

THE POSITION OF DIGITAL FORENSICS AS EVIDENCE IN LAW ENFORCEMENT OF CRIMINAL VIOLATIONS COPYRIGHT IN THE CYBER DOMAIN

Windy Anggraini¹, M. Citra Ramadhan², Azwir Agus³
Magister Ilmu Hukum / Universitas Medan Area, Indonesia
E-mail: windyanggraini63@gmail.com

Received : 20 June 2026
Revised : 29 June 2026

Accepted : 11 July 2026
Published : 31 July 2026

Abstract

This study discusses the position of digital forensics as evidence in law enforcement of copyright infringement crimes in the cyber realm. The formulation of the research problem is: (1) What is the role of digital forensics in the criminal evidence system in Indonesia? (2) What are the legal challenges in utilizing digital forensics to uncover copyright infringement on the Internet? and (3) How effective is digital forensics in supporting the legal evidence process for copyright crimes committed online? This study uses a normative juridical research type with a descriptive-analytical nature, through a literature study of primary, secondary, and tertiary legal materials. The analysis is carried out using a statutory approach and a conceptual approach to examine relevant regulations, doctrines, and legal theories. The results of the study indicate that digital forensics has an important role in proving copyright infringement, despite legal challenges related to its validity, procedures, and application. This study provides a normative overview of the position of digital forensics and its contribution to law enforcement in the digital era.

Keywords: Digital Forensics, Electronic Evidence, Copyright, Law Enforcement

INTRODUCTION

The development of information and communication technology has brought about significant changes in various aspects of life, including the legal field and the protection of Intellectual Property Rights (IPR). Advances in digital technology enable creative works such as music, films, books, software, and various other digital works to be produced, copied, and distributed rapidly via the internet. On the one hand, this development facilitates the dissemination of works and increases the economic value of human creativity. However, on the other hand, this ease also opens up opportunities for copyright infringement on an increasingly widespread scale. Creative works can easily be pirated, copied, modified, and distributed without the permission of the creator or rights holder. This situation makes copyright infringement in the digital space an increasingly complex legal issue.

Copyright is a part of Intellectual Property Rights that provides legal protection for works in the fields of science, art, and literature. This protection includes the economic rights and moral rights of the creator. Economic rights authorize the creator or rights holder to obtain economic benefits from the use of his creation, while moral rights relate to recognition of the creator and protection of the integrity of his creation. In Indonesia, copyright protection is regulated by Law Number 28 of 2014 concerning Copyright. Although it has provided a fairly comprehensive legal basis, the development of digital technology has created new challenges in the implementation and enforcement of copyright law, particularly related to proving violations committed through electronic media.

Copyright infringement in the digital space has distinct characteristics from conventional infringement. Perpetrators can use false identities, conceal their location, and distribute works across regions and even countries. Furthermore, evidence of infringement is generally in the form of electronic data that can be easily altered, moved, deleted, or hidden. In such circumstances, the law enforcement process depends not only on the existence of laws and regulations but also on the ability of law enforcement officials to locate, secure, analyze, and prove the authenticity and integrity of digital evidence.

This problem is further complicated by the fact that Indonesia's criminal evidence system was initially built on the characteristics of conventional evidence. Article 184 of the Criminal Procedure Code (KUHP) regulates valid evidence in the form of witness testimony, expert testimony, letters, clues, and defendant testimony. Meanwhile, technological developments have given rise to various forms of electronic evidence, such as metadata, activity logs, Internet Protocol (IP) addresses, e-mail, digital communication recordings, and various data stored on

THE POSITION OF DIGITAL FORENSICS AS EVIDENCE IN LAW ENFORCEMENT OF CRIMINAL ACTS OF COPYRIGHT INFRINGEMENT IN THE CYBER DOMAIN

Windy Anggraini et al

electronic devices and digital platforms. Although the existence of electronic information and electronic documents has been recognized through the Electronic Information and Transactions Law, issues remain regarding the procedures for obtaining, securing, examining, and ensuring the integrity of digital evidence so that it can be optimally used in the criminal evidence process.

In this context, digital forensics plays a crucial role. Digital forensics is a discipline focused on the identification, collection, preservation, examination, analysis, and presentation of digital data related to a legal event. Through digital forensic methods, law enforcement can trace the origins of a file, analyze metadata, examine device activity, trace digital traces, and identify the relationship between electronic data and the perpetrator of a crime. Thus, digital forensics serves not only as a technical means to recover data but also as an instrument to maintain the authenticity and integrity of evidence so that it can be accounted for in the judicial process.

In digital copyright infringement cases, the application of digital forensics is becoming increasingly important because most crimes are committed through electronic devices and the internet. Movie piracy, unauthorized music distribution, illegal e-book distribution, and the use of unauthorized software leave digital traces that can be used to uncover crimes. Data in the form of file metadata, access history, activity logs, electronic communications, digital transactions, and information from online platforms can be crucial in constructing evidence. However, the evidentiary value of this data depends heavily on the process by which it is obtained, the examination method, and the ability to demonstrate that the data has not been altered or manipulated.

The application of digital forensics in law enforcement against copyright infringement still faces various obstacles. These obstacles include limited technical regulations regarding digital evidence procedures, a lack of uniform mechanisms for handling and preserving electronic evidence, limited human resources competent in digital forensics, and coordination issues between law enforcement agencies and institutions authorized to protect intellectual property. Furthermore, the anonymous, rapid, and cross-jurisdictional nature of digital copyright infringement complicates the process of identifying perpetrators and gathering relevant evidence.

