International Journal of Social and Education (INJOSEDU) https://languar.net/index.php/INJOSEDU
Vol. 3 No. 4 July 2026, hal., 504-515 e-ISSN: 3047-6151

# CYBERCRIME AND DAMAGES IN CIVIL LAW: TECHNICAL MEASURES AND CASE LAW IN DISPUTE RESOLUTION

**Gunawan Widjaja**
Senior Lecturer, Faculty of Law Universitas 17 Agustus 1945 Jakarta
widjaja_gunawan@yahoo.com

**Abstract**

This article analyses the relationship between cybercrime and claims for damages under Indonesian civil law, focusing on technical approaches and case law in dispute resolution. The research method is a legal-normative literature review examining legislation, court rulings, academic literature and policy documents relating to cybercrime, electronic evidence, restitution and Article 1365 of the Civil Code. The findings reveal three main conclusions. Firstly, the incidence of cybercrime has increased significantly, resulting in complex material and immaterial losses. Secondly, technical measures such as digital forensics, digital asset tracing, the authentication of electronic evidence, and the role of forensic experts are prerequisites for proving claims and recovering losses. Thirdly, case law and judicial practice have opened up avenues for restitution and civil claims, but these still face obstacles in the form of imprecisely formulated claims, challenges in authenticating evidence, and inconsistencies in the assessment of non-material damages. The article recommends harmonising legal standards between the criminal and civil spheres, strengthening digital forensic capabilities within law enforcement agencies, and developing jurisprudential guidelines to enhance the certainty and effectiveness of restoring victims' rights.
**Keywords**: cybercrime, damages, electronic evidence, digital forensics, restitution.

## Introduction

The rapid development of digital technology in Indonesia is now accompanied by the serious threat of cybercrime. Cyberattacks no longer target individuals alone, but have spread to organisations, companies and even government institutions. According to data from the National Cyber and Cryptography Agency (BSSN), there was a very significant surge in cyber attacks throughout 2025, with 5.5 billion attacks recorded – a figure that has increased sevenfold, or by 714 per cent, compared to the annual average for the period 2020–2024. This upward trend continued into early 2026; in the period from 1 January to 15 April alone, 1.52 billion cyber attacks were recorded( Budiyanto, 2025).

Statistics on cybercrime in Indonesia show an extremely worrying increase. According to the National Criminal Information Centre (Pusiknas), the Indonesian National Police have handled 1,062 criminal cases relating to cybercrime, the internet, online media, electronic media and social media. Based on data from the EMP application of Pusiknas, Criminal Investigation Division of the Indonesian National Police, in 2022 there were 8,636 recorded cases of cybercrime (YOGI OKTAFIAN

ARISANDY, 2021). This figure rose dramatically by Thursday, 23 January 2025, with a total of 32,073 reports and 29,067 victims of cybercrime. The most common types of cybercrime, according to Cyber Patrol Statistics, included 14,495 cases of online fraud, 8,614 cases of threats of violence, 6,556 cases of defamation, 3,675 cases of threats of defamation, 952 cases of pornography, 778 cases of fake news, 597 cases of unauthorised data manipulation, 499 cases of provocation , 237 cases of online prostitution, and 220 cases of online gambling( Sumadiyasa et al.., 2021). This article discusses the phenomenon of cybercrime in Indonesia, emphasising statistical trends for the 2024 period, where research findings indicate a significant increase in online fraud, phishing, and ransomware (Singgi et al.., 2020).

Reports of online fraud have totalled more than 572,000 cases since 2017, whilst in 2024 there were 26.7 million phishing incidents and 514,000 ransomware attacks. Public concern about online fraud has also surged from 10.3 per cent (2023) to 32.5 per cent (2024). These findings confirm that the digital space has now become a new arena for crime that is more complex than conventional crime (Sumadiyasa et al., 2021).

According to data compiled by the government, between November 2024 and January 2025, financial losses resulting from cybercrime amounted to Rp 476 billion. Meanwhile, by mid-2025, 1.2 million reports of digital fraud had been submitted to the public complaints system (Singgi et al.., 2020). In a regional context, Indonesia ranks 12th on the list of countries with the highest levels of cyber activity in the Asia-Pacific, accounting for around 3.6 per cent of the region's total cyber activity (Budiyanto, 2025).

