



## A Juridical Analysis of the Use of Technology in Investigation and Inquiry Processes Based on Scientific Crime Investigation to Uncover the Murder Case of a Former Member of the Langkat Regional House of Representatives

Syaiful Bahri<sup>1\*</sup>, Triono Eddy<sup>2</sup>

Magister Ilmu Hukum, Universitas Muhammadiyah Sumatera Utara, Medan  
[bahri9783@gmail.com](mailto:bahri9783@gmail.com), [trionoeddy@umsu.ac.id](mailto:trionoeddy@umsu.ac.id)

**Corresponding Author:** Syaiful Bahri [bahri9783@gmail.com](mailto:bahri9783@gmail.com)

### ARTICLE INFO

*Keywords:* Information Technology, Electronic Evidence, Criminal Procedure

*Received :* 10 December 2025

*Revised :* 17 January 2026

*Accepted:* 20 February 2026

©2026 Bahri, Eddy: This is an open-access article distributed under the terms of the [Creative Commons Attribution 4.0 International](https://creativecommons.org/licenses/by/4.0/).



### ABSTRACT

The development of information technology has brought significant changes to the criminal justice system in Indonesia, particularly in the investigation and inquiry stages of criminal acts. This study aims to analyze the legal basis for the use of technology in the investigation and inquiry process, its application in solving the murder case of a former member of the Langkat Regional People's Representative Council (DPRD), and the validity of technological evidence in the evidentiary process according to criminal procedural law. This study uses a normative-empirical legal method with a conceptual approach and a case approach. Data were obtained through a literature review of primary, secondary, and tertiary legal materials, and supported by an analysis of the practice of applying technology in investigations. The results of the study indicate that the use of technology in investigations and inquiries has a legal basis sourced from the Criminal Procedure Code, the Electronic Information and Transactions Law, and the Police Law. In practice, technologies such as CCTV, telecommunications data, and digital forensics play an important role in helping investigators uncover crimes more objectively and accurately. Legally, technological evidence is basically legitimate for use in the criminal evidentiary process as long as it is obtained through legal procedures, its authenticity and integrity are maintained, and it meets the principles of legality, authenticity, and integrity.

## **INTRODUCTION**

The development of information technology has brought significant changes to the criminal justice system in Indonesia, particularly in the investigation and prosecution of criminal acts. This digital transformation has not only impacted the way investigators gather information but has also transformed the standards and paradigms of evidence in modern law enforcement. Investigators no longer rely solely on traditional methods such as witness testimony, suspect confessions, or conventional evidence, as these methods often carry a high degree of subjectivity and are susceptible to various factors such as psychological pressure, limited memory, or manipulation by certain parties.

In response to these challenges, investigators are now utilizing various forms of digital technology that can strengthen the evidentiary process through objective, systematic, and scientifically verifiable data. One of the most commonly used forms of technology is CCTV footage, which can record the chronology of events in real time, providing a visual depiction impossible with traditional witness testimony. Furthermore, digital forensics has become a crucial tool in uncovering electronic evidence from digital devices, such as cell phones, computers, social media accounts, and digital activity logs, which can illustrate the communication patterns and movements of perpetrators.

Another technology that plays a significant role is BTS (Base Transceiver Station) tracking and telecommunications device metadata analysis. Through these techniques, investigators can determine a person's location at a specific time based on their device's connection data to the BTS tower. This information is extremely helpful in confirming alibis, mapping the perpetrator's movements, and reconstructing the sequence of events more accurately.

Furthermore, the use of electronic data analysis, including call data records, digital messages, electronic transactions, and audio or video recordings, provides a new dimension of evidence that strengthens the reliability of investigations. Electronic evidence obtained through legitimate procedures is also legally recognized as stipulated in the Electronic Information and Transactions (ITE) Law and various other implementing regulations.

Thus, the use of digital technology not only increases the effectiveness and efficiency of investigators' work but also encourages a more modern, transparent, and accountable law enforcement process. Technology enables more objective, accurate, and scientifically verifiable evidence, thereby reducing reliance on subjective evidence and improving the quality of evidence in the Indonesian criminal justice system. The application of Scientific Crime Investigation (SCI) in the investigation and inquiry process is a modern approach that prioritizes the use of scientific methods, digital technology, and forensic analysis to uncover crimes more accurately and objectively. SCI emphasizes that every step—from identification and collection to securing and analyzing evidence—must be conducted in accordance with scientific standards to ensure legal accountability.