The gap between technological developments and legal and institutional capacity to handle digital evidence demonstrates the need to strengthen the evidentiary system in copyright infringement cases. Recognizing electronic evidence alone is insufficient without a clear mechanism for how it is obtained, safeguarded, analyzed, and presented in court. In this regard, the testimony of digital forensic experts plays a crucial role in explaining the technical processes surrounding the origin, authenticity, integrity, and relationship of electronic data to the crime. Thus, digital forensics serves as a bridge between the development of information technology and the need for evidence in the criminal justice system.

Based on the above description, the issue of the position and role of digital forensics in proving criminal acts of copyright infringement in the digital space is important to study. This research focuses on a legal analysis of the use of digital forensics as an evidentiary instrument in copyright infringement cases, including aspects of the validity, integrity, and effectiveness of digital evidence in the law enforcement process. This study is expected to contribute to the development of criminal evidence law in Indonesia, particularly in dealing with the characteristics of digital crimes, as well as provide ideas for strengthening regulations, the capacity of law enforcement officers, and mechanisms for handling electronic evidence in copyright infringement cases.

LITERATURE REVIEW

1. Copyright in Legal Perspective

Copyright is a subset of Intellectual Property Rights that provides legal protection for works produced through human intellectual ability. Copyright protection covers works in the fields of science, art, and literature, including works created and distributed in digital form. Copyright grants the creator or rights holder exclusive rights to control the use of their creation, both economically and morally. With the development of information technology, copyright protection faces increasingly complex challenges because digital works can be copied, modified, and distributed quickly without permission.

Law Number 28 of 2014 concerning Copyright provides the legal basis for the protection of creators and copyright holders. However, the characteristics of copyright infringement in the digital space present unique challenges in the law enforcement process. Infringements can be committed anonymously, using various digital platforms, and involving the distribution of data across regions. Therefore, copyright law enforcement requires evidentiary methods that adapt to the characteristics of digital technology.

THE POSITION OF DIGITAL FORENSICS AS EVIDENCE IN LAW ENFORCEMENT OF CRIMINAL ACTS OF COPYRIGHT INFRINGEMENT IN THE CYBER DOMAIN

Windy Anggraini et al

2. Digital Forensics and Electronic Evidence

Digital forensics is a field of science that focuses on the identification, collection, preservation, examination, analysis, and presentation of digital data for legal purposes. Digital data can originate from computers, mobile phones, internet networks, servers, storage media, and various digital platforms. Digital forensics must be conducted systematically to ensure the authenticity of the evidence obtained and ensure its legal validity.

In digital copyright infringement cases, digital forensics can be used to trace the origins of a file, analyze metadata, examine access history, identify devices used, and link digital activity to the alleged infringer. Thus, digital forensics serves not only to locate data but also to ensure its integrity and relevance to the case under investigation.

Electronic evidence differs from conventional evidence in that it is easily copied, moved, altered, and deleted. Therefore, the acquisition and preservation of digital evidence must be conducted using methods that guarantee the authenticity and integrity of the data. Failure to maintain these processes can cast doubt on the validity of digital evidence in judicial proceedings.

3. Proving Criminal Acts in the Indonesian Legal System

Proving is a crucial stage in the criminal justice process because it determines whether a crime and the defendant's involvement can be proven. The criminal proof system in Indonesia generally refers to the provisions of the Criminal Procedure Code, which recognizes several valid forms of evidence: witness testimony, expert testimony, letters, clues, and the defendant's testimony.

The development of information technology has led to the emergence of various forms of electronic data that are relevant to proving criminal acts. Electronic information and electronic documents have received legal recognition through laws and regulations in the field of electronic information and transactions. However, the issue extends beyond the recognition of electronic evidence to the process of obtaining, examining, securing, and presenting such evidence in court.

In digital copyright infringement cases, the testimony of a digital forensics expert plays a crucial role in explaining the technical aspects of electronic evidence. Experts can explain the data examination process, file authenticity, metadata, device activity, and the relationship between digital evidence and criminal events. Therefore, expert testimony is a crucial element in bridging the technical aspects of information technology with the needs of legal evidence.

4. Digital Forensics in Copyright Law Enforcement

The use of digital forensics in copyright enforcement is becoming increasingly important as the internet becomes a means of distributing copyrighted works. Violations such as film piracy, unauthorized distribution of music, illegal distribution of digital books, and the use of unauthorized software can leave numerous digital traces that can be forensically analyzed.

Evidence in the form of metadata, activity logs, IP addresses, communication records, transaction histories, and data from digital platforms can help uncover the process of violations and identify the parties involved. However, the effectiveness of using such evidence depends heavily on the capabilities of law enforcement officials, the availability of technological resources, and the existence of clear legal procedures for handling digital evidence.

Literature discussing copyright generally focuses more on legal protection for creators, forms of infringement, and legal liability of perpetrators. Meanwhile, studies on digital forensics focus more on the technical aspects of collecting and analyzing electronic evidence. There is still room for research specifically linking copyright protection, criminal evidence systems, and the use of digital forensics in copyright infringement cases in the digital space.