The Law on Electronic Information and Transactions (ITE Law) is the primary legal framework for dealing with cybercrime in Indonesia. Law No. 11 of 2008 on Electronic Information and Transactions, subsequently amended by Law No. 19 of 2016, provides a strong legal basis for the recognition of electronic evidence as admissible evidence in legal proceedings, including in civil cases (Singer & Friedman, 2013). Some of the cybercrimes regulated under the ITE Law include illegal content relating to obscenity, gambling, defamation, threats and extortion (Article 27), as well as false news that is misleading and harmful to consumers (Article 28) (Septiari & Ujianti, 2025).

Article 27 has been split into Article 27 on public decency and gambling; Article 27A on defamation and libel; and Article 27B on extortion and threats. One paragraph has been added to Article 28, thereby regulating false news that causes material loss to consumers, incitement based on ethnicity, religion, race or inter-group relations (SARA), and false news that causes unrest (Singgi et al.., 2020). Article 29 on cyberbullying prohibits acts that utilise information technology containing threats of violence or intimidation directed at an individual (Sari, 2021) .

Article 5(1) of the ITE Law states that "Electronic Information and/or Electronic Documents and/or their printed outputs constitute valid legal evidence". This provision is clarified in paragraph (2), which states that electronic evidence constitutes an extension of the types of evidence permitted under the applicable procedural law in

Indonesia. Since the ITE Law came into force, electronic information, electronic documents and/or their printed copies (electronic evidence) have been regarded as an extension of admissible evidence under criminal procedural law (Hakim & Yehezkiel, 2024) .

The main issue arising in the handling of cybercrime is the gap between criminal law enforcement and the recovery of damages for victims. Article 1365 of the Civil Code stipulates that any unlawful act causing loss to another person obliges the person who, through their fault, caused that loss to compensate for it (Indonesian Attorney General's Office, 2025). According to Article 1365 of the Civil Code, an unlawful act is defined as any act that contravenes the law, committed by a person, and which, due to that person's fault, has caused loss to another person. Losses resulting from an unlawful act may take the form of material or non-material losses. Non-material losses are losses relating to fear, pain or the loss of enjoyment of life. Generally, claims for such non-material losses may be brought on the grounds of an unlawful act (Alfianto et al.., 2024). Compensation in the context of an unlawful act includes nominal damages, compensation and punitive damages.

The rights of victims through restitution may take the form of compensation for loss of assets and/or income, compensation for both material and non-material losses resulting from suffering, reimbursement of medical and/or psychological treatment costs, and other losses resulting from a criminal offence (Zakky et al.., 2026) . Articles 98–101 of the Criminal Procedure Code (KUHAP) regulate the mechanism for claims for compensation (restitution) in criminal proceedings. Following the entry into force of Law No. 13 of 2006 on the Protection of Witnesses and Victims, all victims of criminal offences are also given the option to submit a claim for compensation in the form of restitution through the LPSK (Tomalili, 2019) .

Case law from the Supreme Court of the Republic of Indonesia indicates that where a civil claim is brought against the person reporting or lodging a complaint regarding an alleged criminal offence, the claim may be dismissed on the grounds of ' et al.., 2026) . However, a more in-depth analysis of judicial practice in claims for damages arising from cybercrimes is required. Technical measures in dispute resolution include mechanisms for tracing perpetrators and digital assets, the collection and validation of electronic evidence, and the role of digital forensic experts in the judicial process. This article aims to examine the technical measures and case law relating to the resolution of disputes concerning compensation for damages arising from cybercrimes under Indonesian civil law.

**Research Methodology**

This study employs a literature review method using a juridical-normative approach to analyse cybercrime and compensation under civil law. Data were collected from secondary sources, including national and international journals, books and other

relevant documents. Data analysis was conducted qualitatively by examining, interpreting and synthesising relevant legal material to identify technical approaches and patterns of case law in the resolution of disputes regarding compensation for damages resulting from cybercrime (Eliyah & Aslan, 2025); (Zed, 2008). This approach enables researchers to develop a comprehensive understanding of the harmonisation between criminal law enforcement and mechanisms for compensating victims through civil proceedings without conducting field research.

