Walisongo Law Review (Walrev), Vol 7 No. 2 (2025)
DOI: 10.21580/walrev.2024.6.2.28653
P-ISSN: 2715-3347 E-ISSN: 2722-0400

LEGAL PROTECTION FRAMEWORK FOR DIGITAL FORENSIC EXPERTS IN THE SOCIETY 5.0 ERA

Eko Wahyu Ramadani,[1*] Maksun[2] Rido Idham,[3] Ziya'ul Fikri,[4] Muhammad K. Ridwan.[5]

[123] Universitas Islam Negeri Walisongo Semarang, Indonesia
[4]Diponegoro University, Indonesia
[5] McGill University, Canada

[*]Correspondence: *wahyuramadani_1802026009@student.walisongo.ac.id*

Citation:

Ramadani, Eko Wahyu, Maksun, Rido Idham, Ziya'ul Fikri, and Muhammad Kholil Ridwan. 2025. "Legal Protection for Digital Forensic Expert Witnesses in the Era of Society 5.0". *Walisongo Law Review (Walrev)* 7 (2). https://doi.org/10.21580/walrev.2025.7.2.28653.

Abstract: This study aims to propose a preventive and responsive legal protection framework for digital forensic experts to ensure legal certainty within the criminal justice system. Digital forensic experts play a strategic role in the evidentiary process of cybercrime cases, but often face legal risks arising from their courtroom testimonies. This research employs a normative juridical method, utilizing both statutory and conceptual approaches. The statutory approach examines relevant legal norms and international standards, while the conceptual approach interprets legal principles related to legal certainty, legal protection, and immunity rights for expert witnesses. The data are analyzed descriptively and analytically from a comparative perspective to identify pertinent international legal principles and to formulate a globally applicable framework for the legal protection of digital forensic experts. The novelty of this study lies in the formulation of a limited legal immunity model that integrates professional standards with the principle of due process of law. This study contributes by developing a new normative framework that strengthens the legal protection of digital forensic experts. The findings indicate that limited immunity rights are essential to safeguarding the independence and objectivity of digital forensic experts, provided their actions comply with internationally recognized procedures and ethical standards.

Penelitian ini bertujuan untuk merumuskan kerangka perlindungan hukum yang bersifat preventif dan responsif bagi ahli forensik digital guna menjamin kepastian hukum dalam sistem peradilan pidana. Ahli forensik digital memiliki peran strategis dalam proses pembuktian perkara kejahatan siber, namun kerap menghadapi risiko hukum yang timbul dari kesaksiannya di pengadilan. Penelitian ini menggunakan metode yuridis normatif dengan pendekatan perundang-undangan dan konseptual. Pendekatan perundang-undangan digunakan untuk menelaah norma hukum dan standar internasional yang relevan, sedangkan pendekatan konseptual digunakan untuk menafsirkan

prinsip-prinsip hukum yang berkaitan dengan kepastian hukum, perlindungan hukum, serta hak imunitas bagi saksi ahli. Data dianalisis secara deskriptif dan analitis dengan perspektif komparatif guna mengidentifikasi prinsip-prinsip hukum internasional yang relevan dan merumuskan kerangka perlindungan hukum bagi ahli forensik digital yang berlaku secara global. Kebaruan penelitian ini terletak pada perumusan model imunitas hukum terbatas yang mengintegrasikan standar profesional dengan prinsip due process of law. *Kontribusi penelitian ini adalah pengembangan kerangka normatif baru yang memperkuat perlindungan hukum bagi ahli forensik digital. Hasil penelitian menunjukkan bahwa pemberian hak imunitas hukum terbatas sangat penting untuk menjamin independensi dan objektivitas ahli forensik digital, sepanjang tindakan yang dilakukan tetap sesuai dengan prosedur dan standar etika yang diakui secara internasional.*

Keywords: Digital Forensic Experts; Due Process of Law; Legal Protection; Limited Legal Immunity; Society 5.0

INTRODUCTION

Current technological developments are in a phase called the era of society 5.0 (Burhanuddin and Pharmacista 2023). The era of Society 5.0 refers to a society capable of solving various social challenges and problems by utilizing various innovations that emerged during the Industrial Revolution era, such as IoT, AI, big data, and robots, which aim to improve the quality of human life (Atay et al. 2025). In the era of Society 5.0, human life is inseparable from technology because almost all aspects of human life use the internet (Kapoyos et al. 2023). This era is marked by the integration of the physical and digital worlds (cyberspace), which has given rise to new forms of human interaction as well as modern crimes known as cybercrime (*cybercrime*) (Ramadani, Harahap, and Fibriani 2025). With the existence of cybercrime, the law enforcement sector must be able to adapt and adjust to technological developments.