Based on the literature review, this study positions digital forensics as a crucial instrument in proving copyright infringement. This research not only examines the position of digital evidence in the Indonesian legal system but also analyzes the legal and technical challenges in its application. Therefore, this research is expected to fill the gap in research regarding the relationship between digital technology developments, copyright protection, and the criminal evidence system in law enforcement in Indonesia.

RESULTS AND DISCUSSION

1. The Role of Digital Forensics in the Criminal Evidence System in Indonesia

The development of information technology has changed the characteristics of criminal acts and the evidence used in law enforcement. Crimes committed through electronic devices and the internet generally do

THE POSITION OF DIGITAL FORENSICS AS EVIDENCE IN LAW ENFORCEMENT OF CRIMINAL ACTS OF COPYRIGHT INFRINGEMENT IN THE CYBER DOMAIN

Windy Anggraini et al

not leave physical evidence like conventional crimes, but rather leave digital traces that are easily changed, deleted, moved, or manipulated. Therefore, digital forensics plays a crucial role in the criminal evidence system in Indonesia, as it systematically identifies, secures, collects, examines, analyzes, and presents digital data in a scientifically and legally justifiable manner.

From a legal perspective, digital forensics plays a role in validating electronic evidence used in the evidentiary process. Electronic information, electronic documents, and their printouts have been recognized as valid legal evidence under the provisions of laws and regulations in the field of electronic information and transactions. However, digital forensics is not essentially a stand-alone form of evidence, but rather a scientific method used to obtain and ensure the authenticity, integrity, and relevance of digital evidence to the crime. Therefore, digital forensics can strengthen existing evidence recognized in the criminal procedure system, including expert testimony, letters, clues, and electronic evidence.

The role of digital forensics is also evident in its ability to transform volatile digital data into evidence that can be used in the legal process. Through the stages of identification, acquisition, preservation, analysis, and reporting, digital data can be scientifically processed to explain the relationship between devices, accounts, digital activities, and criminal acts. The application of chain of custody principles and the use of hash values are crucial to ensure that the evidence obtained remains intact and unchanged from its initial discovery until its presentation in court. Therefore, digital forensics plays a strategic role in discovering material truth and supporting the implementation of due process of law in the criminal justice process.

In copyright infringement cases, digital forensics can be used to analyze files, metadata, activity logs, IP addresses, electronic devices, and traces of copyrighted works' distribution over the internet. Through these examinations, law enforcement officials can identify unauthorized duplication, distribution, or use of copyrighted works. Thus, digital forensics serves not only as a technical aid in the investigative process but also as a crucial instrument in constructing evidence against crimes committed in the digital space.

Based on this description, it can be understood that the role of digital forensics in the criminal evidence system in Indonesia lies in its ability to bridge the development of digital technology with the needs of legal evidence. Digital forensics ensures that obtained electronic evidence can be assessed objectively, scientifically, and responsibly. In the context of online copyright crimes, digital forensics serves to strengthen the criminal evidence system by providing a technical and scientific basis for judges in assessing the authenticity and relevance of digital evidence to the crime being charged.

2. Legal Challenges in Using Digital Forensics to Uncover Copyright Infringement on the Internet

The use of digital forensics to uncover copyright infringements on the internet still faces various legal challenges. The first challenge relates to the incomplete integration of regulations regarding electronic evidence and digital forensic procedures within the criminal procedural law system. Although electronic information and documents have been recognized as valid evidence, regulations regarding technical standards for the collection, examination, preservation, and presentation of digital evidence have not been comprehensively regulated. This situation can lead to differing interpretations regarding the validity and evidentiary value of digital forensic findings in judicial proceedings.

This challenge is further complicated by the interplay between several different regulations: criminal procedure law, regulations on electronic information and transactions, and regulations on copyright. The Copyright Law protects the economic and moral rights of creators, while regulations on electronic information provide the basis for recognizing digital evidence. However, there are no specific and detailed regulations governing the mechanism for proving copyright infringement committed over the internet using digital forensic methods. This lack of consistency can create uncertainty for law enforcement officials in determining the appropriate procedures for obtaining and using digital evidence.

Another legal challenge relates to the validity of the digital evidence acquisition process. Electronic evidence is highly susceptible to alteration and manipulation. If the collection, seizure, acquisition, or examination process is conducted without due regard for procedural principles and forensic standards, the authenticity and integrity of the evidence may be questioned in court. Therefore, every process for handling digital evidence must be transparent, documented, and follow procedures that ensure the continuity of the chain of custody. Irregularities in this process can cause digital evidence to lose credibility and reduce its evidentiary value. In addition to regulatory issues, copyright infringement via the internet also raises jurisdictional issues. Perpetrators, victims, servers, and digital platforms can be located in different countries. This situation means that the evidence-gathering process cannot always be carried out directly by Indonesian law enforcement. In

certain circumstances, international cooperation through mutual legal assistance mechanisms is required. This process can be lengthy and depends on the laws and policies of the country where the digital evidence is located. This situation is one of the obstacles to maintaining the speed and effectiveness of the investigation process.

Another challenge stems from the perpetrators' use of obfuscation technologies, such as encryption, VPNs, fake identities, offshore servers, and anti-forensic techniques. These technologies can be used to conceal the perpetrator's identity, location, and activities, making tracking more difficult. Furthermore, limited human resources, technological resources, forensic laboratories, and law enforcement officials' understanding of the characteristics of digital evidence also influence the effectiveness of digital forensics. Therefore, it is necessary to improve the competence of investigators, prosecutors, and judges, as well as to develop uniform operational standards for handling digital evidence.

