a reliable basis for ensuring its integrity. It also outlines the weights that must be applied to relevant computer evidence, allowing the court to make reasonable inferences based on the circumstances of a document or statement, including its creation method, purpose, and accuracy (Mohamad, 2019). This encompasses the document's construction technique, purpose, and originality. The section specifies the timeframe between the occurrence of the facts stated in the document or statement and the input of the relevant data or information into the computer. Additionally, it considers whether the person providing the information, or anyone connected with the provision or storage of such information or the document containing the statement, has any motive to conceal or distort all or any of the facts stated in the document.

Meanwhile, Section 90C addresses digital signatures, providing them with the same legal standing as handwritten signatures, provided they adhere to prescribed security procedures. In the Section 90C of the Evidence Act 1950 [Act 56] stated:

### **Section 90C**

The provisions of sections 90A and 90B shall prevail and have full force and effect notwithstanding anything inconsistent therewith, or contrary thereto, contained in any other provision of this Act, or in the Bankers' Books (Evidence) Act 1949 [Act 33], or in any provision of any written law relating to certification, production or extraction of documents or in any rule of law or practice relating to production, admission, or proof, of evidence in any criminal or civil proceeding.

Section 90C, on the other hand, stipulates that Sections 90A and 90B have full authority and effect, notwithstanding any provisions in this Act that are inconsistent with or contrary to them, as well as any provisions in the Bankers' Books (Evidence) Act 1949, or any rule of law. This includes any laws or procedures related to the production, processing, or proving of evidence in any criminal or civil proceeding and any provisions of written legislation concerning document certification, production, or extraction.

## Legal Rules on the Admissibility of Electronic Documents in Malaysian Civil Courts

The legal rules on the admissibility of electronic documents in Malaysian civil courts reflect an ongoing adaptation to modern evidence methods and the evaluation of electronic documents. This evolution is crucial given that electronic evidence is now a prevalent source of proof in legal proceedings, and courts must resolve related issues decisively (Moussa, 2021).

Both civil and Syariah laws in Malaysia generally recognize the admissibility of electronic or computer evidence. For civil courts, relevant legislation includes the Evidence Act of 1950 [Act 56], the Criminal Procedure Code, the Rules of Court 2012, and the Penal Code. The Administration of Islamic Law Act governs Syariah courts, Syariah Court Evidence Act, Syariah Court Civil Procedure Act, Syariah Criminal Procedure Act, and Syariah Criminal Offences Act. The table below summarizes the key legal provisions under Malaysian civil law concerning the admissibility of electronic documents:

**Table 1:** Summary of Legal Provisions on the Admissibility of Electronic Documents in Malaysian Civil Law

No.	Legal Provision	Subject	Explanation
1.	Section 3	Definition of documents	A "document" includes data produced, stored, or transmitted through electronic means such as digital data or electronic signals.
2.	Section 90A	Admissibility of computer documents	Computer documents are admissible if generated during the ordinary use of a computer. Certification by a responsible person is required to prove authenticity.
3.	Section 90B	Inference based on circumstances	Courts may infer the reliability of a document based on the circumstances of its creation, including the time gap between the facts and the computer input.
4.	Section 90C	Precedence of provisions	Sections 90A and 90B take precedence over conflicting laws, ensuring electronic documents are admitted under a clear and authoritative framework.

Source: Evidence Act 1950 [Act 56]

These provisions demonstrate Malaysia's effort to keep pace with technological advancements while maintaining the integrity of evidence in legal proceedings. Continuous updates to the legal framework are essential to ensure the effective handling and evaluation of electronic documents in court.

Under Section 3 of the Evidence Act 1950 [Act 56], evidence can take various forms, including electronic documents, which are increasingly significant in court proceedings. This section acknowledges that a "document" may consist of data expressed through various means, including electronic impulses, data stored digitally, or even transmitted over a distance, covering a wide array of digital and electronic media forms. This broad definition facilitates the inclusion of modern digital data formats within the scope of admissible evidence, thus reflecting the adaptability of Malaysian law to technological advancements.

Section 90A of the Evidence Act particularly addresses the admissibility of computer documents, specifying that such documents are admissible if produced by the computer during its ordinary use. This section implies a reliance on the regular functioning and reliability of computing systems to generate evidence, highlighting the legal system's trust in automated processes under controlled conditions. The section also facilitates the certification process, allowing a responsible person to certify the correct functioning of the computer, thus simplifying the proof of authenticity and integrity of electronically generated documents.