During the investigation phase, SCI is used to gather initial information through scientific observation, crime scene analysis, and systematic data collection of initial evidence. Techniques such as crime scene photography, sketching, digital mapping, and physical and electronic trace tracing are conducted according to standard procedures.

During the investigation phase, SCI plays a crucial role in analyzing evidence using forensic laboratories, including digital forensics, ballistics, serology, toxicology, and communication network analysis. Each piece of evidence is processed through scientific methods to uncover the *modus operandi*, the identity of the perpetrator, and the relationship between the evidence and the crime. A strict chain of custody is implemented to ensure the validity of the evidence and ensure its suitability for presentation in court.

Thus, the SCI approach makes the law enforcement process more modern, transparent, and effective. In addition to increasing the success rate of solving cases, SCI also strengthens the quality of evidence to convince judges legally and scientifically, in accordance with the principles of a professional and accountable criminal justice system.

The murder case of a former member of the Langkat Regional People's Representative Council (DPRD) is a concrete example demonstrating how advances in information technology have significantly contributed to the effectiveness of the investigation and prosecution of serious crimes. In this case, investigators utilized various modern technological instruments to trace the perpetrators' involvement, strengthen the legal framework, and ensure that each stage of the investigation was based on valid and accountable evidence.

One prominent technological aspect in solving this case was the investigators' ability to track the movements of the perpetrator and victim through the use of electronic data. Technologies such as BTS (Base Transceiver Station) tracking, GPS location analysis on mobile devices, and CCTV footage from various points passed by the victim and perpetrator were used simultaneously to depict movement patterns consistent with the chronology of the incident. This data provided objective information and helped investigators refute or verify the alibis of the parties involved.

Furthermore, investigators also relied on digital forensics to extract various forms of electronic evidence from the digital devices of the perpetrators and victims. Through digital forensics, investigators were able to discover communication histories, traces of conversations via instant messaging applications, phone calls, voice recordings, digital documents, and even photos or videos related to the crime. This information was then analyzed to uncover the motive, the relationship between the perpetrators, and the sequence of actions before and after the murder.

The use of technology also allows investigators to systematically reconstruct the chronology of events, based on the integration of digital evidence, physical evidence, and witness testimony. This approach not only strengthens the validity of the investigation but also provides a more accurate picture of the sequence of events, the location of the incident, and the role of each individual in the crime.

## **LITERATURE REVIEW**

However, the use of technology in this case is not without its challenges, both technical and legal. Technically, investigators face limitations in their ability to analyze large amounts of data (big data), device damage, encryption, or the perpetrator's attempts to erase digital traces. The digital forensics process also requires specialized expertise and adequate equipment to ensure scientifically sound findings.

Legally, challenges arise regarding the validity of electronic evidence, data acquisition procedures, and compliance with the chain of custody principle to ensure the authenticity and integrity of digital evidence. Deviations in procedures can potentially weaken the evidentiary value and open the door to objections from the defendant. Furthermore, investigators must ensure that all seizures, searches, and examinations of electronic evidence comply with statutory provisions, particularly the Criminal Procedure Code (KUHAP) and the Electronic Information and Transactions (ITE) Law.

Thus, the murder case of a former member of the Langkat Regional People's Representative Council (DPRD) not only demonstrates the successful use of technology in law enforcement, but also highlights the importance of aligning technical capabilities with legal certainty so that technology can be used effectively, legally, and accountably in the criminal justice process.

Legally, the use of technology in the investigative process must be within clear legal boundaries and in line with statutory provisions. The Criminal Procedure Code (KUHAP), the primary source of Indonesian criminal procedure law, does not explicitly include digital or electronic evidence within the categories of evidence regulated in Article 184 of the KUHAP. It only recognizes five types of evidence: witness testimony, expert testimony, letters, clues, and defendant testimony. This ambiguity creates a normative gap when investigators must handle evidence originating from electronic devices or digital systems.

To fill this gap, the Electronic Information and Transactions Law (UU ITE) was enacted, which expressly legitimizes electronic information and/or electronic documents as valid evidence. This provision represents a significant milestone in the modernization of evidentiary law in Indonesia, as it recognizes that digital transactions and interactions produce legally accountable data. The ITE Law and its amendments also stipulate that electronic evidence has the same standing as conventional evidence as long as it meets legal acquisition procedures.