Thus, the legal challenges in utilizing digital forensics lie not only in imperfect regulations, but also encompass issues of procedural validity, cross-border jurisdiction, institutional limitations, and the ability of authorities to understand and assess digital evidence. Addressing these challenges requires regulatory harmonization, standardization of digital forensic procedures, strengthening inter-institutional cooperation, and increasing human resource capacity to ensure consistent use of digital forensic results and optimal evidentiary value.

3. The Effectiveness of Digital Forensics in Supporting the Legal Evidence Process for Copyright Crimes Committed Online

Digital forensics is highly effective in supporting the process of proving copyright crimes committed online because it can uncover digital traces that cannot be found through conventional evidentiary methods. Copyright infringement via the internet, such as unauthorized duplication, distribution, and dissemination of copyrighted works, generally leaves behind various electronic data that can be scientifically analyzed. This data can include copyright files, metadata, IP addresses, server logs, account activity history, and digital content distribution records.

The effectiveness of digital forensics can be seen in its ability to guarantee the authenticity, integrity, and traceability of electronic evidence. The use of hash values, documentation of the acquisition process, and the implementation of a chain of custody enable law enforcement officials to prove that the digital evidence presented in court is the same as that obtained during the investigation. These procedures are crucial because digital evidence is susceptible to change and manipulation. The better the preservation and documentation processes, the higher the level of confidence in the digital evidence.

Selain itu, digital forensik efektif dalam mengungkap hubungan antara karya cipta yang dilanggar dengan pelaku tindak pidana. Teknik analisis metadata, data carving, pemeriksaan log jaringan, serta penelusuran aktivitas perangkat dapat membantu mengidentifikasi proses penggandaan dan distribusi karya cipta secara ilegal. Penggunaan teknologi digital watermarking dan digital fingerprinting juga dapat membantu mengidentifikasi keaslian karya serta menelusuri jalur penyebaran konten yang dilakukan tanpa izin. Dengan demikian, digital forensik dapat memberikan kontribusi terhadap pembuktian unsur perbuatan, kesalahan, dan keterlibatan pelaku dalam tindak pidana pelanggaran hak cipta.

Meskipun memiliki efektivitas yang tinggi secara teknis dan konseptual, penerapan digital forensik dalam praktik masih belum sepenuhnya optimal. Efektivitasnya dipengaruhi oleh kompetensi aparat penegak hukum, ketersediaan peralatan dan laboratorium forensik, penerapan metodologi yang tepat, serta kejelasan regulasi. Keterbatasan pemahaman penyidik, jaksa, maupun hakim terhadap karakteristik bukti digital dapat menyebabkan hasil pemeriksaan forensik tidak dimanfaatkan secara maksimal dalam proses pembuktian. Selain itu, keterbatasan sarana teknologi dan belum meratanya fasilitas forensik digital juga dapat memperlambat proses pemeriksaan perkara.

Efektivitas digital forensik juga dipengaruhi oleh karakteristik pelanggaran hak cipta yang bersifat lintas batas negara. Penggunaan VPN, enkripsi, server luar negeri, serta platform digital global dapat menghambat proses identifikasi pelaku dan pengamanan bukti. Oleh karena itu, efektivitas digital forensik tidak hanya bergantung pada kecanggihan teknologi, tetapi juga pada kemampuan kelembagaan dan kerja sama antarnegara dalam memperoleh data digital yang relevan.

Berdasarkan uraian tersebut, digital forensik dapat dinilai efektif dalam mendukung proses pembuktian tindak pidana hak cipta yang dilakukan secara daring, terutama karena mampu mengubah jejak digital menjadi bukti yang dapat dianalisis dan dipertanggungjawabkan secara hukum. Namun, efektivitas tersebut bersifat kondisional. Artinya, digital forensik akan memberikan daya dukung pembuktian yang optimal apabila didukung

THE POSITION OF DIGITAL FORENSICS AS EVIDENCE IN LAW ENFORCEMENT OF CRIMINAL ACTS OF COPYRIGHT INFRINGEMENT IN THE CYBER DOMAIN

Windy Anggraini et al

oleh regulasi yang jelas, prosedur yang terstandar, sumber daya manusia yang kompeten, sarana teknologi yang memadai, serta kerja sama antar lembaga dan antarnegara. Dengan demikian, penguatan aspek teknis dan yuridis secara bersamaan merupakan syarat utama agar digital forensik mampu mendukung penegakan hukum hak cipta secara efektif di era digital.