## Results and Discussion

### Technical Measures in the Resolution of Disputes over Compensation for Losses Resulting from Cybercrime

Broadly speaking, there are three legal avenues available to victims of digital investment scams to recover or obtain compensation for the losses they have suffered: filing a claim for restitution in criminal proceedings, consolidating cases for damages, and bringing a civil action. In addition to requests for the joinder of damages cases and applications for restitution, victims of digital investment fraud may also bring a claim for tort against the perpetrators through the competent district court (Afrianto & Jamaludin, 2025). These remedies provide victims with alternatives to choose the most effective course of action in accordance with the circumstances of their case and their legal interests.

Mechanisms for tracing perpetrators and digital assets are a crucial first step in technical dispute resolution efforts. Digital forensics is the process of identifying, collecting, acquiring and analysing digital evidence to reconstruct cyber incidents (Ashilah & Rahman, 2024). The investigation of a cybercrime such as website hacking requires digital forensics, which aims to identify, analyse and map the communication networks within a web-based information system (Sulianta, 2025). Transaction tracing technology enables researchers and investigators to follow the digital trail of cybercriminals through digital payment platforms, bank accounts and crypto wallets.

Digital forensics plays a role in identifying, collecting, analysing and presenting digital evidence so that it meets the requirements to be admissible as evidence in court (Ikumapayi & Ayankoya, 2025). The role of digital forensics in assisting with the prosecution of digital crimes is extremely important; however, digital forensics is not only used to uncover evidence of digital crimes but also of conventional crimes involving electronic or digital evidence (Abbas & Kollwitz, 2025). This tracking process involves analysing metadata, identifying IP addresses, and tracing other digital traces that can help identify the perpetrators of cybercrime.

The collection and validation of electronic evidence is a crucial stage in the evidentiary process. Digital transformation has altered the nature of legal relationships within Indonesian society, including in the context of evidence in civil cases. Documents and information that were previously in physical form are now largely available in

electronic formats, such as emails, instant messages, digital documents and online transaction records. Research findings indicate that, from a normative perspective, electronic evidence has been recognised as admissible legal evidence under the ITE Law and is positioned as an extension of admissible evidence in procedural law. However, its probative value is not automatic but depends on the fulfilment of formal and material requirements, particularly regarding authentication and data integrity. The practice of e-litigation expands the use of electronic documents in legal proceedings, but also raises challenges regarding originality, the risk of manipulation, and compliance with formalities (Kesha et al.., 2026) . The ITE Law has affirmed that electronic information and/or electronic documents, as well as printed outputs of electronic information and/or electronic documents, are recognised as valid legal evidence (Khasanah et al.., 2023) .

The role of digital forensic experts in the judicial process is essential and cannot be overlooked. In an optimal legal framework, information technology experts are not an optional addition, but rather an essential component of the evidentiary process (Utami & Wiraguna, 2025). The presence of an expert is required either at the request of a party or on the judge's initiative, particularly in complex cases or when there is a dispute regarding the authenticity of evidence. Digital forensics experts play a role in issuing reports on the results of digital forensic examinations and explaining these reports in court (Sulianta, 2025) .

The purpose of expert testimony is to shed light on a criminal offence, identify the perpetrator of the offence, support other evidence in a criminal case, and provide the judge with the confidence to deliver a verdict on the defendant. The Supreme Court has issued Supreme Court Regulation (PERMA) No. 1 of 2022 on Procedures for the Settlement of Applications and the Granting of Restitution and Compensation to Victims of Criminal Offences. To submit an application for restitution, the administrative requirements set out in Article 5 of PERMA (Fadhilah dkk., 2026).

A claim for restitution must be made in writing in Indonesian and submitted to the President/Head of the Court, either in person or via the LPSK, an investigating officer or a public prosecutor. Pursuant to Article 8 of PERMA 1 of 2022, victims may also submit a claim for restitution directly to the investigating officer whilst the case is still at the investigation stage. The investigating officer who receives the claim for restitution shall forward it to the public prosecutor to be included in the indictment (Winata & Adhari, 2024).

If a claim for restitution is rejected because the defendant has been acquitted or the charges against them have been dropped, the victim may still seek compensation by bringing a civil action before the District Court where the criminal proceedings took place (Article 9 of PERMA 1 of 2022). Under PERMA No. 1 of 2022, every District Court throughout Indonesia is obliged to receive, examine, adjudicate and settle applications for restitution or compensation submitted by victims in need. Applications for

compensation may be submitted by victims, their families or their heirs to the LPSK (Witness and Victim Protection Agency) (Purwadi, 2018) ).