However, in practice, investigations involving digital technology still face a number of challenges and debates, particularly regarding the legality of digital seizure procedures, the authentication of electronic evidence, and the protection of privacy rights.

From a procedural perspective, the seizure of digital evidence often raises issues due to the nature of electronic data, which is easily damaged, altered, or deleted. The Criminal Procedure Code (KUHAP) does not yet provide technical guidelines on the correct procedures for confiscating, copying, securing, and examining digital devices. Consequently, investigators must refer to internal regulations such as Police Regulations (Perkap) or Standard Operating

Procedures (SOPs), but these regulations are not as firmly grounded as law. This leaves room for defendants to challenge the legality of seizures.

Another challenge arises in the authentication and integrity of electronic evidence. Digital evidence must be proven authentic through a strict chain of custody process, from the moment it is discovered until it is presented in court. Any change, even the slightest change to the data, can weaken its evidentiary value. Courts require assurance that electronic evidence has not been digitally modified, manipulated, or contaminated, potentially compromising its validity.

Furthermore, the issue of protecting privacy rights is crucial in the context of technology-based investigations. Collecting electronic data such as communication histories, CCTV recordings, or location tracking has the potential to involve personal information protected by the constitution and laws and regulations. Investigators must ensure that these actions are conducted with legitimate authority, have probable cause, and do not exceed the limits necessary for the purposes of the investigation. Failure to do so can lead to human rights violations and compromise the legality of evidence.

Therefore, although the ITE Law has normatively expanded the scope of evidence in the Indonesian legal system, investigators must still implement appropriate and principled procedures to ensure that the use of technology in investigations remains lawful, proportional, and respects individual rights. Harmonization between the Criminal Procedure Code (KUHP), the ITE Law, and other technical regulations is essential for optimal acceptance of digital evidence.

## **METHODOLOGY**

This study employs a normative-empirical legal research approach, a mixed approach that combines analysis of written legal norms with a study of their application in practice. This approach was chosen because the issues studied are not only at the regulatory level but also relate to how these legal provisions are implemented in the field by law enforcement officials. From a normative perspective, the study examines various laws, doctrines, and legal principles that form the basis for case resolution, including provisions regarding investigators' authority, the principle of restorative justice, and regulations on conflict resolution mechanisms within the criminal justice system. The normative analysis also aims to assess the conformity of investigators' actions with applicable positive legal provisions.

Meanwhile, from an empirical perspective, the study examines facts on the ground through interviews, observations, and analysis of case documents. Empirical research focuses on the behavior of law enforcement officials, community responses, social dynamics, and practical obstacles to implementing legal provisions. Through this approach, the research can demonstrate whether legal regulations have been implemented effectively, consistently, and in accordance with their stated purpose.

By combining these two approaches, normative-empirical legal research allows researchers to identify the gap between ideal law (*das sollen*) and the law in practice (*das sein*), while simultaneously providing a comprehensive picture

of the effectiveness of the application of legal norms in actual social contexts. This mixed approach is particularly relevant for examining legal issues that require both theoretical and practical understanding.

In this research, a conceptual approach is used to provide a strong theoretical foundation for analyzing the use of technology in the investigation and inquiry process. This approach focuses on understanding fundamental theories and concepts in criminal law and criminal procedure, particularly those related to the theory of evidence, the digital chain of custody, and the principle of legality. Through this approach, the research examines how modern evidentiary theory views electronic evidence and digital forensic results, how the chain of custody concept ensures the authenticity and integrity of digital data in the investigative process, and how the principle of legality limits or directs the use of technology to ensure it remains within the legal framework.

Furthermore, the research also uses a case-based approach to directly examine the structure and process of the investigation into the murder of a former member of the Langkat Regional People's Representative Council (DPRD). This approach is conducted by analyzing court decisions, investigative chronologies, and data related to the mechanisms for using technological evidence in handling these cases. Through case analysis, the research can illustrate concrete practices in the field regarding the effectiveness of technology use by investigators, including how electronic evidence is collected, verified, and used as a basis for solving criminal cases.

