ISSN 2808-4314

Evidentiary Value of Internet Protocol Address Similarity in Tender Collusion: a Study of Case No. 445 K/PDT.SUS-KPPU/2021

Raissa Sundari[1], Rismawati[2]
[1,2]Fakultas Hukum, Universitas Syiah Kuala, Jl. Teuku Nyak Arif No. 441, Banda Aceh, Aceh, 2311 Indonesia
Email: sundariraissa@gmail.com, rismawati_fh@usk.ac.id

Background: Collusion in electronic tenders represents a fundamental violation of fair competition principles, as it systematically undermines the transparency, fairness, and efficiency of government procurement processes, prompting the adoption of the e-tender system to safeguard integrity. Objectives: This study aims to critically assess the legal validity and probative strength of IP addresses as electronic evidence in digital collusion cases, while specifically examining the judicial reasoning applied in relevant Indonesian court decisions. Methods: Employing a normative legal methodology with a descriptive-analytical approach, this research draws upon diverse legal literature, statutes, and comparative case studies. Results: The analysis establishes that while Article 5 of Indonesia's ITE Law formally recognizes IP addresses as valid electronic evidence due to their unique device-identifying function, the ruling in Decision Number 445 K/Pdt.Sus-KPPU/2021 is jurisprudentially flawed; the court erroneously limited the comparison of IP addresses to a superficial administrative verification by the procurement working group (pokja), despite the pokja lacking statutory access to the SPSE system. In contrast, international jurisdictions such as Brazil, Singapore, and China robustly admit IP addresses as compelling evidence when corroborated by metadata and system logs. Conclusions: Consequently, this study underscores the urgent necessity for Indonesia to establish consistent, technology-adaptive, and procedurally clear standards for electronic evidence to ensure legal certainty and reinforce the effective enforcement of fair competition law in the digital procurement landscape.
Keywords: Digital collusion evidence, electronic evidence law, IP Address geolocation.

Corresponding Author:
Raissa Sundari
Fakultas Hukum, Universitas Syiah Kuala, Jl. Teuku Nyak Arif No. 441, Banda Aceh, Aceh, 2311 Indonesia
sundariraissa@gmail.com

1. Introduction

The government procurement process for goods or services has been conducted electronically in accordance with Presidential Regulation No. 54 of 2010, as amended by Presidential Regulation No. 12 of 2021. However, in practice, the public procurement sector is vulnerable to tender collusion, namely closed cooperation to manipulate auction results in violation of the law as prohibited by Article 22 of Law No. 5 of 1999 on Business Competition [1]. The government implements an electronic procurement system through the Electronic Procurement Agency (LPSE) in accordance with Presidential Regulation No. 16 of 2018 to create a method that upholds the principles of openness and accountability [1]. This aims to reduce the practice of abuse of authority, collusion, and favoritism through the electronic documentation of all transaction activities to ensure transparency and public accountability.

Digital records, including Internet Protocol Addresses (IP Addresses), are used by the Business Competition Supervisory Commission (KPPU) as preliminary indicators of suspected tender collusion. Based on the Electronics Information and Transactions Law (UU ITE) and Article 42 of Law on Business Competition, IP Addresses are recognized as valid evidence [2]. However, in Landmark Decision MA Number 445K/Pdt.Sus-KPPU/2021, hereinafter referred to as Supreme Court Decision 445/2021, the Court assessed that the similarity of IP addresses was only part of the verification process by the working

group (Pokja) and did not have sufficient probative value, differing from the KPPU's interpretation that it was evidence of coordination, thus creating legal uncertainty in the assessment of digital evidence.

Supreme Court Decision 445/2021 shows a different direction from previous decisions such as Landmark Decision No. 154K/Pdt.Sus-KPPU/2015, 917K/Pdt.Sus-KPPU/2016, 5K/Pdt.Sus-KPPU/2019, 339K/Pdt.Sus -KPPU/2021, which essentially recognize the similarity of IP addresses and metadata as strong evidence of tender collusion. The core research gap lies in the fundamental doctrinal divergence between these rulings: while the earlier jurisprudence (e.g., Decisions 154/2015, 917/2016, 5/2019, and 339/2021) consistently treated identical IP addresses and matching metadata timestamps as prima facie corroborating evidence—effectively shifting the burden of proof to the defendants to disprove coordination—Decision 445/2021 drastically breaks from this established trajectory by recharacterizing IP address similarity as merely a pre-award administrative verification task reserved for the Pokja, despite the Pokja lacking statutory access to the SPSE system to conduct such verification. This judicial departure does not merely differ in degree but in kind: it substantively nullifies the probative value of digital evidence that the KPPU and lower courts had previously relied upon, creating a direct contradiction with Article 5 of the ITE Law, which explicitly acknowledges IP addresses as valid electronic evidence. This inconsistency underscores the importance of establishing clear digital evidence standards as has been implemented in a number of jurisdictions such as Brazil, Singapore, and China [3]. Unlike these comparative jurisdictions, which have progressively adopted harmonized evidentiary frameworks that integrate IP metadata and system logs cohesively, Indonesia currently suffers from a judicial schism where the evidentiary weight of identical digital traces depends entirely on which panel of justices hears the case, leaving the standard of proof for electronic collusion highly unpredictable and fragmented.