The complexity of cybercrime demands the presence of digital forensic experts as strategic parties in the evidence process. Digital forensics is the application of informatics analysis techniques to ensure the presentation of computer crime evidence data to the court, especially to maintain the integrity of the evidence and maintain the chain of custody of digital evidence (Dimitriadis et al. 2020). Digital evidence is the product of the digital forensic process, according to ISO/IEC 27037:2012, digital evidence is information or data stored or transmitted in binary form that can be relied upon as evidence (Antwi-boasiako et al. 2018). Digital evidence is important because of the involvement of electronic devices and systems in criminal activities. Digital evidence is highly volatile, unlike traditional types of evidence, which can be rapidly altered through computing-related activities (Antwi-boasiako et al. 2018).

Perpetrators of computer crimes often attempt to destroy evidence and avoid criminal liability. Perpetrators often possess advanced technical skills to protect themselves and erase

digital evidence. Therefore, the primary role of a digital forensic expert is to uphold the rule of law by preserving evidence, reconstructing the crime, and ensuring that the collected evidence is useful in court proceedings (Awaluddin, Amsori, and Mulyana 2024). The results of digital forensic testing presented in court are not limited to letters or expert testimony, but also include test results, including digital evidence that has undergone forensic testing (Haris et al. 2024).

However, the position of digital forensic experts is highly vulnerable. The volatile nature of digital evidence and its heavy reliance on technical expertise make expert testimony potentially contested, both in terms of accuracy and the procedures used to handle it. In numerous cases, experts in other fields have faced criminal or civil charges for testimony given in court, such as the cases of Prof. Basuki Wasis, Prof. Bambang Hero Saharjo, and Dr. Eva Achjani Zulfa (Rahim 2023). This situation indicates that digital forensic experts face potential criminalization or lawsuits that could compromise their independence and objectivity in carrying out their professional roles. However, to date, there is no legal framework specifically protecting digital forensic experts in carrying out their professional duties.

Technological advances pose ethical challenges, such as the risk of privacy violations, data manipulation, and external pressures that can influence the results of forensic analysis (Aleke and Trigui 2024). Without adequate legal protection, digital forensic experts can become the most vulnerable parties in the criminal justice system. Lawsuits, pressure, and threats aimed at influencing expert testimony and the validity of evidence obtained from forensic processes represent a real threat. This situation demonstrates a gap between the important role of digital forensic experts and the weak legal protection that guarantees their independence. Based on these issues, this study aims to formulate a preventive and responsive legal protection framework for digital forensic experts of the era of society 5.0.

RESEARCH METHOD

This research uses a normative juridical method with a statutory and conceptual approach. The statutory approach is applied to examine and interpret various international legal instruments relevant to legal protection for digital forensic experts. The instruments studied include the Universal Declaration of Human Rights (1948), the International Covenant on Civil and Political Rights (1966), the Budapest Convention on Cybercrime (2001), and international technical standards such as ISO/IEC 27037:2012 and ISO/IEC 27050-3:2020. The selection of legal sources was carried out purposively, based on their relevance to the principles of legal certainty, legal protection, and immunity rights for expert witnesses. The analysis was carried out through systematic and comparative interpretation, by comparing legal norms and principles in various instruments to find similarities and differences that can form the basis for formulating a legal protection model for digital forensic experts. The conceptual approach was used to examine legal theories related to due process of law, expert witness independence, and professional responsibility in the criminal justice

system. This approach is applied by linking these theories to digital forensic practice to develop a concept of preventative and responsive legal protection. All data is analyzed descriptively and analytically, systematically interpreting legal findings to develop a legal protection framework for digital forensic experts in the Society 5.0 era.

RESULT AND DISCUSSION

The Role, Status, and Legal Risks of Digital Forensic Experts

Evidence plays a crucial role in the courtroom and is a central element in handling criminal cases. The evidentiary process determines the defendant's fate, as only through it can it be determined whether the defendant committed a crime (Kaligis 2013). If the evidence stipulated by law is insufficient to prove the guilt of the accused, the defendant must be acquitted of all charges. Conversely, if the defendant's guilt can be proven, the defendant is found guilty and sentenced (Arini and Sujarwo 2021).

In the context of modern crime developments, digital forensics plays a crucial role in the investigation and prosecution of criminal cases. The digital forensic process must be conducted using a clear, structured, and accountable methodology (Amarini et al. 2024). Digital forensic experts play a crucial role in explaining and analyzing digital evidence so that it can be accepted in court (Budianto 2025). Digital evidence is a key element in the investigation and prosecution of cybercrimes (AllahRakha 2024). Unlike conventional crimes that leave physical traces, cybercrimes produce volatile electronic traces. Through the stages of identification, acquisition, analysis, and preservation of digital data, investigators can reconstruct events, link actions to perpetrators, and prove intent (AllahRakha 2024).

