Available at https://journalenrichment.com/index.php/jr/

Enrichment: Journal of Multidisciplinary Research and Development

# Evidence of Criminal Acts in the Field of Electronic Information and Transactions in Review of Law No. 19 of 2016 concerning Electronic Information and Transactions

Alcapon Sidabutar[1], Risdalina[2], Indra Kumalasari M[3]

Universitas Labuhanbatu, Sumatera Utara, Indonesia

*Email: alcaponesid@gmail.com, risdalinasiregar@gmail.com, indrakumalasarim@gmail.com

**ARTICLE INFO**

***Keywords:***
*Evidence of Crimes, Information and Electronics, Law Number 19 of 2016 concerning ITE.*

**ABSTRACT**

*Advances in information technology have increased the number of crimes related to electronic transactions in Indonesia. Electronic evidence plays an important role in legal proceedings but often faces challenges in proving it. Law Number 19 of 2016 concerning Electronic Information and Transactions (ITE) establishes the legal framework for electronic evidence. This research aims to explore evidence of crime in information and electronic transactions according to the provisions of Law Number 19 of 2016 concerning ITE. This study uses a normative legal research method with a doctrinal approach. Secondary data are collected from relevant legal literature and analyzed to understand the application of legal doctrine related to electronic evidence. The results of the study show that electronic evidence such as electronic information, electronic documents, and printed documents are recognized as valid evidence based on Article 5 of the ITE Law. Proving criminal acts in the field of information and electronic transactions refers to Article 184 of the Criminal Procedure Code (KUHAP) which includes witness testimony, expert testimony, letters, instructions, and statements of the defendant. This research has implications for the importance of electronic evidence recognition in the Indonesian criminal justice system to increase the effectiveness of law enforcement in the digital era. These findings can be a reference for legal practitioners and policymakers in improving legal procedures related to electronic evidence.*

## INTRODUCTION

Law enforcement in Indonesia must take into account the quantity of cases involving crimes involving electronic transactions. These crimes are committed by people with a variety of backgrounds. from both the general public and government representatives. The evidence of illegal activity in internet typically has several benefits and drawbacks. Finding proof that someone has committed a crime can be challenging at times. Because there is often no proof that a person has committed a crime, lawsuits pertaining to the Electronic Information and Transaction Law henceforth referred to as the ITE Law are extremely challenging to settle. A few instances that frequently include the ITE Law are the dissemination of false information, hate speech, pornographic film distribution, and defamation on.

Electronic records and information are often what make up electronic evidence. Article 1 Point 1 of the ITE Law defines electronic information as any document, sound, image, map, design, photograph, Electronic Data Interchange (EDI), electronic mail, telegrams, telexes, text copies or the like, letters, signs, numbers, codes, access, symbols, or perforations that have been processed and have meaning or can be understood by people who are able to understand them. Moreover, Article 1 Point 2 specifies that legal activities conducted using computers, computer networks, and other electronic media are considered Electronic Transactions (Amajihono, 2022).

There are flaws in the way that ITE Law is applied to law enforcement, and as a result, not all criminal offenses involving the law can be adequately resolved. This is why the number of cases pertaining to the ITE Law is increasing, particularly in the area of cyberlaw enforcement. In the ITE field, the difficulty of the proof plays a crucial role in case resolution. On the other hand, supporting evidence can be used to resolve some other cases.

Under the heading Evidence of Crimes in the Field of Electronic Information and Transactions, the author of the research emphasizes this purpose in the Review of Law No. 19 of 2016 regarding Electronic Information and Transactions. Therefore, it is thought that this study would be able to determine.

From the background above, the purpose of this study is to find out about proof of criminal acts of information and electronic transactions in terms of Law Number 19 of 2016 concerning Electronic Information and Transactions.

## METHOD

Legal normative research is what this study is. Finding legal doctrines, rules, and principles to address the current legal concerns is the process of normative legal research, according to Peter Mahmud Marzuki (Marzuki, 2010). This type of normative legal research involves studying secondary data or library materials (Soekanto, 2007). Normative legal study, also known as doctrinal research, conceptualizes the law as either what is written in books or as laws and regulations, or as standards or norms that serve as guidelines for acceptable human behavior (Amiruddin, 2006).

## RESULTS AND DISCUSSION

### Evidence in criminal offences of information and electronic transactions based on Law Number 19 of 2016 concerning ITE

Since proof is an attempt to gather information through evidence and evidence, it basically plays a critical part in the investigation of criminal offenses involving information and electronic transactions. The evidence that has been collected so far will be used by the judge to determine whether or not the accused person actually committed a crime. In the event that the defendant presents evidence that is legally valid but insufficient to support the charges against him, the court is required to immediately absolve the defendant of all penalties. If the contrary occurs, though, the criminal will be punished appropriately for his actions.