Therefore, a legal-normative analysis of Supreme Court Decision 445/2021 is needed, using Aristotle's theory of justice and legal certainty to formulate a proportional basis for assessing IP addresses as a credible electronic verification tool equivalent to conventional evidence in business competition cases, by examining how the judges considered the similarity of IP addresses as evidence in the decision and to what extent this assessment affects legal certainty and justice for business actors.

2. Literature Review And Problem Statement

The evidentiary value of digital traces in competition law cases has garnered increasing scholarly attention as procurement systems migrate online. Internet Protocol (IP) addresses, functioning as unique identifiers for devices accessing network resources, occupy a contested position within electronic evidence frameworks (Mason, 2016). In Indonesia, Article 5(1) of Law No. 11 of 2008 concerning Electronic Information and Transactions (ITE Law) accords electronic information and documents the status of legally admissible evidence, yet the operationalization of this provision in tender collusion cases remains inconsistent [4]. Prior jurisprudence, including Supreme Court Decision No. 5 K/Pdt.Sus-KPPU/2019, recognized IP address similarity as corroborative evidence of coordination among tender participants when combined with metadata anomalies and document irregularities [5]. However, technical limitations inherent to IP evidence particularly dynamic addressing via DHCP and NAT configurationsnecessitate caution in assigning probative weight absent supporting digital forensic analysis [6].

The legal problem emerging from existing literature is twofold. First, Indonesian courts have demonstrated divergent approaches to assessing IP address evidence, with Decision No. 445 K/Pdt.Sus-KPPU/2021 rejecting its probative value while earlier decisions accepted it as circumstantial evidence of collusion. This judicial fragmentation undermines legal certainty for business actors participating in electronic tenders [7]. Second, there exists a conceptual gap between technological understandings of IP address functionality

and judicial interpretations thereof, particularly regarding whether IP similarity indicates participant coordination or merely reflects routine network administration . Comparative jurisdictions Brazil, Singapore, and China (Cybersecurity Law, 2017) have established statutory log retention obligations and presumptive authenticity frameworks for digital evidence, thereby providing coherent standards that Indonesian competition law currently lacks [8]. Accordingly, this study investigates how Supreme Court Decision 445/2021 assessed IP address similarity as evidence and evaluates the implications of this assessment for legal certainty and justice in business competition cases.

3. Method

The research approach employed in this study is normative, as the underlying issue is driven by the unavailability and lack of clarity of norms concerning the use of IP addresses as evidence in procurement collusion cases. This normative character is essential because positive legal provisions in Indonesia do not explicitly regulate the evidentiary weight of digital network artifacts like IP addresses [9]. The ambiguity is particularly evident in the contradictory outcomes between Supreme Court Decision No. 445 K/Pdt.Sus-KPPU/2021 and earlier jurisprudence that recognized IP address similarity as corroborative evidence. The rationale for selecting this normative-doctrinal method over an empirical-sociological one is rooted in the nature of the research problem: the central issue is not a factual deviation in societal behavior that requires field observation or interviews, but rather a structural and doctrinal inconsistency within the judicial hierarchy itself. Resolving this doctrinal fragmentation necessitates an internal legal examination of statutory texts, judicial reasoning, and hierarchical norm-conformity. This methodological choice is directly relevant to the research objectives because it specifically enables the study to: (a) deconstruct the judges' legal considerations (ratio decidendi) in Decision 445/2021, (b) measure these considerations against the higher statutory hierarchy particularly Article 5 of the ITE Law and Article 42 of the Business Competition Law and (c) evaluate whether the decision aligns with the overarching principles of legal certainty and substantive justice. Without this normative approach, the study would lack the doctrinal toolkit required to critically assess the probative strength of IP addresses and formulate a proportional legal standard for their admissibility, which are the core objectives of this research. To resolve this normative deficit, the study does not merely describe existing laws but instead evaluates them against higher legal principles. Specifically, the research looks at the big picture in terms of legal principles such as legal certainty, substantive justice, and the principle of fair business competition. Furthermore, the study compares what is happening in many other countries, including Brazil, Singapore, and China, which have established statutory frameworks for digital evidence. This comparative dimension allows the research to identify best practices and potential models for Indonesian legal reform. By integrating doctrinal analysis with comparative law, the normative approach transcends simple black-letter interpretation. Consequently, the methodology is designed to produce recommendations that address both the lacunae in current regulations and the inconsistencies in judicial application.