CONCLUSION

1. Digital forensics plays a crucial role in the criminal evidence system in Indonesia, particularly in cases of copyright infringement in cyberspace. Digital forensics serves as a scientific method to ensure the authenticity, integrity, and reliability of electronic evidence through the application of the principles of authenticity, integrity, reliability, and chain of custody. Through a legitimate and standardized digital forensics process, electronic data and information can be transformed into legally binding evidence and can be accounted for in court. In the Indonesian criminal law system, digital forensics is closely related to evidence as stipulated in Article 184 of the Criminal Procedure Code, particularly through expert testimony, documentary evidence, and instructions, with legal recognition of electronic evidence as stipulated in the Electronic Information and Transactions Law. Therefore, digital forensics is an important foundation in bridging technological developments with the criminal law evidence system, so that law enforcement against criminal copyright infringement in cyberspace can be carried out effectively, legally, and fulfill the principles of legal certainty and justice.
2. The use of digital forensics to uncover copyright infringement on the internet still faces complex and interrelated legal challenges. These challenges include the lack of harmonization between the Criminal Procedure Code (KUHP), the ITE Law, and the Copyright Law, which has created legal uncertainty regarding the status and evidentiary value of digital forensics results. The validity of digital evidence is often questioned due to the lack of uniform procedural standards, weak chain of custody implementation, and limited technical capacity and coordination among law enforcement officials. Technical challenges such as perpetrator anonymity, cross-border jurisdiction, and the volatile nature of digital data further complicate the tracing and evidence-gathering process. These conditions indicate that although digital forensics is substantively important in proving copyright infringement in the cyber realm, its effectiveness is still hampered by regulatory, institutional, and technical factors that have not been optimally integrated.
3. Digital forensics plays a strategic role in supporting the process of proving criminal acts of copyright infringement committed online. Digital forensics enables the identification, security, analysis, and presentation of digital evidence in a legal and accountable manner, thus becoming the primary means of proving the perpetrator's actions, guilt, and accountability. Its effectiveness is influenced by technical factors, such as human resource competence and forensic methodology; legal and institutional factors, including legal certainty, the availability of forensic laboratories, and synergy between institutions; and external factors, such as the cross-jurisdictional nature of cybercrime and the use of obfuscation technology by perpetrators. Although digital forensics is technically highly effective, law enforcement practices in Indonesia still face obstacles related to limited human resources, technology, institutions, and regulations that are not yet fully adaptive to the dynamics of online copyright crime.

REFERENCES

- Rahmi. *Perlindungan Hak Cipta di Era Digital*. Yogyakarta: Deepublish, 2018.
- Abdul Wahid dan Mohammad Labib. *Kejahatan Mayantara (Cyber Crime)*. Bandung: Refika Aditama, 2018.
- Achmad Ali, *Menguak Tabir Hukum, Edisi kedua*. Jakarta: Penerbit Kencana; Prenadamedia Group, 2015.
- Agus Rahardjo. *Pembuktian Digital dalam Sistem Peradilan Pidana Indonesia*. Jakarta: Prenadamedia Group, 2020.
- Ahmad M. Ramli. *Cyberlaw dan HAKI dalam Sistem Hukum Indonesia*. Bandung: Refika Aditama, 2013.
- Ahmad M. Ramli. *Hak Cipta dalam Era Digital*. Bandung: Alumnus, 2020.
- Ahmad Sofian. *Pembuktian Digital dalam Sistem Peradilan Pidana Indonesia*. Jakarta: Prenadamedia Group, 2021.
- Al-Azhar, Muhammad Nuh. *Digital Forensic Panduan Praktis Investigasi Komputer*, 2012.
- Al-Azhar. *Digital Forensics: Theory and Practice*. Jakarta: Salemba Teknika, 2012.
- Alfian. *Hukum Pembuktian dalam Perkara Pidana*. Yogyakarta: FH UII Press, 2017.
- Amiruddin dan Zainal Asikin. *Pengantar Metode Penelitian Hukum*. Jakarta: RajaGrafindo Persada, 2015.
- Ante. *Sistem Pembuktian dalam Hukum Acara Pidana*. Jakarta: Kencana, 2016.
- Budi Agus Riswandi. *Hukum Hak Cipta di Era Digital*. Yogyakarta: UII Press, 2022.
- Budi Suhariyanto. *Cybercrime dan Pembuktian Digital*. Jakarta: Rajawali Pers, 2019.

THE POSITION OF DIGITAL FORENSICS AS EVIDENCE IN LAW ENFORCEMENT OF CRIMINAL ACTS OF COPYRIGHT INFRINGEMENT IN THE CYBER DOMAIN