Alternative dispute resolution (ADR) methods such as mediation and arbitration offer more effective and efficient non-litigation approaches. There are various forms of non-litigation dispute resolution; in particular, this article will discuss dispute resolution through mediation. Mediation is a non-litigious dispute resolution process; there are two types of mediation: in-court and out-of-court. In accordance with the provisions of Law No. 30 of 1999 on Alternative Dispute Resolution and Arbitration, out-of-court mediation is conducted in good faith (Safitri & Sa'adah, 2021). The form of dispute resolution for cybercrime in the form of phishing in international trade transactions involves opting for a non-litigation approach in the form of mediation. The mediation process involves the following stages: First, the establishment of a forum. Second, the presentation of the findings of the investigation into the evidence. Third, the problem-solving stage. Fourth, the decision-making stage (Sari, 2021). The second method of resolution is negotiation, whereby the parties reach an agreement without the intervention of a third party. The third method is mediation, whereby a mediator provides advice on resolving the dispute (Hatibie, 2025) .

The integration of criminal proceedings and civil claims (parallel proceedings) introduces complexity into judicial practice. In a single legal matter, two sets of proceedings—one criminal and one civil—may run concurrently. In such cases, where there is a connection between a civil matter currently before the court and a concurrent criminal offence, the civil matter must be resolved first before the criminal proceedings can proceed. This is referred to as a 'prejudicial geschill' in accordance with the provisions of Supreme Court Circular No. 4 of 1980 (Hakim & Yehezkiel, 2024) .

In such circumstances, law enforcement authorities must first suspend the criminal proceedings until the judge has ruled on the related civil case and the decision has become final and binding (BHT)/inkracht van gewijsde (Fakhirah, 2026) . Civil disputes or differences of opinion may be resolved by the parties through alternative dispute resolution based on good faith, thereby avoiding litigation in the District Court (Supriyadi, 2024) . In this matter, the perpetrator of the criminal offence should pay compensation, and efforts to consolidate claims for damages can be carried out in four ways, namely: (1) restitution; (2) consolidation of claims for damages; (3) through ordinary civil proceedings/actions for unlawful acts and breach of contract; and (4) through the concept of Alternative Dispute Resolution (Tomalili, 2019) .

The existence of digital forensic evidence plays a vital role in providing objective, authentic and verifiable information to uncover the material truth of a legal matter, whether in the virtual or physical realm. Digital forensics plays a crucial role in uncovering information technology-based criminal offences, including electronic fraud, digital corruption and document manipulation. The presence of experts is vital to explain the technical aspects of digital evidence to judges (Kesha et al.., 2026). Digital

forensic experts play a role in verifying the authenticity of data, analysing digital traces and providing technical validation of electronic evidence.

**Case Law and Judicial Practice in Cyber Damages Claims**

In cyber cases, claims for damages often depend on the claimant's ability to set out the damages in detail. Supreme Court case law emphasises that the claim for damages must be clear and quantifiable, as claims that are not detailed tend to be deemed vague or 'obscuur libel' (Hakim & Yehezkiel, 2024). In practice, the judge will assess whether the claim sets out the factual basis, the subject matter of the dispute, and the amount of damages in a manner that is logically and consistently provable (Rohmah, 2013) .

Civil litigation practice in cyber disputes also shows that victims can sue electronic system operators or parties who use information technology in a manner that causes harm to the public. This principle is consistent with the rationale behind Articles 38 to 39 of the ITE Law, which provide scope for civil claims for losses arising from electronic transactions. Consequently, victims of online fraud, data breaches or system manipulation may pursue their claims through civil proceedings in addition to criminal proceedings (Prayitno et al., 2023) .

In many cases, the judge first examines whether the elements of a tort have been satisfied. These elements include the existence of a tortious act, fault, damage, and a causal link between the act and the damage. If any one of these elements is not proven, the claim risks being dismissed or declared inadmissible because the grounds for the claim are not sufficiently strong (Alfianto et al.., 2024). This framework is particularly important in cyber disputes because digital evidence is often scattered and requires more rigorous proof.