In implementing this normative approach, the study collected legal sources by exploring the literature using a case approach that focused on a comprehensive review of relevant laws, jurisprudence, and scientific articles. The statutory materials examined included Indonesia's Business Competition Law (Law No. 5 of 1999), the Electronic Information and Transactions Law (ITE Law), and Presidential Regulations governing electronic procurement [10]. The jurisprudence review centered on Supreme Court decisions concerning tender collusion, with special emphasis on Decision No. 445/2021 and earlier contrasting rulings such as Decision No. 5 K/Pdt.Sus-KPPU/2019. Scientific articles and scholarly commentaries from both Indonesian and international sources were incorporated to understand evolving doctrines on electronic evidence admissibility. All collected materials were examined qualitatively, meaning the analysis

focused on meaning, interpretation, and logical coherence rather than statistical measurement. This qualitative examination proceeded through a step-by-step process that included inventorying legal sources, reducing data to relevant portions, categorizing information by legal issues, and interpreting findings in light of legal principles. Each step was designed to ensure transparency and replicability in the analytical process. To ensure transparency, rigor, and replicability, the data analysis followed a strictly operationalized five-stage procedure: (1) Systematic Inventory and Source Triangulation all primary legal materials (statutes, regulations, and jurisprudence) and secondary materials (scholarly articles and comparative legal documents) were catalogued chronologically and cross-verified across different legal hierarchies to confirm their authenticity, official status, and direct relevance to the research questions; (2) Doctrinal Reduction and Issue-Coding the collected data were segmented and coded into specific thematic clusters using a pre-defined analytical matrix derived directly from the research objectives, namely: (a) the normative validity of IP addresses as electronic evidence under Indonesian law, (b) the procedural authority of the Pokja versus the KPPU in verifying digital traces, (c) the evolution of judicial reasoning across contrasting Supreme Court decisions, and (d) the evidentiary standards adopted in comparative jurisdictions; (3) Multi-Lens Interpretive Assessment the coded data were systematically interpreted using three distinct but complementary hermeneutic techniques: first, grammatical interpretation to parse the literal and textual meaning of Article 5 of the ITE Law and Article 42 of the Business Competition Law; second, teleological interpretation to ascertain the underlying legislative intent and purposive rationale behind the recognition of electronic evidence; and third, comparative-contrastive analysis to juxtapose the Indonesian judicial approach against the statutory and case-law frameworks of Brazil, Singapore, and China; (4) Synthetic Argumentation and Normative Evaluation the findings from the interpretive stage were systematically collated and weighed against the higher benchmarks of legal certainty and Aristotle's theory of justice, allowing the study to construct a coherent legal critique of Decision 445/2021 and to identify the specific doctrinal gaps that require reform; and (5) Audit Trail Documentation every interpretive choice, analytical judgment, and conclusion drawn throughout the process was recorded in a detailed audit trail, documenting the reasoning behind each step to ensure that the analytical pathway is fully transparent, independently verifiable, and replicable by other legal scholars. Each step was designed to ensure transparency and replicability in the analytical process. The purpose of this systematic procedure was to provide a complete picture of the issue, encompassing technical, legal, and institutional dimensions. Ultimately, the step-by-step qualitative method produced strong and reasoned conclusions capable of supporting structured recommendations for judicial standardization, legislative amendments, and institutional capacity building.

4. Results And Discussion

The Position of IP Addresses in Indonesian Law

The principle of fair business competition is a conditio sine qua non in a market economy system and is explicitly protected by Article 22 of the Law on Business Competition. Collusive practices in the procurement process are classified as per se illegal, and are therefore considered unlawful without the need to prove any consequences. The implementation of e-procurement through SPSE aims to improve accountability, but it also opens up opportunities for collusion with digital traces being used as key evidence by the KPPU. Decision of Mahkamah Agung No. 445/2021 has created a contradiction in competition law by rejecting IP addresses as evidence on the grounds that they are technically weak. This consideration differs from previous decisions, such as Supreme Court Decision No. 5K/Pdt.Sus-KPPU/2019, which recognized IP addresses as evidence supporting the existence of collusion [11].

This inconsistency undermines legal certainty and reflects differences in legal approaches to digital

forensic evidence. IP addresses, as a form of network forensic evidence, have important probative value for tracing access patterns, communication channels, and the timing of digital activities related to electronic tendering cases. IP addresses are included in the category of digital information according to the provisions of Article 1 paragraph (1) of the ITE Law and are considered legitimate evidence because Article 5 paragraph (1) of the ITE Law states that digital evidence is recognized as having evidentiary value equivalent to physical documentary evidence. Similarities in public IP addresses between tender participants within a similar time frame can be interpreted as prima facie (initial indication) of coordination or shared network usage that could potentially violate the confidentiality of bids. However, as network forensic evidence, IP addresses are not absolute due to technical factors including the use of dynamic configuration protocols or Dynamic Host Configuration Protocol (DHCP) and Network Address Translation (NAT), which can cause IP sharing. Therefore, the application of the principle of corroboration is important, requiring at least two additional pieces of digital or textual evidence, such as metadata, identical typing errors, or pricing patterns.