Windy Anggraini et al

- Budi Suhariyanto. *Tindak Pidana Teknologi Informasi (Cybercrime)*. Jakarta: Rajawali Pers, 2019.
- Budi Suhariyanto. *Tindak Pidana Teknologi Informasi (Cybercrime)*. Jakarta: Raja Grafindo Persada, 2019.
- Budi Suhariyanto. *Tindak Pidana Teknologi Informasi (Cybercrime)*. Jakarta: RajaGrafindo Persada, 2019.
- Budi Suhariyanto. *Tindak Pidana Teknologi Informasi (Cybercrime)*. Jakarta: RajaGrafindo Persada, 2019.
- Casey, Eoghan. *Digital Evidence and ComputerCrime*. 3rd ed. Burlington: Academic Press, 2011. *Dalam Mempercepat Reformasi Peradilan*. Jakarta: Komisi Yudisial, 2007.
- Data statistic Asosiasi Penyelenggara Jasa Internet Indonesia (APJII 2020-2021).
- Eddy O.S. Hiariej. *Teori dan Hukum Pembuktian*. Jakarta: Erlangga, 2020.
- Edmon Makarim. *Forensik Digital dalam Penegakan Hukum*. Jakarta: RajaGrafindo Persada, 2021.
- Edmon Makarim. *Pengantar Hukum Telematika*. Jakarta: RajaGrafindo Persada, 2021.
- Eoghan Casey. *Digital Evidence and Computer Crime*, 4th Edition. London: Academic Press, 2020.
- Eoghan Casey. *Digital Forensics and Investigation*, 2nd Edition. London: Academic Press, 2019.
- Feri Sulianta. *Cyber Crime dan Forensik Digital*. Jakarta: Elex Media Komputindo, 2019.
- Haris Munandar dan Sally Sitanggang. *Mengenal HAKI Hak Kekayaan Intelektual: Hak Cipta, Paten, Merek, dan Seluk-beluknya* (Jakarta: Erlangga, 2008).
- Indriyanto Seno Adji. *Pembuktian dan Hukum Acara Pidana*. Jakarta: Diadit Media, 2022.
- Jimly Asshiddiqie. *Cita Negara Hukum Indonesia Kontemporer*, Papper. Disampaikan dalam Wisuda Sarjana Hukum Fakultas Hukum Universitas Sriwijaya Palembang, 23 Maret 2004 dalam Simbur Cahaya No. 25 Tahun IX Mei 2004 ISSN No. 14110-0614.
- John W Creswell. *Research Design: Qualitative & Quantitative Approach*. London: Sage, 1993.
- Johnny Ibrahim. *Teori dan Metodologi Penelitian Hukum Normatif*. Malang: Bayumedia Publishing, 2006.
- Kamus Bahasa Indonesia. Balai Pustaka: Jakarta, 2002.
- Kurniawan, Fajar. *Cyber Crime dan Penegakan Hukumnya di Indonesia*. Jakarta: Sinar Grafika, 2017
- Lilik Mulyadi. *Hukum Acara Pidana Indonesia*. Bandung: Alumni, 2020.
- M. Citra Ramadhan, Fitri Yanni Dewi Siregar, dan Bagus Firman Wibowo, *Buku Ajar Hak Kekayaan Intelektual*, Medan: Universitas Medan Area Press, 2023.
- M. Yahya Harahap. *Hukum Acara Perdata tentang Pembuktian*. Jakarta: Sinar Grafika, 2020.
- Margono Suyud dan Longginus Hadi. *Pembaharuan Perlindungan Merek*. Jakarta: Novindo Pustaka Mandiri, 2002.
- Muhammad Citra Ramadhan. *Metode Penelitian Hukum*. Yogyakarta: Kaizen Sarana Edukasi, 2021.
- Muhammad Nuh Al-Azhar. *Digital Forensic Panduan Praktis Investigasi Komputer*. Jakarta: Salemba Infotek, 2021.
- Muhammad Nuh Al-Azhar. *Digital Forensic: Practical Guidelines*. Jakarta: Salemba Humanika, 2020.
- Munir Fuady. *Teori Pembuktian (Pidana dan Perdata)*. Bandung: Citra Aditya Bakti, 2020.
- National Institute of Standards and Technology (NIST). *Guide to Integrating Forensic Techniques into Incident Response*, Special Publication 800-86, 2018.
- Paul Goldstein. *International Copyright: Principles, Law, and Practice*. Oxford: Oxford University Press, 2015.
- Peter Mahmud Marzuki. *Penelitian Hukum*, Edisi Revisi. (Jakarta: Kencana, 2010).
- Prayudi dan Yudi Prayitno Afrianto. *Digital Forensic: Teori dan Implementasi dalam Penegakan Hukum*. Yogyakarta: Andi Offset, 2007.
- R. Nugroho. *Tindak Pidana Siber dan Forensik Digital*. Yogyakarta: Graha Ilmu, 2015.
- Rachmad, Dani. *Perlindungan Hukum Hak Cipta dalam Era Digital*. Jakarta: Prenada Media, 2020.
- Raharjo. *Keamanan Sistem Informasi Berbasis Digital Forensik*. Yogyakarta: Andi Offset, 2013.
- Satjipto Raharjo. *Masalah Penegakan Hukum: Suatu Tinjauan Sosiologis*. Bandung: Sinar Biru, 2005.
- Sentosa Sembiring. *Hukum Teknologi Informasi*. Bandung: Refika Aditama, 2019.
- Sinta Dewi Rosadi. *Cyber Law: Aspek Data dan Keamanan Informasi*. Bandung: Refika Aditama, 2021.
- Sinta Dewi Rosadi. *Cyber Law: Aspek Data Pribadi dan Hak Kekayaan Intelektual*. Bandung: Refika Aditama, 2019.
- Soerjono Soekanto dan Sri Mamudji. *Penelitian Hukum Normatif: Suatu Tinjauan Singkat*. Jakarta: Rajawali Press, 2003.
- Soerjono Soekanto. *Pengantar Penelitian Hukum*. Jakarta: UI Press, 2014.
- Soerjono Soekanto. *Sosiologi Hukum dalam Masyarakat*. Rajawali: Jakarta, 1987.