However, sections 90B and 90C further refine the requirements for such admissibility, emphasizing the need for reliability and accuracy in the digital documents' creation and maintenance. Section 90B allows courts to draw inferences based on the circumstances surrounding the creation of the electronic document, including the time elapsed between the facts stated and the information entered the computer. This consideration is crucial in ensuring that the data reflects an accurate and timely representation of the facts. Section 90C asserts the precedence of sections 90A and 90B over other conflicting laws,

underscoring the importance of maintaining a clear and authoritative framework for the admissibility of electronic evidence.

The integration of these sections into the Evidence Act represents a robust response to the challenges posed by electronic documents in legal settings. By allowing detailed provisions for their admissibility and the assessment of their credibility, Malaysian law endeavors to keep pace with technological evolution while ensuring that justice remains based on reliable and accurate evidence. Thus, as technology advances, continuous updates to these legal frameworks are imperative to align with new digital realities, ensuring that the legal system remains effective in assessing and utilizing electronic documents as evidence.

### The Admissibility of Electronic documents in Malaysian Civil Courts

The admissibility of electronic documents in civil court cases in Malaysia involves stringent processes and legal scrutiny to ensure justice is served accurately (Mohamad Zain et al., 2017). Various cases have highlighted the complexities and legal criteria digital evidence must meet to be valid and admissible in court as shown in table 2.

**Table 2.** Summary of Key Cases on the Admissibility of Electronic Documents in Malaysian Law

No.	Case	Issue	Description
1.	<i>Geoforce East Sdn Bhd v. Melati Evergreen Sdn Bhd &amp; Another Appeal</i> [2020] 1 LNS 862	Acceptance of electronic documents with digital signatures	Court recognized the legitimacy of digitally signed documents, affirming their binding nature under Malaysian law. Established precedent for accepting digital signatures.
2.	<i>Public Prosecutor v Goh Hoe Cheong &amp; Anor</i> [2007] 7 CLJ 68	Exclusion of digital evidence due to procedural deficiencies	Electronic check-in baggage tags were excluded as there was no oral testimony or certification under Section 90A (1) to establish chain of custody and control.
3.	<i>Hanafi bin Mat Hassan v Public Prosecutor</i> [2006] 4 MLJ 134	Compliance with technical requirements for admitting digital evidence	The court emphasized the need for a certificate from the person managing the computer's operations, as required by Section 90A (2) of the Evidence Act 1950 [Act 56].

One notable case is *Geoforce East Sdn Bhd v. Melati Evergreen Sdn Bhd & Another Appeal* [2020] 1 LNS 862, which illustrates the acceptance of electronic documents in legal proceedings. In this instance, THK used a digital signature on behalf of MESB. The court recognized the legitimacy and binding nature of digitally signed documents, affirming the legal standing of digital signatures under Malaysian law. This case sets a precedent for accepting electronic documents, provided they are executed following established legal standards.

Conversely, the *Public Prosecutor v Goh Hoe Cheong & Anor* [2007] 7 CLJ 68, presents scenario where digital evidence was not admitted due to procedural shortcomings. The electronically generated check-in baggage tags were excluded because there was no oral testimony or requisite certification under Section 90A (1) of the Evidence Act 1950 [Act 56] to establish the evidence's chain of custody and control. This case highlights the importance of adhering to specific procedural requirements to ensure the integrity and authenticity of digital evidence.

Furthermore, the case of *Hanafi bin Mat Hassan v Public Prosecutor* [2006] 4 MLJ 134 delves into the technical compliance of digital evidence, specifically the performance and reliability of machines producing such evidence. The pivotal question was whether the necessary conditions of Section 90A (2) of the Evidence Act 1950 [Act 56] had been met, which includes obtaining a certificate from the person managing the computer's operations. This requirement underscores the necessity of certifiable verification to support digital documents' reliability in legal contexts.

These cases collectively emphasize that while digital documents are increasingly recognized as valid evidence, their admissibility hinges on rigorous verification processes and legal compliance. Courts must scrutinize how digital evidence is collected, maintained, and presented to ensure it meets the high standards required for legal proceedings. This ensures that the evidence is relevant and secured against potential tampering or damage, maintaining the integrity of the judicial process.

Thus, the evolving landscape of digital evidence in Malaysian civil courts necessitates continuous legal education and adaptation to incorporate technological advancements while upholding the rigorous standards of evidence law. Ensuring the proper handling and authentication of digital documents is crucial for their admissibility and effectiveness in achieving judicial fairness.

### **Practical Challenges and Technological Implications**

Integrating electronic documents into legal proceedings presents several practical challenges for courts and legal practitioners in Malaysia, primarily centered on establishing such documents' authenticity, integrity, and reliability. These challenges are compounded by the rapid pace of technological advancements, which continually reshape the landscape of digital evidence.