Basis for the Supreme Court's Decision

Decision of Mahkamah Agung Number 445/2021 stated that the case originated from the selection process for a contractor to improve and maintain roads in the Aceh Barus Simbolga section in the 2018 fiscal year. Decision No. 23/KPPU-L/2018, hereinafter referred to as the KPPU decision, stated that the three tender participants, namely PT Swakarsa Tunggal Mandiri (STM), PT Sekawan Jaya Bersama (SJB), and PT Fifo Pusaka Abadi (FPA), were found guilty of engaging in illegal coordination during the procurement process. This action is classified as bid rigging, which is contrary to the requirements of Article 22 of the Law on Business Competition. Based on its conclusions regarding the similarity of IP addresses, the similarity of document metadata, and the identity of typing errors that indicate coordination between participants, the KPPU requested the court to review the decision [12]. Decision 692/Pdt.Sus-KPPU/2019/PN Mdn, hereinafter referred to as the Medan District Court Decision, overturned the KPPU's decision because the similarity of IP addresses was deemed insufficient to prove collusion and was the responsibility of the tender working group. At the Cassation level, the KPPU was rejected by the Supreme Court in Supreme Court Decision 445/2021, which confirmed that IP address similarities only have limited evidentiary value due to technical factors such as DHCP. The Court ruled that responsibility for data entry errors lies with the working group, in line with Article 13 Paragraph (1) of Presidential Regulation No. 16 of 2018, and therefore cannot be attributed to tender participants.

Analysis of the Supreme Court's Ratio Decidendi

In its ruling, the KPPU established a solid pattern of evidence by combining a number of pieces of indirect evidence as a basis for assessing the potential for coordination between tender participants. In line with the 2024 OECD guidelines, the evidence found includes similarities in IP addresses, close timestamps, metadata of documents with similar types (Pdf Version 1.3 Acrobat 4.x), and identical typing errors in the documents of the reported parties. These similarities indicate a systematic pattern of cooperation constituting bid rigging, as seen in the documents of PT Swakarsa Tunggal Mandiri and PT Fifo Pusaka Abadi, including spelling errors such as “Memerus” (Menerus), “Faraksi” (Fraksi), dan “anti striping agent” (anti stripping agent) as stated in the KPPU Decision. The error stems from the Supreme Court's decision to treat IP addresses, which are network forensics, as part of metadata or file system forensics . This misinterpretation by the judge illustrates the limited understanding of digital forensics at the judex juris level, which fundamentally hinders the process of analyzing the evidentiary value of digital evidence.

Table 2: Conceptual Errors in Digital Forensics in Supreme Court Decision 445 K/Pdt.Sus-KPPU/2021

Forensic Dimensions	IP Address (Network Forensics)	Metadata File (File System Forensics)	Judicial Error
Primary Function	Tracking Access Path (Network Path), Connection Time (Timestamp).	Recording Intrinsic Document Characteristics (Author, Software, PDF Version).	The judge incorrectly interpreted the IP address as part of the file metadata.
Probative Value	Indications of the same access location and time coordination.	Evidence of document duplication and use of the same work source	Ignoring cumulative scores, assessing GPAs solely as an administrative matter Working Group

Source:(Yuancheng Xie dkk., 2025)

Table 2 provides a systematic critique of the Supreme Court's analytical framework in Decision No. 445/2021 by exposing a fundamental category error in how the Court distinguished between different types of digital evidence. The table separates forensic dimensions into two distinct domains: network forensics, which governs Internet Protocol (IP) addresses, and file system forensics, which governs metadata embedded within documents. This distinction is not merely technical jargon but represents a foundational principle in digital forensic science. Network forensics concerns itself with the movement of data across networks—tracking access paths, recording connection timestamps, and identifying communication patterns between devices. File system forensics, conversely, examines static characteristics of stored files, such as author identities, software versions, and editing histories. The Supreme Court's error, as the table demonstrates, lay in conflating these two separate forensic categories, treating an IP address as if it were a type of file metadata subject to the same verification standards.

According to the table, the primary function of an IP address within network forensics is to track access paths (network routes) and connection timestamps. Unlike file metadata, which resides within the document itself and can be altered after creation, an IP address reflects real-time network behavior at the moment of access. When a tender participant logs into an electronic procurement system (SPSE), the system assigns or records the public IP address from which the connection originates. This address serves as a digital footprint that can be correlated across multiple users and time periods. In the context of bid rigging investigations, IP address similarity between competing tender participants—particularly when connections occur within minutes of each other—provides a factual basis for inferring that the participants accessed the system from the same network location, potentially indicating coordination. This inferential chain is fundamentally different from file metadata analysis, which might show that two documents were created using the same software or by the same author.