Judgements in cybercrime cases show that courts still tend to focus on the punishment of perpetrators, whilst redress for victims' losses is not always a primary concern. A study of court judgements in cybercrime cases indicates that the predominant types of cases are online fraud, defamation, hate speech and the distribution of illegal content. The study also highlights inconsistencies in judges' interpretations, as well as technical obstacles in assessing electronic evidence (Singer & Friedman, 2013). When a civil claim is brought concurrently with criminal proceedings, the court must carefully assess the relationship between the two. Procedural law recognises situations where a civil case becomes a 'prejudicial geschill' in relation to a criminal case, meaning that the resolution of the civil case may first determine the factual basis of the dispute. In such circumstances, the judge may adjourn the criminal proceedings until there is legal certainty regarding the relevant civil case (Hakim & Yehezkiel, 2024). This practice demonstrates that the sequence of proceedings has a significant impact on the effectiveness of claims for damages.

Another issue arises when the authenticity of electronic evidence is called into question. In modern civil procedure, electronic documents, emails, instant messages and online transaction records can constitute admissible evidence, but their probative value remains dependent on the authentication and integrity of the data. Judges do not merely consider the form of the evidence, but also assess whether it is intact, has not been tampered with, and is relevant to the claims in the case (Kesha et al.., 2026). Consequently, many cyber cases require the support of digital forensic experts to strengthen the court's conviction.

In judicial practice, expert testimony is often used to explain technical aspects that cannot be readily understood by either the judge or the parties. Digital forensics experts play a role in explaining the process of examining data, metadata, activity logs and the reconstruction of cyber incidents. This function is important because cyber disputes often involve technical information that is not immediately apparent, such as changes to data, access logs or the source of message transmission (Sulianta, 2025). Without expert testimony, the evidence is often weak and it is difficult to link the perpetrator to the loss.

The Supreme Court has also regulated restitution and compensation for victims of criminal offences through PERMA No. 1 of 2022. This regulation provides a clearer pathway for victims to claim compensation from the perpetrator or a third party through the judicial system. Applications for restitution may be submitted in writing and must meet certain administrative requirements, including through the investigating officer, the public prosecutor, or the National Commission for the Protection of Victims of Crime (LPSK) (Fadhilah dkk., 2026). In the context of cybercrime, this regulation is important because many victims require a formal channel to recover their financial losses.

In practice, the courts also accept applications for restitution filed as early as the investigation stage. Victims may submit an application via the investigating officer so that the losses can be included in the prosecution proceedings. If restitution is granted, victims receive compensation for material losses and, in certain situations, other losses recognised by law (Wijaya & Purwadi, 2018). This mechanism strengthens the position of victims, who have often merely been witnesses in criminal cases. However, if restitution fails or cannot be enforced, victims may still pursue a standard civil claim. Such claims are usually based on Article 1365 of the Civil Code concerning unlawful acts, with claims for damages that must be substantiated in detail (Fakhirah, 2026) . Case law indicates that claims which do not specify the amount of loss risk being deemed inadmissible (Rohmah, 2013) . Consequently, the formulation of the claim becomes crucial in cyber damages disputes.

In cases involving personal data breaches, judicial practice is increasingly recognising that aggrieved victims may bring claims for damages before the competent courts. This demonstrates an expansion of protection for victims who have suffered

losses not only financially, but also as a result of the misuse of their personal data. Nevertheless, victims must still demonstrate a clear causal link between the data breach and the losses suffered (Zakky et al.., 2026) . This burden of proof often poses a major obstacle in cyber litigation.

In e-commerce disputes or cases of digital fraud, the court also frequently considers whether electronic transactions can be substantiated by digital contracts, proof of transfer, electronic communications and system logs. Such evidence is crucial for establishing the existence of a legal relationship between the parties and the occurrence of actual loss. If the evidence is sufficiently strong, the judge may award some or all of the damages claimed (Tamba, 2018) . Conversely, if the evidence is inconsistent, the claim may be dismissed even if, in fact, the claimant feels they have suffered a loss.

Developments in case law also show that the courts still require more uniform standards when assessing non-pecuniary damages. In practice, there are no fixed criteria for non-pecuniary damages, meaning that judges have considerable discretion. This discretion can result in differing judgements for similar cases (Fakhirah, 2026). Consequently, consistency in case law is an urgent necessity in cyber damages cases.