Using normative juridical methods, this research utilizes primary legal materials, such as Law Number 8 of 1981 concerning Criminal Procedure Code (KUHAP), Law Number 11 of 2008 concerning Electronic Information and Transactions as amended by Law Number 19 of 2016, the Police Law, and other regulations relating to the authority and procedures for using technology in the investigative process. These primary legal materials provide a normative basis for how electronic evidence, digital forensics, and other technological instruments are recognized and used in the criminal justice system.

In addition, this research also relies on secondary legal materials, such as legal literature, scientific journals, textbooks, expert opinions, previous research results, and academic commentary regarding the application of technology in law enforcement. These secondary materials help interpret written norms, enrich theoretical understanding, and clarify legal positions in modern investigative practice.

In addition, tertiary legal materials such as legal dictionaries, encyclopedias, and regulatory indexes are used to clarify technical concepts and terms related to forensic technology, electronic evidence, and evidentiary theory.

To process and interpret the data obtained, this study applies analytical descriptive analysis techniques. This technique is carried out by systematically describing legal facts, investigative phenomena, and the mechanisms of technology use, then connecting them to applicable legal theory and norms. Descriptive analysis provides an objective picture of investigative practice, while analytical analysis serves to test the suitability of the data.

## **RESEARCH RESULT AND DISCUSSION**

### **A. Legal Basis for the Use of Technology in Criminal Investigations and Prosecutions in Indonesia**

The use of technology in criminal investigations and probings in Indonesia is essentially based on several laws and regulations. In general, investigators' authority to seek and collect evidence is regulated by the Criminal Procedure Code (KUHAP), specifically regarding inquiries, searches, seizures, and the gathering of evidence. Although the KUHAP does not explicitly regulate digital evidence or forensic technology, this authority remains the normative basis for law enforcement officials to use modern means to uncover crimes.

A more specific legal basis for the use of technology is contained in Law Number 11 of 2008 concerning Electronic Information and Transactions in conjunction with Law Number 19 of 2016, particularly the provision recognizing Electronic Information and/or Electronic Documents and their printouts as valid legal evidence. This provision expands the criminal evidence system, which previously relied solely on Article 184 of the KUHAP. With this recognition, various forms of evidence, such as CCTV footage, digital messages, communication histories, location data, call data records, and other electronic documents, can be used in the evidentiary process.

Furthermore, the use of technology in investigations is supported by Law Number 2 of 2002 concerning the Indonesian National Police, which authorizes the police to carry out their investigative and inquiry functions professionally by utilizing science and technology. In practice, this is further reinforced through internal police policies, such as the implementation of Scientific Crime Investigation (SCI), a modern investigative method that emphasizes the use of scientific approaches, forensic laboratories, and digital analysis in solving crimes.

Thus, it is understandable that the legal basis for the use of technology in the investigation and inquiry process in Indonesia rests not only on the Criminal Procedure Code (KUHAP), but is also reinforced by the ITE Law, the Police Law, and scientific approaches in modern law enforcement. This demonstrates that the Indonesian criminal justice system has gradually adapted to developments in information technology.

### **B. Application of Technology in Solving the Murder Case of a Former Langkat Regional People's Representative Council Member**

Based on research results, the resolution of the murder case of a former Langkat Regional People's Representative Council member demonstrates the crucial role of technology in the investigation and prosecution of serious crimes. In murder cases, technology serves not only as a fact-finding tool but also as an instrument to strengthen the objective construction of evidence. In this context, law enforcement officials can utilize various forms of technology such as CCTV footage, communication data, mobile phone location traces, and digital device analysis to reconstruct the criminal incident.

The application of technology in solving murder cases generally involves several stages. First, investigators trace the movements of the victim and related parties using electronic data such as CCTV footage around the scene, travel

routes, and points suspected of being linked to the crime. Second, investigators can use BTS (Base Transceiver Station) data or other telecommunications data to determine the location of mobile devices at specific times. This data is highly relevant for testing alibis, observing movement patterns, and linking the perpetrator to the scene.

Third, the application of digital forensics allows investigators to extract data from electronic devices such as mobile phones, laptops, and digital communication accounts. Through this process, investigators can discover traces of conversations, phone calls, electronic documents, photos, videos, and metadata that can shed light on the relationship between the victim and the perpetrator, the motive, and the sequence of events before and after the crime. In murder cases, this type of digital evidence is crucial because it can serve as a link between physical evidence, witness testimony, and expert testimony.