In contrast, the table identifies the primary function of file metadata as recording intrinsic document characteristics, including author names, editing software, PDF version numbers, and creation or modification timestamps. File system forensics examines these attributes to detect patterns suggesting common origin or unauthorized copying. For example, when two supposedly independent tender submissions contain PDF files saved with the same version of Adobe Acrobat (e.g., PDF Version 1.3, Acrobat 4.x), or when both documents exhibit identical typing errors such as "Memerus" instead of "Menerus" or "Faraksi" instead of "Fraksi," forensic analysts infer that the documents likely originated from a single source. This evidence supports claims of document duplication and shared work product. However, crucially, file metadata tells investigators nothing about network access patterns or whether the uploaders were physically or virtually co-located at the time of submission. The two forensic domains address distinct questions and must be evaluated under distinct frameworks.

The table's third column specifies the judicial error: the Supreme Court judge incorrectly interpreted the IP address as part of the file metadata. This conceptual mistake is not a minor technical oversight but a jurisdictional error that fundamentally undermined the evidentiary analysis. By treating IP addresses as metadata, the Court applied verification standards appropriate to file system forensics—standards that focus on document integrity and authorship—to a network forensic artifact that requires different authentication methods. IP addresses cannot be verified by examining document properties or checking for editing traces; they must be verified through system logs, ISP records, and network infrastructure audits. The Court's failure to recognize this distinction led it to conclude that IP evidence was inherently weak because it could not be authenticated through the same mechanisms as metadata. In reality, IP evidence requires different, not weaker, authentication procedures, but those procedures were never invoked because the Court mischaracterized the nature of the evidence from the outset.

The table further compares probative values across forensic dimensions. For IP addresses under network forensics, the probative value lies in providing indications of the same access location and time coordination among multiple tender participants. When PT Swakarsa Tunggal Mandiri, PT Sekawan Jaya Bersama, and PT Fifo Pusaka Abadi all accessed the SPSE system from identical IP addresses within a narrow temporal window, the natural inference—absent countervailing explanation—is that these participants were either using the same physical device, the same network gateway, or coordinating their login activities. This inference gains additional weight when combined with other circumstantial evidence such as identical document errors and pricing patterns. However, the Supreme Court disregarded this cumulative probative value, instead assessing IP addresses in isolation as if they were merely administrative data within the Working Group's purview. The table notes this as "ignoring cumulative scores, assessing GPAs solely as an administrative matter Working Group," meaning the Court reduced complex forensic indicators to a simple administrative checklist.

For file metadata under file system forensics, the table identifies probative value as evidence of document duplication and use of the same work source. When multiple tender submissions contain identical PDF version numbers, identical author names in document properties, or identical unusual spelling errors, the inference of common authorship becomes compelling. In the underlying KPPU decision, investigators found that PT STM and PT FPA submitted documents containing the same three distinctive typographical errors: "Memerus" (correct spelling "Menerus"), "Faraksi" (correct spelling "Fraksi"), and "anti striping agent" (correct spelling "anti stripping agent"). These errors were not common grammatical mistakes but highly specific anomalies unlikely to occur independently. The probative value of such metadata is strong because it directly points to shared document preparation. However, the Supreme Court erroneously treated IP address similarity as if it belonged to this category, then dismissed it because the Working Group had not verified the metadata, when in fact IP addresses require a completely different verification chain.

The accompanying text reveals a second critical error: the Supreme Court assigned the task of digital trace extraction and verification to the procurement Working Group (Pokja). This assignment is legally and practically problematic. Under Article 13 paragraph (1) of Presidential Regulation Number 16 of 2018 concerning Government Procurement of Goods/Services, the Working Group's responsibilities are limited to administrative functions such as evaluating bid documents, verifying bidder qualifications, and ensuring compliance with tender requirements. The Working Group has no statutory authority to access system logs, conduct forensic analysis of IP address records, or perform network authentication. Moreover, the Working Group lacks technical training in digital forensics and does not maintain chain-of-custody protocols for electronic evidence. By shifting responsibility to an entity without legal mandate or technical capacity, the Supreme Court effectively ensured that no meaningful verification of IP evidence would

occur, then cited the absence of verification as grounds for rejecting the evidence.

The text further notes that in April 2021, when the relevant tender occurred, the SPSE (Electronic Procurement System) version 4.3 did not yet have a feature to record IP addresses. This factual assertion requires careful scrutiny. If the system did not record IP addresses at all, then any claim of IP address similarity would be based on incomplete or non-existent data. However, the KPPU's original decision relied on IP address data that was allegedly extracted from system logs. The Supreme Court appears to have accepted the argument that because the SPSE 4.3 system lacked dedicated IP recording features, any IP data presented could not be considered reliable or authentic. This reasoning conflates the absence of a dedicated recording feature with the impossibility of IP address capture. In many systems, IP addresses are automatically logged by web servers and network infrastructure even if the application layer does not explicitly display them. The Court did not engage with this technical distinction, instead accepting a blanket assertion that the technological standards of April 2021 precluded any reliable IP evidence.