The primary goal of digital forensics is to obtain evidence to answer the 5W and "how" (5WH) questions. The 5WH questions include what happened, who was involved, when it happened, where it happened, why it happened, and how the incident occurred. These questions lead to confirmation or refutation of allegations of a cybercrime incident (Dimitriadis et al. 2020). With the advancement of technology, digital forensics has become faster and more precise, making the investigation process more effective. However, these advances also raise several ethical issues. First, digital forensics often involves processing large amounts of personal and sensitive information, making privacy a critical concern. In addition to privacy, data integrity is crucial in forensic investigations, as any manipulation or bias in the handling of evidence can compromise the identification process (Aleke and Trigui 2024).

According Black's Law Dictionary[1] testimonial evidence is "a person, testimony offered to prove the truth of the matter asserted, especially evidence elicited from a witness" (A'yun 2014). Meanwhile, what is meant by "*expert evidence*" is evidence of a scientific,

[1]Black's Law Dictionary is the leading and most frequently used legal dictionary in the United States and the world, written by Henry Campbell Black in 1891 and continually updated with extensive research to become a reliable reference in legal terminology. It provides concise, authentic definitions supported by case law and other sources, and often includes examples of word usage in various legal contexts.

technical, professional, or other specialized expertise to provide testimony due to familiarity with the subject or special training in the field, which is also called expert testimony (A'yun 2014). Thus, the opinion presented by a digital forensic expert in court is a form of expert evidence. The use of the term testimonial evidence and expert evidence the treatment of expert witnesses often differs between legal systems that adhere to the Civil Law System and the Common Law System. In common law systems such as in America, there is no explicit mention of expert testimony or defendant testimony; expert testimony is combined into the category of "testimonial evidence" (Ubwarin 2014). Meanwhile, in a civil law system such as Indonesia (Tri Bowo Hersandy Febrianto 2023), expert testimony is explicitly mentioned in Article 184 of the Criminal Procedure Code (KUHAP) as one of the five valid pieces of evidence (Richard 2015).

Both legal systems fundamentally recognize the crucial role of expert witnesses, including digital forensic experts, in the evidentiary process. This demonstrates that the presence of digital forensic experts is becoming increasingly crucial in handling complex electronic evidence. Therefore, investigators and digital forensic experts are required to act quickly and accurately in securing evidence, while maintaining its integrity so that it can be legally admissible in court (Aini and Lubis 2024).

Digital forensic experts play a crucial role in the judicial process, but this role is not without risks. Digital forensic experts can face both criminal and civil lawsuits based on testimony provided in court. This situation is often exploited by certain parties through Strategic Lawsuit Against Public Participation (SLAPP) aimed at silencing or intimidating experts (Rahim 2023). A SLAPP is a form of abuse of legal instruments by certain parties with the aim of silencing, weakening, or intimidating individuals or groups exercising their right to public participation (Riyadi and Hadi 2021).

This lawsuit is generally filed not to obtain justice, but to create a deterrent effect (chilling effect) so that the defendant, including expert witnesses, no longer wants to convey their opinions or statements in public or in court (Riyadi and Hadi 2021). In general, SLAPPs use civil lawsuits and take the form of criminal reports (Riyadi and Hadi 2021). The main characteristics of SLAPPs lie in their intimidatory purpose, their targets are usually vocal or critical parties such as activists, academics, journalists, or experts, and their impact, which is financially and psychologically burdensome for the defendant (Pring 1989).

The phenomenon of SLAPP use can be seen in cases against experts in Indonesia, such as the lawsuit against Prof. Basuki Wasis filed by former Southeast Sulawesi Governor Nur Alam, Prof. Bambang Hero Saharjo filed by PT. Jatim Jaya Perkasa, and Dr. Eva Achjani Zulfa, each of whom was reported or sued for their testimony in court. Although the lawsuits were ultimately rejected or withdrawn, these cases demonstrate that digital forensic experts are potentially subject to criminalization or counterclaims for testimony given in court, especially if their testimony is detrimental to a particular party (Rahim 2023).