However, the application of technology in solving the murder of a former member of the Langkat Regional People's Representative Council (DPRD) must also be understood carefully. From an academic perspective, the use of technology should be viewed as a relevant and logical tool in modern investigations, unless its full use has been explicitly proven in case files, court decisions, or official investigative documents. Therefore, analytically, it can be concluded that the application of technology in this case demonstrates how modern investigations require the integration of conventional and technology-based evidence to produce a more effective and objective law enforcement process.

### C. Legal Analysis of the Validity of Technological Evidence in the Proof Process According to Criminal Procedure Law

From a legal perspective, the validity of technological evidence in criminal proceedings in Indonesia is part of the development of modern evidentiary law. The Criminal Procedure Code (KUHAP), as the primary criminal procedural law, does not explicitly mention electronic evidence as a type of evidence under Article 184 of the KUHAP. This article only recognizes five types of evidence: witness testimony, expert testimony, letters, clues, and defendant testimony. This situation creates problems when investigators and public prosecutors encounter evidence originating from digital devices or electronic systems.

This normative gap was then filled by the ITE Law, which recognizes Electronic Information, Electronic Documents, and printouts as valid legal evidence. Thus, technology-based evidence is inherently legally binding, as long as it is obtained through legitimate and legally accountable procedures. In criminal justice practice, technological evidence typically does not stand alone but is associated with other forms of evidence such as expert testimony, letters, and clues.

The validity of technological evidence depends heavily on three essential elements: legality of acquisition, authenticity, and integrity. First, from a legal perspective, evidence must be obtained through legitimate procedures, such as seizure, search, or data request, in accordance with the investigator's legal authority. Second, from an authenticity perspective, evidence must be proven to

be authentic from its original source. Third, from an integrity perspective, the evidence must be protected from alteration, manipulation, or contamination from the time it is discovered until it is presented in court. In this regard, the principle of chain of custody is crucial for maintaining its evidentiary value.

From a criminal procedural law perspective, technological evidence can be deemed valid if it meets formal and material requirements. Formally, evidence must be obtained according to legal procedures. Materially, the evidence must be relevant, verifiable, and logically related to the criminal event being examined. Therefore, although Indonesian positive law has opened up space for the use of technology in the provision of evidence, its application must be carried out carefully to avoid violating the right to privacy, the principle of due process of law, and human rights.

Thus, the legal analysis shows that technological evidence is essentially valid and can be used in criminal proceedings in Indonesia. However, its evidentiary strength is largely determined by the method of acquisition, the examination process, and guarantees of its authenticity and integrity. Therefore, harmonization between the Criminal Procedure Code (KUHAP), the ITE Law, and technical investigative guidelines is crucial for optimal acceptance of technological evidence in the Indonesian criminal justice system.

## **CONCLUSIONS AND SUGGESTIONS**

### **A. Conclusion**

Based on the research results and discussion, it can be concluded that the use of technology in the investigation and prosecution of criminal acts in Indonesia has a strong legal basis, both through the Criminal Procedure Code (KUHAP), the ITE Law, and the Police Law. The presence of technologies such as CCTV, telecommunications data, and digital forensics has made a significant contribution to supporting a more objective, effective, and accurate evidentiary process. In solving the murder case of a former member of the Langkat Regional People's Representative Council (DPRD), the application of technology demonstrated that digital-based evidence can play a vital role in assisting investigators in tracing criminal events, linking perpetrators to incidents, and strengthening the construction of evidence. Legally, technological evidence is essentially legitimate for use in criminal evidence proceedings, as long as it is obtained through legitimate procedures, its authenticity is maintained, and it meets the principles of legality, authenticity, and integrity.

### **B. Recommendations**

It is recommended that the government and lawmakers reform criminal procedural law, particularly by providing more stringent regulations regarding the status, procedures for obtaining, and examination of technological evidence in criminal proceedings. Furthermore, law enforcement officials need to improve their technical capacity and professionalism in the use of forensic technology so that digital-based evidence can be conducted accurately and responsibly. Furthermore, clearer operational standards are needed for the handling of electronic evidence, including the implementation of chain of custody, so that digital evidence presented in court has optimal probative value and does not give rise to legal disputes.