Taken together, the conceptual errors identified in Table 2 produced a cascading failure of evidentiary analysis. First, the Court misclassified IP addresses as file metadata, applying incorrect verification standards. Second, the Court assigned verification responsibilities to the Working Group, which lacked both legal authority and technical capacity. Third, the Court relied on an oversimplified technological assessment—that SPSE 4.3 did not record IP addresses—to dismiss all network forensic evidence. Fourth, the Court ignored the cumulative probative value of combining IP evidence with metadata evidence and typographical error evidence, treating each piece in isolation rather than as part of a corroborative evidentiary package. This approach violates established principles of circumstantial evidence, where the whole may be greater than the sum of its parts. In conspiracy cases involving bid rigging, direct evidence of coordination is rarely available; competition authorities necessarily rely on patterns of indirect indicators. By dismantling these patterns through forensic misclassification, the Supreme Court created a standard of proof that is practically impossible to meet in digital procurement environments.

The most significant implication of Table 2 extends beyond the specific case to the broader need for digital forensic training within the Indonesian judiciary. The conceptual error—treating network forensics as identical to file system forensics—reflects a lack of specialized knowledge among judex juris (Supreme Court) level judges regarding the technical foundations of electronic evidence. As procurement systems continue to digitize and collusion schemes increasingly leave digital traces, Indonesian courts cannot afford to maintain such forensic illiteracy. Comparative jurisdictions such as Singapore have established judicial training programs on electronic evidence, including specialized modules on network forensics, log authentication, and chain-of-custody for digital artifacts. Brazil's CADE employs in-house forensic analysts who can testify to the technical distinctions between different categories of digital evidence. China's cybersecurity courts include technical examiners who advise on forensic classifications. Indonesia, following the errors exposed in Decision 445/2021, must consider similar institutional reforms. Without judicial capacity to distinguish between network forensics and file system forensics, future tender collusion cases will continue to suffer from the same misclassifications, allowing coordinated bidders to evade accountability while undermining legal certainty and fair competition in public procurement.

Implications of Judicial Inconsistency on Justice and Legal Certainty

Supreme Court Decision 445/2021 has sparked controversy between legal certainty and justice. This ruling differs from previous decisions that recognized IP addresses as evidence, thereby reducing legal predictability. The rejection of digital evidence also shows that justice has been neglected, as it benefits those who collude and undermines market integrity.

Table 3: Comparison of Supreme Court Jurisprudence on IP Address Evidence

No	Decision Number	Year	The Judge's Consideration of IP Addresses	Probative Weight
1	154 K/Pdt.Sus-KPPU/2015	2015	Indications of coordination, reinforced by similarities in format, typographical errors, pricing, and distributors.	Additional Evidence
2	917 K/Pdt.Sus-KPPU/2016	2016	Coordination indicators must be linked to document and facility uniformity.	Valid Supporting Evidence
3	5 K/Pdt.Sus-KPPU/2019	2019	Indications of coordination when logging in to upload documents, strengthening family relationships and guaranteeing offers.	Important Evidence
4	570 K/Pdt.Sus-KPPU/2022	2022	Evidence supporting the conspiracy, backed up by the similarity in the format of the documents and letters of guarantee.	Strong Evidence Reinforcer
5	445 K/Pdt.Sus-KPPU/2021	2021	Weak evidence and only part of the Working Group's verification. Reducing the weight of the IP Address.	Evidence Overruled

Sorce: direktori putusan mahkamah agung

New Paradigm of Digital Evidence and Legal System Transformation

Unifying IP addresses as the main indication of tender collusion, through comparative research on the legal basis across jurisdictions. Generally, almost all countries justify the use of IP addresses as indirect evidence, although the reality of capturing them from technical data to legal evidence tends to vary in each legal system. In Brazil, IP addresses are regulated by court supervision regarding data storage. Under applicable law, internet providers are required to store a registro de conexão, or log containing all data necessary to access the internet, from IP addresses to access times, for at least one year. This rule ensures that the data remains authentic, so that the Conselho Administrativo de Defesa Econômica (CADE) can use it as valid preliminary evidence. However, its use must still be approved by the court in order for the evidence to remain valid in the eyes of the law. The legitimacy of IP addresses in Singapore is based on the principle of presumption of authenticity, which stipulates that electronic records, including IP address logs generated by reliable and legitimate operating systems, are accurate and prima facie. As a result, IP components generated are given strong initial weight, while the burden of proof is shifted to the opposing party to demonstrate that the data is fabricated or invalid. The Competition and Consumer Commission of Singapore (CCS) has the authority to prove invalidity from the outset. In China, IP addresses are positioned within the legal framework as an Institutional Mandate for Log Retention. Based on the 2017 Cybersecurity Law, network operators are required to store access logs, including IP addresses, for at least six months to ensure data availability for investigations. In about half of the previous Chinese immigration data privacy cases, the logs were found to be unavailable. In addition, the same law regulates The provision of goods and services and explicitly refers to the similarity of IP addresses as formal preliminary evidence of the tender conspiracy under investigation, which means that IP addresses are considered de jure as lead evidence that can lead to a legal investigation.