Galaxy Computer Servs., Inc. v. Baker[2] A case in the United States also reflects the risks facing digital forensic experts. In that case, the defendant attempted to discredit the expert's testimony by alleging lack of qualifications and procedural errors. Although the court ultimately recognized the expert's competence and experience, the case demonstrates that the legitimacy of digital forensic practice depends heavily on adherence to legally recognized professional and procedural standards (Ami-Narh and Williams 2008). An important lesson for the Indonesian context is the need for legal guarantees to protect the independence of digital forensic experts, preventing them from being easily attacked through repressive legal mechanisms.

Based on this, a legal protection framework is needed that guarantees the freedom, security, and independence of digital forensic experts in carrying out their professional duties. However, this protection is not absolute but rather limited, that is, it only applies if the expert has implemented procedures in accordance with international standards such as ISO/IEC 27037:2012 which regulates the principles of identification, collection, acquisition, and preservation of digital evidence, and ISO/IEC 27050-3:2020 concerning the Code of Practice for Electronic Discovery which emphasizes the principles of traceability, transparency, and accountability. Thus, the freedom of digital forensic experts to provide opinions in court must always be placed within the framework of compliance with applicable legal, scientific, and ethical standards.

Legal Protection and Immunity of Digital Forensic Experts

The concept of Society 5.0, introduced by the Japanese government in 2016, describes a “super smart society" that integrates technological advances into all aspects of human life to improve social welfare and sustainability (Fukuda 2020). In this era, the development of digital technology not only brings benefits but also increases the potential for cybercrimes such as phishing, ransomware, IoT hacking, as well as data misuse and privacy violations (Nopit Ernasari and Naib 2024). The implications of technology use in the Society 5.0 era present unique challenges for legal development (Fendawati 2025). This condition raises the need for a legal framework capable of providing adequate legal protection for digital forensic experts who play a crucial role in establishing evidence.

The concept of legal protection is very important for society, especially those in a weak position, both economically and legally (Djufri 2023). As stated by Satjipto Rahardjo and Philipus M. Hadjon, who emphasized the importance of protecting human rights for society through two forms of mechanisms, namely preventive and repressive legal protection (M. Hadjon 1987). In the context of digital forensics, preventive legal protection aims to prevent prosecution or intimidation against digital forensic experts due to testimony given in court, so that experts can carry out their roles independently and professionally without pressure.

Why is the concept of preventive legal protection emphasized more in the context of legal protection for digital forensic experts? Because, if we look at the function of digital

[2] U.S. Bankruptcy Court – Eastern District of Virginia

forensic experts in a trial process, protection must be provided before a problem or dispute arises (M. Hadjon 1987). This is intended to ensure that the trial process involving digital forensic experts can proceed as it should and as an effort to close the gap of intimidation that can disrupt an expert's independence. This differs from repressive legal protection that only applies after intimidation or a lawsuit has occurred (M. Hadjon 1987), this approach has the potential to hinder the expert's function and affect the course of the judicial process. Therefore, the concept of preventive legal protection is more effective in maintaining the objectivity and professionalism of experts. Preventive legal protection for digital forensic experts can take the form of regulations that guarantee expert independence, granting limited immunity for professional opinions, and ethical oversight mechanisms by neutral institutions.

Philosophically, the elements of legal protection include three main components, namely: (1) legal subjects, in this case digital forensic experts as expert witnesses who provide information based on their expertise, this is in line with what was expressed by L. J. van Apeldoorn, that everything that has legal authority is considered a legal subject (M. Manullang 2021); (2) protected objects, namely freedom of expression in court and protection from threats or pressure; and (3) methods or forms of protection, which are sourced from international instruments (Firdaus 2024). International legal instruments that can be used are Article 12 and Article 19 of the Universal Declaration of Human Rights (UDHR), Article 17 paragraphs 1-2 and Article 19 of the International Covenant on Civil and Political Rights (ICCPR), Article 24 paragraphs 1-4 of the United Nations Convention Against Transnational Organized Crime (UNTOC), and Article 15 of the Budapest Convention on Cybercrime. The interment contains principles for protecting privacy, freedom of expression, and the safety of witnesses from actions aimed at compromising the expert's independence. These principles serve as the normative basis for legal protection for digital forensic experts in carrying out their duties in court.

International legal instruments have provided a normative basis for digital forensic experts' protection in carrying out their roles in court. This protection must be implemented in accordance with the principles due process of law (Barnett 2023). The principle process of law is a fundamental concept in a state of law (rule of law) and constitutional democracy (Ayu Wulandari and Sidi Ahyar Wiraguna 2025). This principle essentially requires that every legal process carried out by the judicial institution must fulfill the elements of procedural justice, protect individual rights, and guarantee a fair opportunity to be heard before a decision is made (Ayu Wulandari and Sidi Ahyar Wiraguna 2025). This principle is closely related to the implementation of the international standards ISO/IEC 27037:2012 and ISO/IEC 27050-3:2020, which provide procedural legitimacy to the way digital evidence is managed, from identification, collection, preservation, analysis, to presentation in court.