On the other hand, research into court rulings on cybercrime indicates that judges tend to consider the legality, fairness and social impact of criminal offences. Whilst these considerations are important, they are not always sufficient to meet victims' needs for swift and certain redress. Therefore, reforms to judicial practice must strengthen the focus on victim redress, rather than merely punishing perpetrators (Singer & Friedman, 2013). This will make cyber law more responsive to victims' needs.

Thus, case law and judicial practice in cyber damages claims reveal two key points. Firstly, the courts have already opened the door to electronic evidence, restitution and civil claims based on tort. Secondly, there are still obstacles regarding the quantification of damages, the authentication of evidence and the consistency of judicial rulings. Consequently, strengthening the guidelines on the burden of proof and the drafting of claims is key to ensuring that victims of cybercrime receive effective redress.

**Conclusion**

Cybercrime is a complex new criminal phenomenon that is on a significant upward trend in Indonesia, encompassing online fraud, phishing, ransomware and defamation. According to data from the National Cyber and Cryptography Agency (BSSN) and the Indonesian National Police (Polri), financial losses resulting from cybercrime reached Rp 476 billion between November 2024 and January 2025, with over 32,000 reports and 29,000 victims. However, criminal law enforcement still shows a gap in the recovery of victims' losses, where the primary focus on punishing perpetrators often overlooks the need for restitution and compensation for victims.

Technical efforts in resolving disputes over compensation for damages resulting from cybercrime encompass several key, interrelated components. The mechanism for tracing perpetrators and digital assets through digital forensics is a crucial first step in identifying electronic traces and mapping communication networks. The collection and validation of electronic evidence require compliance with formal and substantive requirements, particularly regarding data authentication and integrity. The role of digital forensic experts is essential in explaining the technical aspects of digital evidence to judges. Furthermore, there are alternative dispute resolution methods through mediation and arbitration, which offer a non-litigious approach, as well as the integration of criminal and civil proceedings (parallel proceedings), which requires the establishment of a 'prejudicial geschill'.

Case law and judicial practice in cyber damages claims indicate that the courts have already made provision for electronic evidence, restitution under PERMA No. 1 of 2022, and civil claims based on Article 1365 of the Civil Code concerning unlawful acts. However, there remain obstacles regarding the specification of damages in the statement of claim, the authentication of electronic evidence, and the consistency of judges' rulings in assessing non-pecuniary damages. To strengthen the effectiveness of protection for victims of cybercrime, there is a need for regulatory harmonisation between criminal and civil law, the strengthening of standards for the authentication of electronic evidence, the enhancement of law enforcement officers' capacity in digital forensics, and the development of consistent jurisprudential guidelines for the assessment of cyber damages.

**References**


Abbas, A., & Kollwitz, E. (2025). *Forensic Accounting in the Digital Era: Leveraging AI for Fraud Detection and Risk Management*. ResearchGate. DOI: DOI. https://www.researchgate.net/profile/Zafar-Iqbal-136/publication/390426423_Forensic_Accounting_in_the_Digital_Era_Leveraging_AI_for_Fraud_Detection_and_Risk_Management/links/67ed3b5449e91c0fead5f2cc/Forensic-Accounting-in-the-Digital-Era-Leveraging-AI-for-Fraud-Detection-and-Risk-Management.pdf

Afrianto, T., & Jamaludin, A. (2025). Menyoroti Maraknya Penipuan Investasi Bodong di Era Digital dalam Bentuk Pinjaman Online Ilegal dengan Modus Pinjaman Cepat dan Bunga yang Rendah di Indonesia. *Jurnal Hukum Lex Generalis*, *6*(7). https://doi.org/10.56370/jhlg.v6i7.2070

Alfianto, D., Rido, A., & Wijaya, G. V. (2024). Pertanggungjawaban Perdata dan Tanggung Gugat Dalam Perkara Wanprestasi Dan Perbuatan Melawan Hukum. *Jurnal Pengabdian Masyarakat: Pemberdayaan, Inovasi Dan Perubahan*, *4*(6). https://doi.org/10.59818/jpm.v4i6.986

Ashilah, A. P., & Rahman, R. (2024). FORENSIK JARINGAN UNTUK INVESTIGASI KEJAHATAN CYBER PADA STUDI KASUS PEMBOBOLAN DATA KOMINFO OLEH

BJORKA. *Jurnal Riset Sistem Informasi*, *1*(3), 17–26. https://doi.org/10.69714/g2pay047

Budiyanto. (2025). *Pengantar Cybercrime dalam Sistem Hukum Pidana di Indonesia*. Sada Kurnia Pustaka.