Table 3: Comparison of IP Address Verification Standards: Indonesia vs. International

Country	Legal Basis for IP Evidence	Log Retention Obligation	The Principle of Proving IP Addresses
Indonesia (Following Supreme Court Decision 445/2021)	✓	✗	✗
Brazil	✓	✓	✓
Singapore	✓	✓	✓
China	✓	✓	✓

The table presents a stark contrast between Indonesia's evidentiary framework for IP addresses following Supreme Court Decision No. 445/K/PDT.SUS-KPPU/2021 and the frameworks adopted by three comparator jurisdictions: Brazil, Singapore, and China. All four countries possess a formal legal basis for considering IP addresses as evidence in competition proceedings, as indicated by the checkmark (✓) in the first column. However, the similarity ends there. While Brazil, Singapore, and China have established comprehensive systems that include mandatory log retention obligations and clear principles governing the probative weight of IP address evidence, Indonesia has failed to implement either complementary safeguard. This divergence reveals a fundamental weakness in the Indonesian approach, where the theoretical admissibility of digital evidence is not supported by the institutional and technical infrastructure necessary to give it meaningful evidentiary value.

The second column of the table highlights a critical procedural gap: Indonesia imposes no log retention obligation on internet service providers or procurement system administrators. In contrast, Brazil requires providers to maintain connection logs (registro de conexão) for at least one year under the Marco Civil da Internet, Singapore's Evidence Act creates a presumption of authenticity for logs generated by reliable systems, and China's Cybersecurity Law mandates a six-month retention period for access logs including IP addresses. Log retention is not merely an administrative formality; it is the foundational condition that enables later forensic verification. Without a statutory obligation to preserve IP address data, Indonesian authorities cannot authenticate whether a specific address was actually assigned to a particular participant at a critical moment, rendering any IP-based evidence inherently vulnerable to claims of alteration or unavailability.

The third column exposes the most substantive legal difference: the principle governing how IP addresses are proven and weighted as evidence. Brazil, Singapore, and China have all adopted frameworks that assign presumptive or preliminary probative value to IP address evidence, shifting the burden of rebuttal to the opposing party once basic authenticity is established. Indonesia, following the logic of Supreme Court Decision 445/2021, rejects any such presumption. The Court treated IP address similarity as merely an administrative verification matter for the procurement working group (pokja), which lacked access to the SPSE logs. Consequently, Indonesian courts do not recognize IP address similarity as even a prima facie indicator of coordination. This means that even when multiple tender participants share identical public IP addresses within narrow time windows, Indonesian judges may dismiss this evidence as technically unreliable unless accompanied by corroboration that the current system cannot reliably provide.

The inconsistency illustrated by the table has direct consequences for legal certainty and fair competition enforcement in Indonesia. When the Supreme Court in Decision 445/2021 rejected the KPPU's evidence package which included IP address similarities alongside metadata anomalies and identical typing errors it effectively signaled that digital coordination can occur without meaningful evidentiary consequences. This creates a perverse incentive for colluding tender participants to conduct bid rigging through shared

network infrastructure, knowing that IP evidence will be discounted. Furthermore, the absence of log retention obligations means that even if a future court wished to accept IP evidence, the raw data necessary for forensic authentication may no longer exist. Unlike Singapore, where the burden shifts to the opposing party to prove data fabrication, or China, where IP similarity de jure triggers investigation, Indonesia's framework places an impossible burden on competition authorities while offering no statutory protection for digital evidence integrity.

The table's diagnosis leads inexorably to the conclusion stated in the accompanying text: Indonesia requires structured legal reforms across three dimensions. First, judicial standardization must be pursued through Supreme Court guidance or a formal circular (SEMA) clarifying that IP address similarity, when combined with corroborating digital evidence (timestamps, metadata, document anomalies), constitutes admissible circumstantial evidence of coordination. Second, legislative amendments to the ITE Law or the Business Competition Law should mandate log retention obligations for procurement systems (SPSE) and internet service providers, with specified retention periods and chain-of-custody procedures. Third, institutional capacity building at the KPPU and LKPP is essential to enable scientific analysis of IP address logs and their integration into forensic evidence packages. Only by adopting the integrated approach already implemented in Brazil, Singapore, and China—where legal basis, log retention, and probative principles operate together—can Indonesia achieve the balance between substantive justice and legal certainty in the digital age of public procurement.