International Standards Organization (ISO) and International Electrotechnical Commission (IEC) are used as technical standard references in the context of legal protection for digital forensic experts because ISO/IEC contains internationally applicable guidelines for handling digital evidence related to the investigative process (Veronika and Simanjuntak

2022). ISO/IEC 27037:2012 provides guidelines for specific activities in handling potential digital evidence; these processes include: identification, collection, acquisition, and preservation of potential digital evidence. This standard ensures that responsible individuals manage potential digital evidence in a practical manner that is accepted worldwide, with the aim of facilitating investigations involving digital devices and digital evidence in a systematic and impartial manner, while maintaining its integrity and authenticity (Kao, Wu, and Chiu 2014). The digital forensic investigation process includes identification, acquisition, preservation, examination and analysis, and presentation (Ombu 2023).

In addition to the existing standards in ISO/IEC 27037:2012, another procedure that needs to be considered is ISO/IEC 27050-3 (Part 3) which provides requirements and recommendations related to the elements of the electronic discovery process described in ISO/IEC 27050-1. Additional material in ISO/IEC 27050-3 is intended to help organizations better understand the purpose of each element of the electronic discovery process and considerations for avoiding failures, which can reduce risks and costs if electronic discovery becomes an issue (Teppler and Hibbard 2022). ISO/IEC 27050 is a standard procedure for the discovery of electronically stored information. Electronic discovery (eDiscovery) involves seven main steps: identification, preservation, collection, processing, review, analysis, production (Lin and Lin 2024).

ISO/IEC 27050-3 identifies the need for multifaceted involvement in the electronic discovery process and the need for coordination throughout the entire process. These cross-cutting aspects include Planning, Transparency, Documentation, Expertise, Informedness, Adaptability, and Use of Technology (Teppler and Hibbard 2022). As stated by Eoghan Casey in his book Digital Evidence and Computer Crime, third edition, the credibility of digital evidence is largely determined by the extent to which the identification, acquisition, and preservation processes are carried out responsibly and in accordance with recognized standards (Casey 2011). Digital forensic methods and the independence of expert witnesses are key factors in ensuring expert testimony is admissible by the court. These two standards ensure that the entire digital forensic process is conducted transparently, accountably, and in accordance with internationally recognized legal principles, thereby reducing the risk of data manipulation and accusations of bias against experts.

ISO/IEC has been used as an investigative standard, such as in the Taiwanese case (Lin and Lin 2024). The crimes occurred from September 2021 to March 2022 in Taoyuan, Taichung, and Tainan, Taiwan. There were reports of investment fraud and property losses. Through the LINE community software, fake investment platform URLs or apps such as "MCK" and "AXA Trading" were randomly sent to text message recipients. False information, including stock prices, foreign exchange rates, and virtual currencies, was disseminated. The Taiwanese Criminal Police Bureau conducted 165 big data analyses and arrested 42 suspects. Preliminary investigations indicated that illicit financial flows (IFFs) exceeded USD 3.1 million. To conceal personal information, the group used foreign-developed communication

software or the names and images of famous individuals. The case was investigated using DEFSOP and ISO/IEC 27050 procedures (Lin and Lin 2024).

The relevance of implementing these international standards can be seen in the investment fraud case in Taiwan in 2021–2022. In this case, the police used DEFSOP and ISO/IEC 27050 procedures to trace the flow of illicit funds and obtain valid digital evidence in court. This case demonstrates that adherence to international standards not only improves the accuracy of investigations but also strengthens the credibility and legal protection of digital forensic experts involved in the evidentiary process (Lin and Lin 2024). The existence of international standards, such as ISO/IEC 27037:2012 and ISO/IEC 27050-3:2020, serves not only as technical guidelines but also as an instrument of legal legitimacy that protects expert witnesses from accusations of manipulation or bias.

One form of legal protection that can be implemented is by providing guarantees for digital forensic expert witnesses by involving witness and victim protection agencies (Tuage 2013). In Indonesia, witness and victim protection agencies have been established based on the mandate of Law Number 13 of 2006 concerning witness and victim protection (Satrio and Faisal 2021). Although in Indonesia there is a special agency authorized to provide legal protection for digital forensic experts, this protection remains repressive. There is a need for an expansion of authority or mandate so that this agency has the authority to provide legal protection for digital forensic experts with a preventive nature. International institutions such as the International Criminal Court (ICC) need to encourage each country to have a special witness and victim protection agency that includes protection for digital forensic expert witnesses.