Eliyah, E., & Aslan, A. (2025). STAKE'S EVALUATION MODEL: METODE PENELITIAN. *Prosiding Seminar Nasional Indonesia*, *3*(2), Article 2.

Fadhilah, M. 'Ainul Q., Bimantara, A., Elva, R., & Nurhasan, M. A. R. (2026). Raformulasi Frasa Sejak Diketahui dalam Peraturan Mahkamah Agung Nomor 1 Tahun 2022 tentang Tata Cara Penyelesaian Permohonan dan Pemberian Restitusi dan Kompensasi Kepada Korban Tindak Pidana. *Jurnal Hukum Lex Generalis*, *7*(7). https://doi.org/10.56370/jhlg.v7i7.3522

Fakhirah, N. R. (2026). PENGARUH TEKNOLOGI ARTIFICIAL INTELLIGENCE TERHADAP KEABSAHAN ALAT BUKTI ELEKTRONIK DALAM PEMBUKTIAN PERKARA PIDANA. *Jurnal Riset Multidisiplin Edukasi*, *3*(6), 999–1011. https://doi.org/10.71282/jurmie.v3i6.2224

Hakim, J., & Yehezkiel, N. (2024). Mempertanyakan Bukti Elektronik sebagai Alat Bukti dalam Kasus Pidana. *HukumOnline, nd https://www. hukumonline. com/berita/a/mempertanyakan-buktielektronik-sebagai-alat-bukti-dalam-kasus-pidana-lt667b57ba9f459*.

Hatibie, H. S. (2025). Revolusi Penyelesaian Sengketa Digital: Transformasi Sistem Peradilan Melalui Online Dispute Resolution di Era Ekonomi Digital. *Al-Zayn : Jurnal Ilmu Sosial & Hukum*, *3*(6), 9920–9934. https://doi.org/10.61104/alz.v3i6.2694

Ikumapayi, O. J., & Ayankoya, B. B. (2025). AI-powered forensic accounting: Leveraging machine learning for real-time fraud detection and prevention. *International Journal of Research Publication and Reviews*, *6*(2), 236–250.

Kesha, R., Jafair, M. A. B., & Putri, R. C. (2026). Kekuatan Pembuktian Alat Bukti Elektronik Dalam Hukum Acara Perdata Indonesia. *Journal of Golden Generation Legal Science*, *2*(2), 374–383.

Khasanah, D. D., Iftitah, A., Kasiani, Abas, M., Sipayung, B., Hastarini, A., Arifuddin, Q., Dewi, S. R., Anita, A. A., Dewi, N., Jenar, S., Bhakti, I. S. G., Faried, F. S., Tarmizi, R., Ningtyas, M. A., Puspandari, R. Y., & Rohmah, A. N. (2023). *Hukum Perdata*. Sada Kurnia Pustaka.

Prayitno, M. P. R., Leonard, L. T., & Utama, K. W. (2023). TINJAUAN YURIDIS TERHADAP UPAYA ADMINISTRATIF DALAM PENYELESAIAN SENGKETA TATA USAHA NEGARA. *Diponegoro Law Journal*, *12*(2). https://doi.org/10.14710/dlj.2023.37895

Rohmah, B. M. (2013). *Obscuur libel dalam gugatan waris: Studi perkara No. 1444/Pdt. G/2011/PA. Mlg* [PhD Thesis, Universitas Islam Negeri Maulana Malik Ibrahim]. http://etheses.uin-malang.ac.id/id/eprint/155

Safitri, E. D., & Sa'adah, N. (2021). Penerapan Upaya Administratif Dalam Sengketa Tata Usaha Negara. *Jurnal Pembangunan Hukum Indonesia*, *3*(1), 34–45. https://doi.org/10.14710/jphi.v3i1.34-45

Sari, U. I. P. (2021). Kebijakan Penegakan Hukum Dalam Upaya Penanganan Cyber Crime Yang Dilakukan Oleh Virtual Police Di Indonesia. *Journal of Studia Legalia*, *2*(01), 58–77. https://doi.org/10.61084/jsl.v2i01.7

Septiari, N., & Ujianti, N. M. P. (2025). Kekuatan hukum perjanjian elektronik dalam perspektif KUH Perdata dan UU ITE. *Indonesian Journal of Law and Justice*, *2*(4), 10–10.