## REFERENCES

- Alan, M. F. (2024). Restorative justice and agrarian reform conflict resolution. *BHUMI: Jurnal Agraria dan Pertanahan*, 10(1).
- Andi Hamzah. (2019). *Hukum acara pidana Indonesia*. Sinar Grafika.
- ANTARA. (2023, January 27). *Kapolres Langkat bentuk tim khusus ungkap pembunuhan mantan anggota DPRD Langkat*.
- Artaji, Sulistiani, L., Rajamanicam, R., & Fakhriah, E. L. (2024). Resolution of agrarian conflicts on plantation land through restorative justice in Indonesia. *Lex Scientia Law Review*, 8(1).
- Bakhtiar, H. S., Ilyas, A., Kholiq, A., dkk. (2025). The utilisation of scientific crime investigation methods and forensic evidence in the criminal investigation process in Indonesia. *Egyptian Journal of Forensic Sciences*, 15.
- Ilham, M., Salim, A., & Sudarno. (2025). Efektivitas penggunaan alat bukti elektronik dalam proses pembuktian menurut hukum acara pidana. *Paulus Legal Research*, 3(1).
- Indonesia. (1981). *Kitab Undang-Undang Hukum Acara Pidana*.
- Indonesia. (2002). *Undang-Undang Nomor 2 Tahun 2002 tentang Kepolisian Negara Republik Indonesia*.
- Indonesia. (2008). *Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik*.
- Indonesia. (2016). *Undang-Undang Nomor 19 Tahun 2016 tentang Perubahan atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik*.

- Makarim, E. (2017). Keabsahan bukti elektronik dalam sistem peradilan pidana Indonesia. *Jurnal Hukum & Pembangunan*, 47(4).
- Mendrofa, A. F., Jamaluddin, & Bahreisy, B. (2022). Penguatan alat bukti melalui scientific crime investigation dalam tindak pidana pembunuhan dengan racun. *Suloh: Jurnal Fakultas Hukum Universitas Malikussaleh*, 10(1).
- Mualfah, D., & Ramadhan, R. A. (2020). Analisis forensik metadata kamera CCTV sebagai alat bukti digital. *Digital Zone: Jurnal Teknologi Informasi dan Komunikasi*, 11(2).
- Mustafa, C. (2024). Integritas chain of custody pada pemeriksaan bukti digital. *Judex Laguens*, 2(1).
- Nuh Al-Azhar, M., & Azhari. (2020). Digital forensics: Peran dan tantangannya dalam pembuktian tindak pidana. *Jurnal Legislasi Indonesia*, 17(3).
- Peter Mahmud Marzuki. (2016). *Penelitian hukum*. Kencana.
- Prayudi, Y., & Yudhana, A. (2018). Digital forensics sebagai metode ilmiah dalam penanganan bukti elektronik. *Jurnal Teknologi Informasi dan Ilmu Komputer*, 5(5).
- Ramadhan, R., & Mulyani, N. (2020). Pemanfaatan data BTS dalam mengungkap tindak pidana di Indonesia. *Jurnal Ilmu Kepolisian*, 14(2).
- Rolan Lolong, R. (2025). Peran restorative justice sebagai upaya hukum dalam penegakan hukum di Indonesia berdasarkan Peraturan Kepolisian Negara Republik Indonesia Nomor 8 Tahun 2021. *Lex Crimen*, 13(5).

Rombot, J. (2024). Kajian hukum pemeriksaan alat bukti dengan menggunakan metode scientific crime investigation dalam pengungkapan tindak pidana pembunuhan di Pengadilan Negeri Manado. *Lex Privatum*, 13(5).

Romli Atmasasmita. (2018). *Sistem peradilan pidana kontemporer*. Kencana.

Shidarta. (2020). Hak privasi dan pembatasannya dalam penyidikan berbasis teknologi. *Jurnal Yudisial*, 13(2).

Soerjono Soekanto. (2014). *Pengantar penelitian hukum*. UI Press.

Soponyono, E. (2019). Scientific crime investigation sebagai paradigma modern penyidikan. *Masalah-Masalah Hukum*, 48(3).

Suseno, S. (2019). Bukti elektronik dalam sistem pembuktian pidana. *Jurnal RechtsVinding*, 8(1).

Widodo. (2019). Pendekatan ilmiah dalam olah tempat kejadian perkara. *Jurnal Yudisial*, 12(1).