Furthermore, there is a need for international normative recognition of the right to limited immunity for digital forensic experts to provide legal protection and guarantee the independence, integrity, and effectiveness of the expert's role in the criminal justice system in the digital era. Although the ICC has not explicitly regulated the protection of digital forensic experts, the principle of witness protection contained in rule 87 of the ICC Rules of Procedure and Evidence (2002), which discusses protective measures for victims and witnesses during the trial process, can be the basis for developing legal protection for digital forensic experts. Based on the description above, it can be concluded that legal protection for digital forensic experts is both conceptual and practical, as long as the experts carry out their duties in accordance with applicable international standards, such as ISO/IEC 27037:2012 and ISO/IEC 27050-3:2020. Compliance with these standards is necessary to ensure that all stages of handling and presenting digital evidence are carried out professionally, documented, transparently, and accountably. Thus, the combination of international legal instruments, the principle of due process of law, and ISO technical standards forms a comprehensive legal protection framework for digital forensic experts, which not only maintains the integrity of digital evidence but also guarantees the independence and professional credibility of experts before the court.

CONCLUSION

Digital forensic experts play a strategic role in proving cybercrime in the Society 5.0 era, where technological advances simultaneously increase the potential for cybercrime and data misuse. This position makes them vulnerable to legal threats, including civil lawsuits, criminal prosecution, and Strategic Lawsuits Against Public Participation (SLAPP) practices that can undermine professional independence. International legal instruments such as the UDHR, ICCPR, and the Budapest Convention on Cybercrime provide a normative basis for protecting freedom of expression and witness security, while the technical standards ISO/IEC 27037:2012 and ISO/IEC 27050-3:2020 strengthen the legitimacy of digital forensic processes through the principles of transparency, accountability, and due process of law. The synergy between these legal principles and technical standards forms a comprehensive legal protection framework for digital forensic experts. Legal reforms need to be directed at recognizing the immunity of expert witnesses, expanding the mandate of the Witness and Victim Protection Agency to include protection for digital forensic experts, and regulating the prevention and prosecution of SLAPP practices to ensure the independence, integrity, and effectiveness of the role of experts in the criminal justice system in the digital era. [*W*]

BIBLIOGRAPHY

A'yun, Rafiqa Qurrata. 2014. "The Problems of Expert Witness in Criminal Law." *Indonesia Law Review* 4 (3): 340. https://doi.org/10.15742/ilrev.v4n3.115.

Aini, N, and F Lubis. 2024. "Tantangan Pembuktian Dalam Kasus Kejahatan Siber." *Judge: Jurnal Hukum* 05 (02): 55–63https://doi.org/doi.org/10.54209/judge.v5i02.566

Aleke, Ngozi Tracy, and Mohamed Trigui. 2024. *Legal and Ethical Challenges in Digital Forensics Investigations*. *Digital Forensics in the Age of Ai* https://doi.org/10.4018/979-8-3373-0857-9.ch006

AllahRakha, Naeem. 2024. *Cybercrime and the Law: Addressing the Challenges of Digital Forensics in Criminal Investigations*. *Mexican Law Review*. Vol. 16. https://doi.org/10.22201/iij.24485306e.2024.2.18892

Amarini, Indriati, Rizky Cahyadri Aulia, Maulida Ayu Fitriani, and Noorfajri Ismail. 2024. "The Legal Position of Digital Forensic Expert in the Settlement of Informastion Technology Crimes Cases." *Lex Scientia Law Review* 8 (1): 355–84. https://doi.org/10.15294/lslr.v8i1.2952

Ami-Narh, James Tetteh, and Patricia A.H. Williams. 2008. "Digital Forensics and the Legal System: A Dilemma of Our Times." *Proceedings of the 6th Australian Digital Forensics Conference*, 30–40. https://doi.org/10.4225/75/57b268ce40cb6

Antwi-boasiako, Albert, Hein Venter, Albert Antwi-boasiako, Hein Venter, A Model, Digital Evidence, and Admissibility Assessment. 2018. "A Model for Digital Evidence Admissibility Assessment." https://doi.org/10.1007/978-3-319-67208-3_2

Arini, Khafifah Nuzia, and Herman Sujarwo. 2021. "Kedudukan Saksi Ahli Dalam

Persidangan Perkara Pidana." *Syariati : Jurnal Studi Al-Qur'an Dan Hukum* 7 (2): 245–56. https://doi.org/10.32699/syariati.v7i2.2244