Evidence in criminal offences of information and electronic transactions through evidence based on Law Number 19 of 2016, regulated in Article 5, which determines that:

1. Printouts of electronic documents and information are admissible as legal proof.
2. According to Indonesian procedural legislation that is in effect, electronic information, electronic documents, and their printouts—all mentioned in paragraph (1)—shall be considered an expansion of the legal record.
3. Electronic documents and information are deemed legitimate if they are created using an electronic system in compliance with this law's requirements.
4. The rules pertaining to electronic documents and information mentioned in paragraph (1) will not be applicable.
   a. Letters which by law must be in writing; and
   b. Letters and papers that legally need to be prepared as notarial deeds or deeds created by deed makers.

It is clear that the evidence used to prove ITE criminal acts plays a significant role in establishing the facts surrounding whether or not a person has committed an ITE-related crime in accordance with Article 5 of the ITE Law, which states that electronic information, electronic documents, and their printouts are valid legal evidence to in paragraph (1) are an extension of valid evidence in accordance with the applicable procedural law in Indonesia, namely Law Number 8 of 1981 concerning the Criminal Procedure Code (KUHAP). Valid evidence according to Article 184 of the Criminal Procedure Code, namely:

a. Witness statement
b. Expert statement
c. Letter
d. Instructions
e. Statement of the defendant

These types of evidence are necessary because the judge cannot penalize someone without concluding that the defendant genuinely committed the crime and that the offense truly occurred in the absence of at least two trustworthy pieces of evidence (D. Samosir, 2013). According to Article 184 of the Criminal Procedure Code and Article 5 of the ITE Law, proof of criminal activities involving information and electronic transactions must be founded on credible evidence (Amajihono, 2022). The proof cannot be fake; rather, it must be consistent with the reality. Thus, Article 5 of the ITE Law and Article 184 of the Criminal Procedure Code are the only references the judge will make while imposing the criminal verdict.

1. In general, witness testimony is defined under Article 1 Point 27 of the Criminal Procedure Code as evidence in a criminal case that the witness hears, sees, or experiences personally and gives a justification for his knowledge of it. The preceding essay makes evident that the most important elements of witness evidence are (Waluyo, 1992):
   a. Information from people (witnesses)
   b. Regarding a criminal event
   c. What you hear, what you see and what you experience.

Article 1 Point 26 of the Criminal Code defines a witness as a person who can provide information for an investigation, prosecution, and trial of a criminal case in which he hears, sees, and experiences personally. (Kawengian, 2016). In general, everyone is able to provide testimony. They may withdraw from the pool of potential witnesses and remain silent, unless they are among those protected by Article 168 of the Criminal Procedure Code, namely:

a. Blood relatives or cousins in a straight line up or down to the third degree of the defendant or joint defendants;
b. Siblings of the accused or co-accused, mother's or father's siblings, as well as those related by marriage and children of the accused's siblings up to the third degree;
c. Husband or wife of the defendant, even if divorced or jointly accused.

Apart from familial ties, Article 170 of the Criminal Procedure Code states that individuals who are required to maintain confidentiality due to their occupation, standing, or dignity may apply to be released from the requirement to testify as a witness. The Criminal Procedure Code's Article 171 further states that the following situations do not need testifying under oath:

a. A child who is not yet fifteen years old and has never been married.
b. People with memory loss or mental illness, even if they regain their memory.

In general, witness testimony evidence is the most important evidence in criminal cases (Rintasari, 2020). Since the majority of criminal cases are always predicated on the analysis of witness testimony, it may be claimed that no criminal case is exempt from the evidence of witness testimony. In addition to proof from other types of evidence, witness testimony evidence is always needed. The second category of evidence is witness testimony, as stated in Criminal Procedure Code Article 184. Information provided by a person with specialized understanding on matters needed to clarify a criminal case for investigation is regarded an expert witness, as per Article 1 Point 28 of the Criminal Procedure Code.

Regarding whom and which institutions are authorized to present experts is regulated in Law Number 8 of 1981 concerning the Criminal Procedure Code in several articles as follows (Andi Sofyan, 2017):

1) Article 65 provides that a suspect or defendant has the right to present a person with special expertise.
2) Article 120 stipulates that if deemed necessary, the investigator may request an expert opinion or a person with special expertise.
3) Article 133 stipulates that the investigator is authorized to submit a request for expert testimony to a judicial medical expert, doctor, or other expert.
4) Article 180 provides that the presiding judge may request expert testimony.
5) Article 186 states that public prosecutors can provide expert testimony during the investigation and examination process.
6) Article 229 stipulates that experts who appear to provide testimony at all levels of examination are entitled to reimbursement of expenses in accordance with the law.