Singer, P. W., & Friedman, A. (2013). *Cybersecurity and Cyberwar: What Everyone Needs to Know®*. Oxford University Press.

Singgi, I. G. A. S. K., Suryawan, I. G. B., & Sugiartha, I. N. G. (2020). Penegakan Hukum terhadap Tindak Pidana Peretasan sebagai Bentuk Kejahatan Mayantara (Cyber Crime). *Jurnal Konstruksi Hukum*, *1*(2), 334–339. https://doi.org/10.22225/jkh.1.2.2553.334-339

Sulianta, F. (2025). *Serangan Siber: Teori, Praktik, dan Solusi*. Feri Sulianta.

Sumadiyasa, I. K. A., Sugiartha, I. N. G., & Widyantara, I. M. M. (2021). Pertanggungjawaban Pidana Pelaku Cyber Crime Dengan Konten Pornogafi. *Jurnal Interpretasi Hukum*, *2*(2), 372–377. https://doi.org/10.22225/juinhum.2.2.3443.372-377

Supriyadi, M. W. (2024). Administrasi Sengketa Pajak dan Persidangan Secara Elektronik (E-Tax Court)—Suatu Tinjauan Pustaka. *JURNAL PAJAK INDONESIA (Indonesian Tax Review)*, *8*(1), 127–144. https://doi.org/10.31092/jpi.v8i1.2694

Tamba, I. (2018). Peran Bpsk dalam Penyelesaian Sengketa Konsumen di Indonesia untuk sebagai Wujud Cita-cita Perlindungan Konsumen di Bidang Ekonomi. *Ensiklopedia of Journal*, *1*(1), 79–84.

Tomalili, R. (2019). *Hukum Pidana*. Deepublish.

Utami, G. C., & Wiraguna, S. A. (2025). Pembuktian digital dalam sengketa perdata: Menguji validitas formil dan materiil dokumen elektronik di era modern. *Referendum: Jurnal Hukum Perdata Dan Pidana*, *2*, 40–52.

Wijaya, I. A., & Purwadi, H. (2018). PEMBERIAN RESTITUSI SEBAGAI PERLINDUNGAN HUKUM KORBAN TINDAK PIDANA. *Jurnal Hukum Dan Pembangunan Ekonomi*, *6*(2). https://doi.org/10.20961/hpe.v6i2.17728

Winata, T., & Adhari, A. (2024). Dasar Kriteria Dalam Menentukan Adanya Penipuan Dan Wanprestasi Dalam Yurisprudensi Mahkamah Agung Nomor No.4/Yur/Pid/2018. *UNES Law Review*, *6*(4), 10643–10650. https://doi.org/10.31933/unesrev.v6i4.2026

YOGI OKTAFIAN ARISANDY. (2021). *PENEGAKAN HUKUM PIDANA TERHADAP CYBER CRIME HACKER* [S1, Universitas Muhammadiyah Yogyakarta]. https://etd.umy.ac.id/id/eprint/3466/

Zakky, M. S., Asshidiqi, A., & Simarmata, A. S. H. (2026). Legal Analysis of Issues of Evidence and Testimony in Civil Disputes in Court. *Journal of Legal, Political, and Humanistic Inquiry*, *1*(4), 218–226. https://doi.org/10.65310/08138888

Zed, M. (2008). *Metode Penelitian Kepustakaan*. Yayasan Pustaka Obor Indonesia.

Mahkamah Agung. (2022, Juli 27). *Perma 1 Tahun 2022 atur tata cara pengajuan restitusi dan kompensasi korban tindak pidana*.

Mahkamah Agung. (2025a, September 18). *Restitusi, pelindungan bagi korban tindak pidana*. MariNews.

Mahkamah Agung. (2025b, Mei 11). *Yurisprudensi MA RI: Gugatan ganti rugi kepada pelapor*.