Atay, Salim, Cennet Terzi Müftüoğlu, Neşe Gülmez, and Muhittin Şahin. 2025. "Society 5.0 and Human-Centered Technology: Redefining Talent Management in the Digital Age." *Sustainable Futures* 9 (March). https://doi.org/10.1016/j.sftr.2025.100733

Awaluddin, Fakhri, Amsori, and Momon Mulyana. 2024. "Tantangan Dan Peran Digital Forensik Dalam Penegakan Hukum Terhadap Kejahatan Di Ranah Digital." *Humaniorum* 2 (1): 14–19. https://doi.org/10.37010/hmr.v2i1.35

Ayu Wulandari, and Sidi Ahyar Wiraguna. 2025. "Problematika Penerapan Prinsip Due Process of Law Dalam Hukum Acara Pengujian Undang-Undang Di Mahkamah Konstitusi." *Politika Progresif : Jurnal Hukum, Politik Dan Humaniora* 2 (2): 52–63. https://doi.org/10.62383/progres.v2i2.1613

Barnett, Randy E. 2023. "An Originalist Theory of Due Process of Law." *SMU Law Review* 76:441. https://doi.org/10.25172/smulr.76.3.4

Budianto, T Y A. 2025. "Peran Digital Forensik Dalam Penegakan Hukum Terhadap Kejahatan Konvensional." *Lex Progressium: Jurnal Kajian Hukum ...* 2 (1): 1–8. https://jurnal.dokterlaw.com/index.php/lexprogressium/article/download/146/135.

Burhanuddin, Sisca Ferawati, and Gandhi Pharmacista. 2023. "Transformation of Companies and Trade in the Era of Society 5.0." *International Journal of Science and Society* 5 (5): 1067–77. https://doi.org/10.54783/ijsoc.v5i5.973

Casey, Eoghan. 2011. *Digital Evidence and Computer Crime Third Edition. Securing the Information Infrastructure*. 3rd ed. Waltham, Massachusetts, USA: Academic Press. http://www.elsevierdirect.com/companions/9780123742681

Dimitriadis, Athanasios, Nenad Ivezic, Boonserm Kulvatunyou, and Ioannis Mavridis. 2020. "D4I - Digital Forensics Framework for Reviewing and Investigating Cyber Attacks." *Array* 5 (October 2019): 100015. https://doi.org/10.1016/j.array.2019.100015

Djufri, Darmadi. 2023. *Perlindungan Hukum Terhadap Warga Negara Dalam Proses Peradilan Tindak Pidana*. Banyumas: CV Amerta Media.

Fendawati. 2025. "Analisis Kebutuhan Kebijakan Hukum Di Masa Society 5.0." *Integrative Perspectives of Social and Science Journal* 2 (1): 336–43. https://ipssj.com/index.php/ojs/article/view/69

Firdaus, Febrian Hilmi. 2024. "Perlindungan Dan Kepastian Hukum Bagi Pengendali Data Pribadi Di Masa Depan." *Jurnal Masalah-Masalah Hukum* 53 (2): 135–44. https://doi.org/10.14710/mmh.53.2.2024.135-144

Fukuda, Kayano. 2020. "Science, Technology and Innovation Ecosystem Transformation toward Society 5.0." *International Journal of Production Economics* 220 (August 2017): 107460. https://doi.org/10.1016/j.ijpe.2019.07.033

Haris, Oheo Kaimuddin, Sitti Aisah Abdullah, Ali Rizky, Sri Ratih Indah, and others. 2024."Penggunaan Digital Forensik Dalam Pembuktian Tindak Pidana Pencemaran Nama Baik Di Media Sosial Berdasarkan UU ITE."*Halu Oleo Legal Research* 6 (2): 588–

603.https://doi.org/https://doi.org/10.33772/holresch.v6i2.788

Kaligis, Jendry. 2013. "Penerapan Alat Bukti Petunjuk Oleh Hakim Dalam Menjatuhkan Putusan Tindak Pidana Pembunuhan." *Lex Crimen* II (4): 23–32. https://ejournal.unsrat.ac.id/index.php/lexcrimen/article/view/3085

Kao, Da-Yu, Guan-Jie Wu, and Ying-Hsuan Chiu. 2014. "A Novel Process Framework for Digital Forensics Tools: Based on ISO/IEC 27037:2012." *The International Academic Forum*. https://api.semanticscholar.org/CorpusID:113863771

Kapoyos, Jeremiah Marvin, Dimas Abimanyu Prasetyo, Mochamad Reyhan Gusnaldi, and Fried Sinlae. 2023. "Pentingnya Cybersecurity Di Era Society 5.0." *Nusantara Journal of Multidisciplinary Science* 1 (5) 1344–51. https://jurnal.intekom.id/index.php/njms/article/view/229/199