THE POSITION OF DIGITAL FORENSICS AS EVIDENCE IN LAW ENFORCEMENT OF CRIMINAL ACTS OF COPYRIGHT INFRINGEMENT IN THE CYBER DOMAIN

Windy Anggraini et al

- Stephen Fishmen. *The Copyright handbook: How to Protect and Use Written Works*, dalam Eddy Damian, *Hukum Hak Cipta Menurut Beberapa konvensi Internasional, Undang-undang Hak Cipta dan Perlindungannya terhadap Buku serta Perjanjian Penerbitannya* (Bandung: PT. Alumni, 2002).
- Sudikno Mertokusumo. *Mengenal Hukum: Suatu Pengantar*. Yogyakarta: Liberty, 2003.
- Sudikno Mertokusumo. *Penemuan Hukum: Sebuah Pengantar*. Yogyakarta: Liberty, 1999.
- Sudirman Asep, Bambang Sugiantoro, Yudi Prayudi. *Kerangka Kerja Digital Forensik Readiness Pada Sebuah Organisasi*. Studi Kasus: Pt Waditra Reka Cipta Bandung, 2019.
- T.A. Yusuf. *Hukum Hak Cipta*, (Jakarta: Sinar Grafika, 2013).
- Tri Suharyanto. *Cyber Crime dan Tantangan Penegakan Hukumnya*. Jakarta: Raja Grafindo Persada, 2010.
- Utrecht. *Pengantar Hukum Administrasi Negara Indonesia*. Jakarta: Ichtiar, 1962.
- WIPO (World Intellectual Property Organization). *Understanding Intellectual Property*. Geneva: WIPO Publications, 2020.
- Yudi Kristiana. *Pembuktian Tindak Pidana Berbasis Teknologi Informasi*. Jakarta: Sinar Grafika, 2020.
- Zainuddin Ali. *Metode Penelitian Hukum*. Jakarta: Sinar Grafika, 2010.
- Jurnal**
- Agus Rahardjo. Tantangan Penegakan Hukum Hak Cipta di Era Ekonomi Digital, *Jurnal RechtsVinding*, Vol. 9 No. 2, 2020.
- Ahmad Sofian. Keterangan Ahli Forensik Digital dalam Pembuktian Tindak Pidana Siber, *Jurnal Legislasi Indonesia*, Vol. 18 No. 3, 2021.
- Aidil Wijaya Kusuma dkk. Analisis Bukti Digital Menggunakan Metode NIST, *Jurnal Cyber Security dan Forensik Digital*, Vol. 4 No. 1, 2024.
- Aidil Wijaya Kusuma dkk. Analisis Bukti Digital Menggunakan Metode NIST, *Jurnal Cyber Security dan Forensik Digital*, Vol. 4 No. 1, 2024, h. 34-36.
- Amsori. Tantangan dan Peran Digital Forensik dalam Penegakan Hukum terhadap sKejahatan di Ranah Digital, *Journal Humaniora: Jurnal Hukum dan Ilmu Sosial*, Vol. 2 No. 1, 2024.
- Anneke Mawlidya, Penerapan Digital Forensik dalam Mengidentifikasi Pelaku Penipuan dan Peran Digital Forensik sebagai Alat Bukti, *Causa: Jurnal Hukum dan Kewarganegaraan*, diakses 2025, <https://doi.org/10.6679/twqykf83>.
- Anneke Mawlidya. Penerapan Digital Forensik dalam Mengidentifikasi Pelaku dan Peran Digital Forensik sebagai Alat Bukti, *Causa: Jurnal Hukum dan Kewarganegaraan*, Vol. 3 No. 1, 2023.
- Blockchain-Based Chain of Custody in Digital Forensics: Ensuring Integrity and Legal Admissibility of Evidence*, *Forensics & Security Journal*, Vol. 1 No. 1, 2025.
- Camelia dan Eka Pratiwi, Analisis Forensik Digital dalam Mendukung Pengungkapan Tindak Kriminal Modern, *Jurnal Intelek Insan Cendikia*, 2025.
- Dewa Gede Sudika Mangku et al. *Legal Challenges of Digital Evidence in Copyright Crime Enforcement*, *Jurnal Rechtsvinding*, Vol. 12 No. 1, 2023.
- Dezfoli, Farhood Norouzizadeh, et al, *Digital Forensic Trends and Future*, *International journal of Cyber Security and Digital Forensik (IJCSDF)* 2(2). The Society of Digital Information and Wireless Communication, 2013.
- Edmon Makarim. Penegakan Hukum Hak Cipta di Era Digital dan Tantangan Koordinasi Antar Lembaga, *Jurnal Hukum & Pembangunan*, Vol. 50 No. 2, 2020.
- Faisal Syukri. Penggunaan Bukti Digital Dalam Persidangan Pidana: Antara Validitas dan Keadilan, *Causa: Jurnal Hukum dan Kewarganegaraan*, Vol. 6 No. 6, 2025.
- Handrizal, Analisis Perbandingan Toolkit Puran File Recovery, Glary Undelete dan Recuva Data Recovery untuk Digital Forensik." *J-Sakti (Jurnal Sains Komputer Dan Informatika)*. <https://doi.org/10.30654/j-sakti.v1i1.31>, 2017.
- Hartono, W. dkk. Digital Evidence and Forensic Standards in Cybercrime Investigation, *Jurnal Forensik Digital Indonesia*, Vol. 4 No. 2, 2024.
- Hendra Setiawan. Peran Open Source Intelligence dalam Penegakan Hukum Siber di Indonesia, *Jurnal Hukum dan Teknologi*, Vol. 5 No. 2, 2021.
- Herdino Fajar Gemilang. Meninjau Ilmu Digital Forensik terhadap Bukti Elektronik dalam Tindak Pidana Informasi dan Transaksi Elektronik, *Perahu: Jurnal Ilmu Hukum*, Vol. 12 No. 2, 2024.