5. Conclusion

The ratio decidendi of the Supreme Court is fundamentally flawed in two respects: first, it conflates network-layer IP addresses which record the origin of an internet connection with static application-layer file metadata, exposing a critical limitation in digital forensic literacy that misclassifies the probative nature of electronic evidence; and second, it procedurally errs by delegating verification to the Pokja, whose jurisdiction under Article 13(1) of Presidential Regulation No. 16/2018 is strictly confined to administrative compliance, critically excluding any authority to access SPSE backend servers or raw log repositories, thereby rendering the assigned task jurisdictionally impossible. This judicial inconsistency creates legal uncertainty and contradicts comparative best practices in Brazil, Singapore, and China, which admit IP evidence as corroborative circumstantial evidence. To remedy these deficits, a concrete three-pillar reform framework is urgently required: (1) the Supreme Court must issue a SEMA or amend PERMA to explicitly classify IP addresses as admissible circumstantial evidence with a rebuttable presumption of coordination when identical IPs appear within the bidding window, adopting ISO/IEC 27037 standards and mandating three technical prerequisites before admission as prima facie proo timestamp correlation, user-session logs from the same node, and SHA-256 cryptographic hashing at collection to ensure integrity; (2) the government must enact a PP or joint ministerial decree imposing a mandatory five-year retention period for all SPSE/LPSE raw access logs in WORM format, coupled with daily BSSN-certified cryptographic timestamping and an independent forensic authentication procedure prior to any court submission; and (3) the KPPU and LKPP must receive dedicated budgets to establish permanent Digital Forensic Units, compulsory certification programs (SANS, CHFI) for investigators, a secure read-only forensic interface granting KPPU direct access to SPSE logs independent of the Pokja, and formal MoUs with the Ministry of Communication and Informatics and BSSN for upstream ISP data retrieval when internal logs are insufficient. Collectively, these targeted measures resolve the jurisdictional overreach, technical misclassification, and forensic incapacity identified in the flawed ruling, operationalizing IP addresses as scientifically valid initial indicators of tender collusion when systematically corroborated with supporting evidence.

6. Referensi

[1] G. Puspaningrum, I. W. Yasa, and L. C. Putri, "A Legal Perspective Toward Unlawful Acts in Tender Collusion in Indonesia," *Media Iuris*, vol. 8, no. 3, pp. 439–460, 2025, doi: 10.20473/mi.v8i3.68535.

[2] L. B. Bukit and H. Sugiyono, "Sanctions Against Working Groups for the Selection of Goods/Services Providers in Cases of Tender Collusion (Study: Comparison between Indonesia and Malaysia)," *Rechtsidee*, vol. 13, no. 2, pp. 1–17, 2025, doi: 10.21070/jihr.v13i2.1093.

[3] X. Wang, K. Ye, T. Zhuang, and R. Liu, "The Influence of Collusive Information Dissemination on Bidder's Collusive Willingness in Urban Construction Projects," *Land*, vol. 11, no. 5, pp. 1–14, 2022, doi: 10.3390/land11050643.

[4] Mochtar, Z. Arifin, and E. O. S. Hiariej, *Understanding Legal Principles, Theories, Foundations, and Philosophy*. Jakarta: Perpustakaan Nasional, 2021.

[5] Firmansyah, Anry, R. Y. Maulana, and A. Z. Miftah, "Transformation Of The Procurement System In The Indonesian Government," *Sosiohumaniora J. Ilmu-ilmu Sos. dan Hum.*, vol. 26, no. 2, pp. 1–40, 2024.

[6] J. Bernardus, N. Kadenko, D. Broeders, M. Van Eeten, K. Borgolte, and T. Fiebig, "Pushing boundaries: An empirical view on the digital sovereignty of six governments in the midst of geopolitical tensions," *Gov. Inf. Q.*, vol. 40, no. 4, pp. 1–20, 2023.

[7] Pavol, L. R. Sokol, K. Lucivjanska, and J. Harašta, "IP Addresses in the Context of Digital Evidence in the Criminal and Civil Case Law of the Slovak Republic," *Forensic Sci. Int. Digit. Investig.*, vol. 32, no. 6, pp. 45–60, 2020.

[8] H. P. Putra and V. Juwono, "Policy Evaluation Of Kppu In The Supervision Of E-Procurement For The Revitalization Of Taman Ismail Marzuki Phase In 2022," *Natapraja*, vol. 13, no. 1, pp. 1–30, 2025.

[9] S. I. Affierni, I. Nafikadini, and D. Rokhmah, "Qualitative Study on Perpetrator of Child Sexual Violence with the Symbolic Interaction Theory Approach," *J. Kesehat. Masy.*, vol. 16, no. 37, pp. 17–27, 2020.

[10] Z. Abdussamad, *Metode Penelitian Kualitatif*, 1st ed. Bandung: CV. syakir Media Press, 2021.

[11] S. Wibowo, "Collusion in Electronic Procurement of Goods and Services for Construction Services (Case Study No. 24/Kppu-I/2020)," *J. Huk. Caraka Justitia*, vol. 2, no. 1, pp. 30–40, 2022.

[12] Y. Xie, Z. Zhang, Y. Liu, E. Chen, and N. Li, "Evaluation Method of IP Geolocation Database Based on City Delay Characteristics.," *Electronics*, vol. 13, no. 1, pp. 40–60, 2023.