Lin, Chao Meng, and I. Long Lin. 2024. "Digital Forensics According to International Organization for Standardization/International Organization for Standardization 27050 and Digital Evidence Forensics Standard Operating Procedure: Use of Sensor Technology." *Sensors and Materials* 36 (6): 2315–24. https://doi.org/10.18494/SAM4871

M. Hadjon, Philipus. 1987. *Perlindungan Hukum Bagi Rakyat Di Indonesia*. Surabaya: Bina Ilmu.

M. Manullang, E. Fernando. 2021. "Subjek Hukum Menurut Hans Kelsen Dan Teori Tradisional: Antara Manipulasi Dan Fiksi." *Jurnal Hukum Dan Peradilan* 10 (1): 139. https://doi.org/10.25216/jhp.10.1.2021.139-154

Nopit Ernasari, and Naib. 2024. "Criminal Law Reform in the Face of the Society 5.0 Era Against Cyber Crime." *International Journal of Accounting, Management, Economics and Social Sciences (IJAMESC)* 2 (6): 2360–68. https://doi.org/10.61990/ijamesc.v2i6.383

Ombu, Atonbara. 2023. "Role of Digital Forensics in Combating Financial Crimes in the Computer Era." *Journal of Forensic Accounting Profession* 3 (1): 57–75. https://doi.org/10.2478/jfap-2023-0003

Pring, George W. 1989. "SLAPPs: Strategic Lawsuits against Public Participation." *Pace Environmental Law Review* 7 (1): 3. https://doi.org/10.58948/0738-6206.1535

Rahim, A. 2023. "Perlindungan Hukum Terhadap Ahli Dalam Proses Peradilan." *The Prosecutor Law Review* 1 (2): 36–66. https://prolev.kejaksaan.go.id/kejaksaan/article/view/12

Ramadani, Eko Wahyu, Rustam Dahar Karnadi Apollo Harahap, and Riza Fibriani. 2025. "Cybercrime Punishment Formulation Using Methods DDoS Attack Regarding Websites from a Positive Legal Perspective." *Jurnal Hukum Prasada* 12 (1): 26–35. https://doi.org/10.22225/jhp.12.1.2025.26-35

Richard, Lokas. 2015. "Barang Bukti Dan Alat Bukti Dalam Kitab Undang-Undang Hukum Acara Pidana." *Lex et Societatis* III (9): 124–25. https://doi.org/10.35796/les.v3i9.10177

Riyadi, Eko, and Sahid Hadi. 2021. "Strategic Lawsuit against Public Participation (SLAPP):

A Legal-Based Threat to Freedom of Expression." *Padjadjaran Jurnal Ilmu Hukum* 8 (1): 141–62. https://doi.org/10.22304/pjih.v8n1.a7

Satrio, Ndaru, and Faisal Faisal. 2021. "Hak Saksi Dan Korban Tindak Pidana Kasus Tertentu Dalam Perlindungan Saksi Dan Korban Perspektif Equality Before the Law." *Cepalo* 5 (1): 1–10. https://doi.org/10.25041/cepalo.v5no1.2109

Teppler, S, and E Hibbard. 2022. "ISO Publishes the Electronic Discovery Standard." *Ave Maria Law Review* 20:160–91. https://www.avemarialaw.edu/wp-content/uploads/2022/09/Teppler-Hibbard-Proof35.pdf

Tri Bowo Hersandy Febrianto. 2023. "Peran Civil Law Dalam Sistem Hukum Indonesia." *Jurnal Hukum Dan Sosial Politik* 2 (1): 235–45. https://doi.org/10.59581/jhsp-widyakarya.v2i1.2183

Tuage, Saristha Natalia. 2013. "Perlindungan Hukum Terhadap Saksi Dan Korban Oleh Lembaha Perlindungan Saksi Dan Korban (LPSK)." *Lex Crimen* II (2): 56–64. https://ejournal.unsrat.ac.id/v3/index.php/lexcrimen/article/view/1541/1236

Ubwarin, Erwin. 2014. "Keabsahan Keterangan Ahli Dalam Tindak Pidana Korupsi." *Sasi* 20 (1): 1. https://doi.org/10.47268/sasi.v20i1.340

Veronika, Veronika, and Binsar H Simanjuntak. 2022. "Implementasi Iso 27037 Dalam Pemeriksaan Investigatif Dengan Teknik Forensik Digital Untuk Memperoleh Bukti Audit Di Badan Pemeriksa Keuangan (Bpk)." *Jurnal Magister Akuntansi Trisakti* 9 (2): 89–104. https://doi.org/10.25105/jmat.v9i2.13343