THE POSITION OF DIGITAL FORENSICS AS EVIDENCE IN LAW ENFORCEMENT OF CRIMINAL ACTS OF COPYRIGHT INFRINGEMENT IN THE CYBER DOMAIN

Windy Anggraini et al

- Herdino Fajar Gemilang. *Meninjau Ilmu Digital Forensik terhadap Bukti Elektronik dalam Tindak Pidana Informasi dan Transaksi Elektronik*, Perahu: Jurnal Ilmu Hukum, Vol. 12 No. 2, 2024.
- Hernowo. *Penegakan Hukum dan Perlindungan Data Pribadi di Era Digital*, Jurnal Hukum dan Teknologi, Vol. 5 No. 1, 2025.
- Indra Janli Manope. *Kekuatan Alat Bukti Surat Elektronik Dalam Pemeriksaan Perkara Pidana*, Lex Cri men Vol. VI/No.2/Mar-apr/2017.
- Kusnadi. *Regulatory Gaps in Digital Forensic Utilization*, Jurnal Hukum Siber Indonesia, Vol. 3 No. 2, 2025.
- M. Citra Ramadhan, Pitra Yadi, Fitri Yanni Dewi Siregar, dan Muhammad Koginta Lubis, *Pelanggaran Hak Cipta Buku yang Diperjualbelikan Melalui E-Commerce di Kota Medan*, Acta Law Journal, Vol. 1 No. 2 (2023), <https://doi.org/10.32734/alj.v1i2.12047>.
- Mery Rohana Lisbeth Sibarani dkk. *Penerapan Konsep Pembuktian Digital dalam Kasus Kejahatan Teknologi Informasi*, Jurnal Kolaboratif Sains, Vol. 6 No. 2, 2022.
- Ni Komang Ratih Kumala Dewi. Digital Forensik Dalam Kasus Pembunuhan, <http://balipost.com/read/opini/2016/08/18/57582/digital-forensik> dalam kasus-pembunuhan.html diakses 14 November 2021.
- Nugroho. *Implementasi Sanksi Pidana dalam Perlindungan Hak Cipta*. Jurnal Hukum dan Pembangunan, 50(2), 145-158, 2020.
- Premanand Narasimhan dan N. Kala, *Ensuring the Integrity of Digital Evidence: The Role of the Chain of Custody in Digital Forensics*, International Journal of Scientific Research in Computer Science, Engineering and Information Technology, 2024.
- R. Susanto. *Digital Evidence dalam Pembuktian Pelanggaran Hak Cipta di Internet*, Jurnal RechtsVinding, Vol. 10 No. 3, 2021.
- R. Wiyono. *Kedudukan Bukti Elektronik dalam Hukum Acara Pidana*, Jurnal Legislasi Indonesia, Vol. 17 No. 3, 2020.
- Ramiyanto. *Kedudukan Alat Bukti Elektronik dalam Pembuktian Tindak Pidana Siber*, Jurnal Hukum dan Peradilan, Vol. 8 No. 2, 2019.
- Ruci Meiyanti, Ismaniah. *Perkembangan Digital Forensik Saat ini dan Mendatang*”, September 2015, Jurnal Kajian Ilmiah UBJ, Vol 15 Nomor 2.
- Satria Utam. *Peran Teknologi Informasi dalam Pembuktian Tindak Pidana Siber*, Jurnal Hukum dan Pembangunan, Vol. 49 No. 2, 2019.
- Tekayadi, dkk. *Transnational Cyber Crime and Legal Harmonization*, Jurnal Hukum Internasional Indonesia, Vol. 12 No. 2, 2025.
- Tumpal Simanjuntak. *Tantangan Pembuktian dalam Kasus Hak Cipta Digital di Indonesia*, Jurnal Hukum dan Teknologi, Vol. 4 No. 2, 2022.
- Wahyudi Agustiono dkk. *Analisis Forensik Digital Menggunakan Metode NIST untuk Memulihkan Bukti Digital yang Dihapus*, Jurnal Teknologi dan Informasi, Vol. 9 No. 1, 2025.
- Yudi Priyanti & R. Herlambang Perdana Wiratraman. *Digital Forensic Evidence and Chain of Custody in Indonesian Criminal Justice System*, Jurnal Hukum & Pembangunan, Vol. 51 No. 2, 2021.

Internet

<http://edokumen.kemenag.go.id/files/VQ2Hv7uT1339506324.pdf>, Pada 15 November 2021.

Disertasi

Yudi Prayudi et al., *Digital Evidence Cabinet sebagai Framework Chain of Custody untuk Bukti Digital*, Disertasi, Universitas Gadjah Mada, 2020.

Perundang-Undangan

Undang-Undang Republik Indonesia Nomor 28 Tahun 2014 tentang Hak Cipta.

Peraturan Mahkamah Agung Nomor 1 Tahun 2019 tentang Administrasi Perkara dan Persidangan di Pengadilan Secara Elektronik.

Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik jo. Undang-Undang Nomor 19 Tahun 2016.

Undang-Undang Nomor 19 Tahun 2016 tentang Perubahan atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik.