

Cyber Prophetic Paradigm: a Reconstruction of Criminal Law Evidencing Process Based on Digital Forensics and Transcendental Values

Kamaruddin

Universitas Muhammadiyah Kendari
kamaruddin@umkendari.ac.id

Turdialiev Mukhammad Ali Polatjon Ogli

Tashkent State University of Law

DOI: 10.23917/jtl.v7i2.14402

Submission Track:

Received:
07 December 2025

Available online:
31 January 2026

Corresponding Author:
kamaruddin@umkendari.ac.id

ABSTRACT

The objective of this research is to offer the cyber prophetic paradigm as an alternative approach in reconstructing the criminal law evidencing system in the digital era. This paradigm integrates digital forensic technologies with humanist and liberalist transcendental values to answer the limitations of the legal-formal and positivistic approaches, which are currently dominant in conventional criminal law practices.

The methodology of this research is that it uses the normative-philosophical approach with the qualitative method of analysis to literary materials on law, philosophy, and digital forensic technologies. The data is systematically analyzed using the library study method on primary and secondary data, including scientific journal articles, academic books, and related regulations.

The main findings show that digital forensics may function as an epistemological and ethical foundation in providing evidence in criminal law if guided by the principles of substantive justice and accountability, as well as the protection of constitutional rights. The cyber prophetic paradigm may form an evidencing system that is more humanist, transformative, and reflective, as well as encourage the renewal of the design of legal education and regulations that are more adaptive to challenges in the cyber era.

The implication of this research encompasses the need for a reformulation of digital evidencing regulations based on ethics and the constitution, as well as the integration of prophetic values in the curricula of legal studies, to educate law enforcers who are not only technically competent, but also have constitutional integrity and humanist sensitivity.

The novelty/originality of this research lies in its construction of the cyber prophetic paradigm as an integrative approach that has not been much developed in the literature on digital criminal law in Indonesia. This research provides theoretical and practical contributions in developing a criminal legal system that is more just, dignified, and relevant with technological advancements.

Keywords: digital forensics, substantive justice, cyber prophetic paradigm, criminal law evidencing, transcendental value.

INTRODUCTION

The advancement of technologies has brought fundamental changes to the criminal patterns and mechanisms of law enforcement, especially in the field of criminal law. Cybercrime emerges as a new form of criminality that has complex and inter-jurisdictional characteristics, exceeding the limitations of conventional law and testing the resilience of the criminal law evidencing system that is so far built upon legal-formal principles and the positivistic approach. The digital evidence produced in cybercrimes has the characteristics of fluctuating, physically invisible, and vulnerable to manipulation. Thus, there is a need for an evidencing method that is more flexible, science-based, and applies the values of ethics in the criminal justice process (Nawwar, 2025).

In this context, digital forensics emerge as a scientific instrument that functions to browse, safeguard, and evaluate electronic evidence in a methodological and structured manner. However, in the law enforcement practice in Indonesia, digital forensics is still positioned as a mere technical instrument at the investigation stage. They have not been acknowledged as an epistemological and ethical basis in the construction of the criminal evidencing system, which upholds the values of substantive justice, human dignity, and moral responsibility. This inequality is perpetuated by the normative approach that has not fully been able to address the complexity and special context of digital evidence, which risks neglecting the substantive dimension of justice and humanity values.

The escalation of cybercrimes in Indonesia is significant, especially in the forms of data hacking, electronic system manipulation, and the distribution of illegal content through digital platforms (Mursyid, Putera, & Jannah, 2025). In the last three years, the intensity of cyber crime threats has drastically increased, reaching 200%, as stated by the State Password and Cyber Agency (*Badan Siber dan Sandi Negara/BSSN*) through reports published by the Proxisis Group. The most prominent forms of attacks include phishing, malware, and ransomware, which show higher levels of complexity and organizational patterns along with the acceleration of digitalization in various sectors of life (Proxisis Group, 2025). This reality reflects that the Indonesian criminal law system is currently facing serious changes in evidencing digital-based criminal actions in a valid and just manner.