A primary concern is the authenticity of electronic documents (Mohamad, 2019). Authenticity involves verifying that the document is what it purports to be and has not been altered or tampered with since its creation. This can be particularly challenging as digital files can be easily altered without leaving physical traces of such changes. For instance, metadata within electronic documents can be manipulated, affecting the document's credibility as evidence unless properly verified. Legal practitioners often rely on forensic methods to establish authenticity, such as digital fingerprinting and hash functions, which create a unique digital identifier for documents that would change if any alteration is made.

Another significant challenge is ensuring the integrity of electronic documents, which relates to maintaining and proving that the document's state has remained unchanged (Tenhunen, 1997). This aspect is critical because the legal admissibility of such documents hinges on their integrity from the point of creation to their presentation in court. Technological solutions such as blockchain technology offer potential methods for maintaining integrity, providing a tamper-evident, chronological chain of custody for digital documents. However, adopting and understanding such technologies in legal contexts is still evolving, necessitating training and updates to legal frameworks.

The reliability of electronic documents also presents a challenge (Duranti, 2002). This depends not only on the document itself but on the reliability of the systems and processes used to create, store, and transmit these documents. Systems must be secure and free from vulnerabilities that could allow unauthorized access or changes to the data. Courts often must rely on expert testimony to ascertain the reliability of the technological systems in handling such documents. This reliance on expert assessments can introduce complexities into legal proceedings, potentially prolonging them and adding to the costs.

Moreover, the technological advancements that impact electronic documents extend to the tools used for their analysis and presentation in court (Plekhanov et al., 2023). While developing more sophisticated digital forensic tools helps address some challenges, legal professionals must stay continually updated through training and professional development. This need for ongoing education represents an additional challenge but is essential for the competent handling of digital evidence.

In conclusion, while technological advancements provide powerful tools for managing electronic documents, they also bring significant challenges that must be addressed through both technological solutions and legal measures. Ensuring the admissibility of digital evidence requires advanced forensic techniques and a robust legal understanding and framework that can adapt to the fast-paced changes inherent in technology. This necessitates a concerted effort from all stakeholders, including legal institutions, practitioners, and technologists, to ensure that handling electronic documents in court settings is effective and just.



## Conclusion

The legal framework governing the admissibility of electronic documents in Malaysian civil courts demonstrates a strong and evolving response to the complexities of digital evidence. Key provisions in the Evidence Act 1950 [Act 56], particularly Sections 90A, 90B, and 90C, offer essential guidelines that ensure the authenticity, reliability, and proper certification of electronic documents. These provisions, while robust, are not without challenges, particularly as rapid technological advancements continue to introduce new forms of digital evidence and potential vulnerabilities. This study highlights both the strengths and limitations of the current legal framework. While electronic evidence is broadly accepted, concerns surrounding its integrity and the practical challenges of verification and authentication persist. The findings underscore the need for continuous legal reforms that not only address existing gaps but also anticipate future developments in digital technology. Legal practitioners must remain well-informed and adaptive to these changes, ensuring that their expertise evolves in line with technological advancements. Moving forward, collaboration between legal and technological experts, alongside ongoing education for legal practitioners, is crucial. By doing so, Malaysia's civil courts can maintain a fair, effective, and forward-thinking legal system that upholds justice while safeguarding the integrity of electronic evidence. In conclusion, the continual refinement of legal provisions and practices will be essential to keeping pace with technological innovation, ensuring that the admissibility of electronic documents remains secure, reliable, and just within the Malaysian legal landscape.

## References

- Abdul Hadi, K. A., & Paino, H. (2016). Legal perspectives towards forgery, fraud and falsification of documents: Recent development. *Malaysian Accounting Review*, 15(2). <http://dx.doi.org/10.24191/mar.v15i2.589>
- Alias, M. A. A. (2022). *The falsification of documents in marriage cases under the civil and Syariah courts in Malaysia: An appraisal analysis* (Master's dissertation). Universiti Sains Islam Malaysia, Nilai, Negeri Sembilan.
- Alias, M. A. A., Wan Ismail, W. A. F., Baharuddin, A. S., & Abdul Mutalib, L. (2021a). Legal analysis of Syariah court evidence law on digital document as evidence and its admissibility in court proceedings: Analisis perundangan bagi undang-undang keterangan Mahkamah Syariah terhadap dokumen digital sebagai kaedah pembuktian dan kebolehterimaannya dalam prosiding mahkamah. *Journal of Management and Muamalah*, 11(2), 54-64.
- Cameron, S. (2011). *Digital evidence*. FBI Law Enforcement Bulletin, 14-20.
- Clancy, T. K. (2011). *Cyber crime and digital evidence: Materials and Cases*. Lexic Nexis.
- Duranti, L. (2002). The reliability and authenticity of electronic records. In *Preservation of the Integrity of Electronic Records* (pp. 45-58). Springer. [https://doi.org/10.1007/978-94-015-9892-7\\_3](https://doi.org/10.1007/978-94-015-9892-7_3)
- Evidence Act 1950 [Act 56].
- Geoforce East Sdn Bhd v. Melati Evergreen Sdn Bhd & Another Appeal* [2020] 1 LNS 862.
- Hanafi bin Mat Hassan v Public Prosecutor* [2006] 4 MLJ 134.
- Haneef, S. S. S. (2006). Modern means of proof: Legal basis for its accomodation in Islamic law. *Arab Law Quarterly*, 20(4), 334-364.
- Kallil, M. K., & Che Yaacob, A. (2019). The Integration of Digital Forensic Science and Islaimc Evidence Laws. *International Journal of Law, Government and Communication*, 4(17), 61-70.
- Lee, E. (2019, January 1). Evidence Act: E-evidence & e-forensics. Lee & Poh Partnership. <https://lpplaw.my/insights/e-articles/evidence-e-evidence-e-forensics/>
- Lim Pang Cheong v. Tan Sri Dato' Dr. Rozali Ismail & Ors* [2012] 2 CLJ 849.
- Mohamad Zain, N. A., Wan Mohamad Saman, W. S., & Mat Yatin, S. F. (2017). Managing electronic records in Malaysian civil courts: A review of literature. *International Journal of Academic Research in Business and Social Sciences*, 7(8), 909-919.
- Mohamad, A. M. (2019). Admissibility and authenticity of electronic evidence in the courts of Malaysia and United Kingdom. *International Journal of Law, Government and Communication*, 4(15), 121-129.
- Mohamed Arifin, I. (2020). Understanding electronic evidence in Malaysia court. Ram Reza & Muhammad Advocates & Solicitors. <https://e-perundangan.pkns.gov.my/img/1-Klinik%20Perundangan%20Siri%2012020-Electronic%20%20Evidence.pdf>



- Moussa, A. F. (2021). Electronic evidence and its authenticity in forensic evidence. *Egyptian Journal of Forensic Sciences*, 11(20). <https://doi.org/10.1186/s41935-021-00234-6>
- Public Prosecutor v Goh Hoe Cheong & Anor* [2007] 7 CLJ 68.
- Radhakrishna, G., Zan, M., & Khong, D. W. (2013, January 30). "Computer Evidence in Malaysia: Where are we?". SSRN. <https://dx.doi.org/10.2139/ssrn.2208973>
- Radhakrishna, G., Zan, M., & Khong, W. K. (2013). Computer evidence in Malaysia: Where are we? *Malayan Law Journal Articles*, 1-18.
- Sa'di, M. M., Kamarudin, A. R., Mohamed, D., & Ramlee, Z. (2019). Authentication of electronic evidence in cybercrime cases based on Malaysian laws. *Pertanika Journal of Social Sciences and Humanities*, 23(S),153-168.
- Stoykova, R. (2023). The right to a fair trial as a conceptual framework for digital evidence rules in criminal investigations. *Computer Law & Security Review*, 49, 1-26.
- Tenhunen, M. (1997). The integrity of electronic evidence. In S. Jajodia, W. List, G. McGregor, & L. Strous (Eds.), *Integrity and internal control in information systems* (pp. 37-48). Springer. [https://doi.org/10.1007/978-0-387-35317-3\\_8](https://doi.org/10.1007/978-0-387-35317-3_8)
- Wan Ismail, W. A. F., Abdul Mutalib, L., Baharuddin, A. S., Abdullah Kahar, N. S., & Alias, M. A. A. (2023). Keperluan prosedur operasi standard dalam penerimaan dokumen digital di Mahkamah Sivil Malaysia: Requirements for standard operating procedure in the admissibility of digital documents in the Malaysian civil courts. *UUM Journal of Legal Studies*, 14(1), 365-390. <https://doi.org/10.32890/uumjls2023.14.1.14>
- Wan Ismail, W. A. F., Baharuddin, A. S., Abdul Mutalib, L., & Alias, M. A. A. (2021). An appraisal of digital documents as evidence in Islamic law. *Academic Journal of Interdisciplinary Studies*, 10(3), 198. <https://doi.org/10.36941/ajis-2021-0076>
- Yahya, M. A., Mohd Shariff, A. A., Mat Rashid, A., & Hashim, F. Y. (2020). Pengemukakan dokumen elektronik sebagai keterangan dalam perbicaraan Mahkamah Syariah. *Journal of Law and Society (JUUM)*, 27, 55-63.