Digital forensics hold a strategic position as an evidencing instrument that may browse and authenticate digital footprints in a precise and legally valid manner. However, a

fundamental challenge being faced concerns the lack of an optimum regulatory framework as well as the limitation of institutional capacities in managing and utilizing digital evidence in an ethical, proportional, and harmonious manner that is aligned with constitutional principles (Mursyid et al., 2025). An imbalance between technical validity and the fulfillment of the substantive justice principle in the criminal court process declares the need for a reconstruction of the criminal law evidencing system that is not only technicality-based but also rooted in ethical values, respect for human rights, and moral-institutional responsibility (Amsori, Awaluddin, & Mulyana, 2024).

As stated by Mursyid et al. (2025), the position of digital forensics in the law enforcement practices in Indonesia is still limited as supporting technical instruments at the investigation stage. This instrument has not yet been fully integrated as a fundamental element in the criminal law evidencing system that is oriented towards the values of justice and ethical-constitutional principles.

The domination of the criminal law paradigm that is rooted in legal positivism, with an emphasis on formal legality and normative certainty, shows limitations in responding to the complexity of cybercrimes and the dynamic characteristic of digital evidence. This approach is still unable to guarantee substantive and constitutional justice in the criminal court process.

As a response to this complexity, the cyber prophetic paradigm is offered as an alternative approach that substantively integrates digital forensics with transcendental, humanist, and constitutional values. This paradigm aims to form a criminal law evidencing system that is more adaptive, dignified, and contextual towards the dynamics of the digital era. Digital forensics are no longer positioned as a mere technical instrument, but as an epistemological and ethical foundation in the criminal law system that guarantees substantive justice, the protection of individual rights, and the humanization of the legal process.

Using a normative-philosophical approach and a conceptual analysis, this research formulates a synthesis model that integrates technological aspects with the values of ethics and humanity. Apart from that, this research offers a strategic recommendation on regulatory renewal, institutional strengthening, and legal education transformation. The cyber prophetic paradigm emerges as a new direction in the development of the Indonesian criminal law system that is more progressive and ethics-based, with an orientation to humanism and liberal-constitutional values. The problem of this research is: How can digital forensics be

epistemologically and ethically integrated into the criminal law evidencing system in the cyber era?

RESEARCH METHOD

This research applies the normative-philosophical approach with the qualitative method of analysis, which consists of four main stages. First, the authors browse positive legal norms that regulate the evidencing process in digital-based criminal cases and acts of cybercrime. Second, the authors analyze transcendental, humanist, and liberalist values in a philosophical manner as an ethical foundation in forming a just criminal law system. Third, the authors formulate a conceptual synthesis to formulate a prophetic paradigm as a form of integration between digital forensic technological devices and the value of humanity. Fourth, the authors develop a critical argumentation of the current criminal law structure that is deemed not adaptive enough in facing the complexity of electronic evidence and has not fully guaranteed substantive justice in the criminal court process.

RESULTS AND DISCUSSION

The development of technology-based criminal actions has pushed a shift in the evidencing paradigm in criminal law, from an approach that was formerly oriented towards physical evidence and conventional methods to a digital-based system with multidimensional characteristics. Digital pieces of evidence produced from cybercrimes are complex, as they have the characteristics of easily modifiable, not directly visible, and often hidden in data structures. In facing this challenge, digital forensics has the role as a scientific instrument that allows the identification, collection, analysis, and presentation of digital evidence in a methodological and structured manner that is legally valid.

Apart from that, several previous studies have also emphasized the urgency in applying ethical and precautionary principles in the utilization of digital forensics as a legal evidencing system. Subekti (2019) states that, “The use of digital forensics in evidencing the crime of defamation through social media must pay attention to precautionary and accuracy principles, as digital evidence has the characteristics of being easy to manipulate and vulnerable.” This condition indicates that the usage of digital forensics in the criminal law evidencing system cannot solely depend on technological advancements, as it must also be harmonized with the principles of ethics and legal accountability. Therefore, the integration of digital forensics as an epistemological basis in the criminal evidencing system requires a strong scientific basis as well as ethical values that may guarantee the achievement of substantive justice.

Even though it has a strategic potential in the criminal evidencing process, in reality, the application of digital forensics in Indonesia is still limited as a supporting technical instrument and has not been fully acknowledged as an epistemological basis in the construction of the legal evidencing system (Amsori et al., 2024). This condition leads to inequality between the technical validity of digital evidence and the fulfillment of the substantive justice principle. Nawwar (2024) argues that without an adequate ethical framework and philosophical basis, the utilization of digital forensics may neglect the due process principle as well as the right to individual privacy (Nawwar, 2025).

In the global context, Alsaireh (2025) highlights that digital forensics should be seen as “a critical epistemological mechanism in the pursuit of justice in cybercrime cases,” that each stage of the digital forensic process requires scientific accuracy and commitment to the principle of ethics (Alsaireh, 2025). Mandayam (2025) also states that the treatment of electronic evidence must follow ethical standards that are aligned with the treatment to conventional evidence, especially in the aspects of the protection of privacy, valid agreements, and compliance with legal procedures.

The advancement of cyber crimes has pushed the occurrence of a shift in the criminal law evidencing system that was formerly conventional, especially in the aspects of validity, reliability, and ethical consideration in the usage of electronic evidence. Digital forensics emerge as an investigative tool that may track digital footprints in a precise manner based on scientific methodologies. However, in the field of criminal law, its existence cannot be merely reduced into supporting technologies. Digital forensics need to be positioned as an epistemological basis that determines the legal truth and likewise positioned as a normative instrument that guarantees that the evidencing process is carried out in a just manner according to the constitutional principle. Therefore, the integration of digital forensics into the cybercrime evidencing system demands a multidisciplinary approach, encompassing the technical, normative, and philosophical dimensions, in an integrated manner.

In the realm of criminal law, digital forensics cannot be merely reduced into a technical instrument to track electronic footprints, but must be positioned as an epistemological basis that determines the validity and legitimacy of evidence in the context of cybercrimes. The cyber prophetic paradigm views the forensic process as an integral part in forming the legal truth that must be based on the principles of integrity, scientific accuracy, and moral responsibility. Therefore, the digital-based criminal evidencing system needs to be guarded by transcendental

values that place honesty, sincerity, as well as respect to human dignity and honor as essential components in the implementation of a just law.

Therefore, the application of digital forensics in the cyber criminal law evidencing system should not be limited to merely the technical aspect and the legal-formal framework. There needs to be an approach based on legal philosophy and ethics to ensure that the electronic evidence not only fulfills the requirements of legal validity, but also reflects justice in the moral and constitutional sense. The cyber prophetic paradigm emerges as a transformative model which combines the scientific validity of digital forensics and transcendental values that have humanist and liberal characteristics. Not only does this approach strengthen the legitimacy of the evidencing process in the digital context, but it also encourages the reformation of the criminal law system to a more dignified direction, which orients towards substantive justice.

The increase in cybercrimes threat at a national scale indicates that the legal-formal approach that has so far dominated the criminal law system is no longer adequate. The cyber prophetic paradigm emerges as a conceptual framework which integrates digital forensic technologies and transcendental-ethical values. Data from the BSSN through Proxis Group shows that there has been a steep increase in cyber attacks of up to 200% in the last three years. This fact declares the need for a reconstruction of the criminal law evidencing system that is more adaptive to technologies, but still rooted in the principle of substantive justice and protection of constitutional rights (Proxis Group, 2025).

The currently dominant criminal law model is still rooted in legal positivism, with an emphasis on formal legality and normative certainty. In the context of cybercrimes, this approach has proven to be inadequate, as it has failed in addressing the complexity of digital evidence and the ever-changing dynamics of the cyber realm. Mursyid et al. (2025) criticize that the normative-positivistic approach tends to put aside the dimension of substantive justice in the legal evidencing process.

As a response to this limitation, the cyber prophetic paradigm is offered as a reconstruction of a more comprehensive model of the criminal law evidencing system. This paradigm is rooted in humanist-transcendental values, such as respect for human dignity, substantive justice, and legal spirituality, as well as liberalist values that encompass the protection of individual rights, liberation, and the due process principle. Apart from having a normative characteristic, this approach is also ethical and visionary. Prof. Absori states that, "It is not enough to only understand the law as norms, as it must also become an ethical energy that liberates human beings from structural injustice" (Absori, Budiono, & Bangsawan, 2023).

Further, Prof. Kelik Wardiono states that, "The reconstruction of criminal law must depart from the values of substantive justice rather than mere certainty of the formal law," (Absori, Wardiono, & Yuspin, 2021). Next, Prof. Dimiyati emphasizes that "Justice is not merely a result of legal procedures, but rather a value that must be internalized in every legal process" (Erwin, 2013; Huda & Dimiyati, 2018). The cyber prophetic paradigm uses these values as a foundation in designing a criminal law evidencing system that is more humanist and constitutional, that liberates people from structural inequality.

The main challenge in the application of digital forensics is not only placed in its technological aspect, but also from the readiness of the legal system to adopt an ethical and multidisciplinary approach in addressing digital evidence. Soni (2025) highlights that the ethical approach is the key in guaranteeing the substantive validity of digital evidence. In the Indonesian context, Amsori, Awaluddin, and Mulyana (2024) emphasize the importance of developing a criminal law system that not only enforces the law, but also comprehensively humanizes the legal process.

The cyber prophetic paradigm views that justice is no longer mere compliance of formal legal norms, but is a substantial value that must be manifested through an evidencing process that is just and transparent, which orients towards the protection of constitutional rights. Digital evidence used in court processes must be examined not only based on procedural legality, but also based on ethical considerations that uphold spiritual values, such as social responsibility, purity of intention, and respect for individual rights. Therefore, the criminal law evidencing system in the digital era must transform into a mechanism that guarantees holistic substantive justice.

The validation of digital evidence in the cyber criminal law system requires an ethical approach that is not only based on technical and legal standards, but is also aligned with prophetic principles sourced from transcendental values. The cyber prophetic paradigm emphasizes that every evidencing process must start with pure intentions, accountable methods, and the aim of justice. In this case, prophetic ethics function as a moral guide, so that digital technologies do not become tools of domination, but rather become facilities to recover justice and protect human rights.

Therefore, the cyber prophetic paradigm functions as a conceptual bridge between technological advancements and transcendental ethical values in the criminal law system. Not only does this approach offer a model with transformative, humanist, and constitutional

characteristics, but this paradigm also allows the criminal law evidencing system to maneuver beyond the orientation of formal legality to a structure that guarantees substantive justice, the protection of constitutional rights, and the respect for human dignity. By integrating digital forensics as an epistemic and ethical instrument, the cyber prophetic paradigm reconstructs the criminal law, making it take the side of humanity values, and become more adaptive and meaningful.

Not only does the cyber prophetic paradigm function as a theoretical basis in the evidencing process in criminal law, but it also brings practical impacts to regulatory reformation and the development of the curricula of legal studies. From the regulative aspect, this approach encourages the formation of legal norms that are more adaptive towards the special characteristics of digital evidence and the dynamics of cyber crimes. Therefore, the regulations on criminal evidencing needs to determine formal acknowledgement of digital evidence as a valid legal object, as well as formulate clear ethical and procedural in applying digital forensics. This idea is in line with the perspective of Alvin Danu Prananta (2017), who states that, "The urgency of digital forensics is placed in its capability to accurately uncover the flow of electronic transactions, but it must be balanced with regulations that guarantee its valid and ethical use," (Prananta, 2017).

On the one hand, this paradigm encourages the need for a transformation in the legal education sector. The legal curriculum must be designed to combine the understanding of digital literacy, the principles of ethics in forensic practices, as well as transcendental values with humanist and liberalist characteristics as important elements in forming the integrity and character of prospecting law enforcers in the future. Widiwati (2019) states that, "The human rights protection in the digital criminal law process must be guaranteed by a legal approach that is not only normative, but also humanist and constitutional." However, on the other hand, this statement declares the importance of the reformation of the legal education that is not merely focused on the legal-formal aspect, but also emphasizes the formation of an ethical awareness and profound constitutional understanding.

The cyber prophetic paradigm also obliges the existence of an institutional transformation in the law enforcement system. Institutions, such as the police force, the attorney, and courts, need to be completed with digital forensic units that not only have technical competencies, but also have a deep understanding of the principles of ethics, human rights, and substantive justice. This step is crucial so that the evidencing process does not evolve into tools of oppression, but rather as legal instruments that highly uphold dignity and liberation values. As argued by Rasyid (2022), "An ethical law enforcement is law enforcement that humanizes

people, rather than merely punishing them.” In this framework, the cyber prophetic paradigm has the role of a bridge between technological advancements and the principles of ethics that need to be profoundly integrated into the criminal law system. Thus, the reformation of legal regulations and education cannot only be surface-level, as it must touch paradigmatic changes that are both fundamental and transformative.

Analytical findings show that digital forensics have a significant capacity in strengthening the evidencing mechanism in criminal law, especially in cyber cases that involve electronic evidence. Even so, the level of effectiveness is highly determined by the existence of regulations that govern the aspects of validity, administration, and ethics in the usage of digital evidence. In research studies conducted by Anggraeni and Salsabila (2025), it was stated that digital forensics must be able to ensure the validity of evidence in the face of a court through procedures that highly uphold the principles of transparency and accountability.

Further, regulatory renewal efforts cannot be separated from the reformation process in legal education. The legal curriculum in Indonesia needs to be developed in a more comprehensive manner by inserting digital literacy elements, the principle of ethics in forensic practices, as well as prophetic values as an integral part of forming the competency of legal study graduates in facing the complexity of cybercrimes. As explained in the Media Mahasiswa Indonesia (Indonesian College Student Media), not only do cybercrimes require a quick legal response, they also require an approach that is based on ethical values and normative awareness (Media Mahasiswa Indonesia, 2025). In this context, the cyber prophetic paradigm has the role as a connector between technological advancement and the humanity value in the criminal law evidencing system.

Therefore, this cyber prophetic paradigm has a significant transformative power in pushing the renewal of the criminal law system, both in the regulatory and education dimensions. At the regulative aspect, this approach encourages the emergence of legal norms that can accommodate the special characteristics of digital evidence and also guarantee the validity and ethical application of the criminal court process. The regulations formulated through this framework must be able to accurately respond to technological challenges without neglecting the principles of substantive justice and the protection of constitutional rights.

On the other hand, in the scope of legal education, the cyber prophetic paradigm opens room for the development of an integrative curriculum. This curriculum needs to contain digital literacy, the principle of ethics in forensic practices, as well as transcendental values that are

humanist and liberalist. This is part of the process to form the character of prospective law enforcers. It is not enough for legal education in the digital era to only give technical skills, as it must also instill ethical awareness and constitutional responsibility, so that graduates may be able to face the complexity of cybercrimes in a comprehensive and dignified manner.

Thus, the cyber prophetic paradigm is proven to bring a transformative contribution to the renewal of the criminal law system in the digital era, especially in the legal education and regulatory aspects. By making digital forensics an epistemological and ethical foundation, this paradigm encourages the birth of regulations that are responsive towards technological development, as well as guarantee substantive justice and the protection of constitutional rights. At the same time, this paradigm also demands the reformation of the legal studies curriculum, so that it may encompass digital literacy, forensic ethics, and humanist-liberalist transcendental values, to create law enforcers with high levels of ethical integrity and constitutional awareness.

CONCLUSION

Digital forensics has the potential to become an epistemological and ethical foundation in the criminal law evidencing system in the cyber era if it is understood not merely as a technical instrument, but rather as a scientific instrument that upholds substantive justice and the protection of constitutional rights. This potential is strengthened by the cyber prophetic paradigm that integrates technologies in humanist transcendental values, thus exceeding the limitations of the legal-formal paradigm and encourages a more just and reflective criminal law system. This transformation encourages regulatory renewal, strict ethical standards, and the reformation of legal education with digital literacy and forensic ethics to create law enforcers who are superior in technicality as well as have constitutional integrity and humanist sensitivity. Therefore, the integration of digital forensics as an epistemological and ethical foundation in the criminal law evidencing system in the cyber era finds its form in the transformative cyber prophetic paradigm.

REFERENCES

- Absori, Budiono, A., & Bangsawan, M. I. (2023). *Hukum Lingkungan Dimensi Etik Profetik (Environmental Law Dimensions of Prophetic Ethics)*. Surakarta: Muhammadiyah University Press.
- Absori, Wardiono, K., & Yuspin, W. (2021). *Kebijakan Reformasi Sumber Daya Alam Bidang Pertanahan Berbasis Kesejahteraan Perspektif Maqasid al-Syari'ah Asy-Syatibi*. Surakarta: MUP. Retrieved from <https://bacabuku.com/detail/politik-hukum-sumber-daya-alam-bidang-pertanahan-berbasis-kesejahteraan-perspektif-maqashid-al-syari/89810>
- Alsaraireh, N. (2025). Digital Forensics in the Age of Cybercrime: Challenges and Future

- Directions. In *Tech Fusion in Business and Society*. Berlin: Springer. Retrieved from https://link.springer.com/chapter/10.1007/978-3-031-84636-6_48
- Amsori, Awaluddin, F., & Mulyana, M. (2024). Challenges and Role of Digital Forensics in Law Enforcement against Crime in the Digital Realm. *Journal Humaniora*, 2(1). <https://doi.org/10.37010/hmr.v2i1.35>
- Anggraeni, D. R., & Salsabila, M. (2025). Analisis Yuridis Peran Digital Forensik Dalam Pembuktian Tindak Pidana di Indonesia. *Jurnal MHI*, 2(2). Retrieved from <https://ojs.daarulhuda.or.id/index.php/MHI/article/download/580/601>
- Erwin, M. (2013). *Filsafat Hukum: Refleksi Kritis terhadap Hukum dan Keadilan*. Jakarta: Raja Grafindo Persada. Retrieved from <https://library.stik-ptik.ac.id/detail?id=50031&lokasi=lokal>
- Huda, N., & Dimiyati, K. (2018). Base Transcendental Value on Judge's Decision (Study of Basic Perspective of Pancasila State). *Jurnal Dinamika Hukum*, 18(2), 139. <https://doi.org/10.20884/1.jdh.2018.18.2.2076>
- Mandayam, R. (2025). Ethical Considerations in Digital Forensic. *International Journal of Innovative Research in Multidisciplinary and Physical Sciences*, 13(1). <https://doi.org/10.37082/IJIRMP.S.v13.i1.231831>
- Media Mahasiswa Indonesia. (2025). Pembaharuan Hukum Forensik Digital dalam Pembuktian Tindak Pidana Kejahatan Siber. Retrieved from MMI website: 24 October 2025
- Mursyid, Putera, A., & Jannah, M. (2025). Rekonstruksi Peran Digital Forensik Dalam Penyidikan Tindak Pidana Siber: Analisis Kritis Terhadap Konstruksi Hukum Pidana di Indonesia. *Jurnal Tana Mana*, 6(2). Retrieved from <https://ojs.staialfurqan.ac.id/jtm/article/view/1194>
- Nawwar, A. (2025). *Analisis Forensik Digital pada Bukti Digital Kejahatan Siber Menggunakan Digital Forensic Research Workshop Model* (UIN Syarif Hidayatullah Jakarta). UIN Syarif Hidayatullah Jakarta. Retrieved from <https://repository.uinjkt.ac.id/dspace/handle/123456789/83810>
- Prananta, A. D. (2017). *Urgensi Forensik Digital dalam Proses Pembuktian Tindak Pidana Pencucian Uang pada Tingkat Penyidikan* (Universitas Gadjah Mada). Universitas Gadjah Mada. Retrieved from <https://etd.repository.ugm.ac.id/penelitian/detail/224710>
- Proxis Group. (2025). Tren Ancaman Siber di Indonesia Meningkat? Berikut Fakta yang Harus Diketahui. Retrieved October 25, 2025, from Proxis Group Website website: <https://it.proxisgroup.com/tren-ancaman-siber-di-indonesia-meningkat-berikut-fakta-yang-harus-diketahui/>
- Rasyid, H. Al. (2022). *Etika dan Moralitas dalam Penegakan Hukum*. Jakarta: Sinar Grafika.
- Soni, N. (2025). Digital Forensics: Confronting Modern Cyber Crimes, Technological Advancements, and Future Challenges. *Journal of Forensic, Legal & Investigative Sciences*, 11, 105. Retrieved from https://www.heraldopenaccess.us/article_pdf/34/digital-forensics-confronting-modern-cyber-crimes-technological-advancements-and-future-challenges.pdf
- Subekti, A. S. (2019). *Penggunaan Digital Forensik Dalam Pembuktian Tindak Pidana Pencemaran Nama Baik Melalui Media Sosial* (Universitas Airlangga). Universitas Airlangga. Retrieved from <https://repository.unair.ac.id/97887/>
- Widiwati, A. (2019). *Tindak Pidana Pengedaran Narkotika Melalui Media Elektronik dalam Perspektif Hukum Islam dan Hukum Positif* (UIN Syarif Hidayatullah Jakarta). UIN Syarif Hidayatullah Jakarta. Retrieved from https://repository.uinjkt.ac.id/dspace/bitstream/123456789/50247/1/AYU_WIDIWATI-FSH.pdf