2. Everything that appears to be meant to express a person's ideas or pour out their heart and is used as proof is considered letter evidence. A letter, as defined by Article 187 of the Criminal Procedure Code, is defined as "a report and other letters in official form made by an authorized public official or made before him, which contains information about events or circumstances that he hears, sees, or experiences, accompanied by clear and firm reasons for his statement." This definition is further expanded in Article 184 paragraph (1) letter c.

a certificate from an expert that expresses his opinion about a circumstance or subject matter that has been formally sought of him. Additional letters can only be accepted if their contents are related to those of other pieces of evidence (C. D. Samosir, 2013). Two types of letters can be used as evidence: genuine letters and shady letters. The judge is free to take into account the evidential capacity of general and special letters because the Criminal Procedure Code does not govern them. Underhand letters are no longer utilized in criminal procedural law, as they were in civil law, although in this instance, the genuine deed may be taken into consideration. However, it is plain that dishonest letters retain significance when there is a link with the information included in other

evidential instruments, in accordance with the material provisions of Article 187 point d. Thus, letters that are connected to a criminal offence in order to be accepted as letter evidence in court proceedings are letters that can be used to prove ITE criminal offenses.

3. In terms of the evidence of clues, clues are behaviors, incidents, or situations that, by virtue of how they relate to each other and to the criminal act in question, reveal the identity of the offender and the fact that a criminal act has taken place. Only witness testimony, correspondence, and the defendant's testimony can yield clues that can be used as evidence (Indonesia & Indonesia, 1981). A sequence of related events that can be utilized as evidence and offer hints regarding the commission of a crime is known as clue evidence.
4. The defendant's statement is what he says in court regarding the things he did, the things he knows, or the things he has personally experienced (in accordance with Article 189 paragraph (1)). (Hamzah 2005) that the evidence provided by the defendant does not have to be identical to or in the form of a confession. Whether the defendant denies, acknowledges, or partially acknowledges certain acts or circumstances, all of their testimony ought to be considered.

The confession as evidence requires the following requirements, therefore the defendant's statement need not be the same as a confession (Raditio, 2014):

1) Confess that he/she committed the offence charged.
2) Admit that he is guilty.

The defendant's declaration therefore holds greater weight than their confession. Article 189, paragraph 4 of the Criminal Procedure Code declares that the evidence of the defendant is insufficient to establish his guilt or innocence of the alleged offense. Consequently, the confessional statement made by the defendant does not absolve the burden of proof. Even in cases where a defendant confesses, more proof is still required to corroborate the material fact that is being sought. Meanwhile, the confession is used in civil procedural law to obtain the formal truth. The court examination process depends heavily on evidence, which judges must employ to prove ITE criminal charges.

**The Position of Electronic Evidence in Proving ITE Crimes**

Printouts of electronic documents are accepted as valid forms of evidence, according to Law Number 19 of 2016's Article 5. According to Article 184 of the Criminal Procedure Code, printouts, data, and electronic documents are considered an expansion of admissible evidence. Printouts of computer transactions and information are considered admissible forms of electronic evidence according to Article 184 of the Criminal Procedure Code. To establish legal certainty for the use of electronic systems and transactions, printouts, electronic information, and electronic documents are admissible forms of proof. This is especially true when it comes to evidence of crimes done using electronic devices (Radio, 2014).

The direct use of information and communication technology is becoming a common element of many crimes and criminal acts. The fact that computers, mobile phones, e-mail, the internet, websites, and other devices are so widely used has made it easier for people to conduct crimes with digital and electronic technologies. As a result, law enforcement has recently acknowledged and employed computer forensic science in their endeavors to uncover criminal activities through the release of evidence based on digital and electronic entities or devices.

Law enforcement will have a tough time demonstrating crimes committed in cyberspace, such as cybercrime cases involving data fabrication, as they are required to prove something that is seen as untrue and invisible. Among other things, the evidence is electronic in the form of electronic documents, which are commonly used and well-known in practice but are not yet governed by procedural law as formal law. Current arrangements pertaining to electronic evidence fall under the purview of material law, as exemplified by the ITE Law.

The electronic data and information that are accurately recorded on the hard drive of the central processor unit (CPU) are crucial pieces of evidence that can be used to prove a criminal offense. On the other hand, the usefulness of IE and ED is contingent upon the comprehension of their contents. Thus, a digital forensic test needs to be performed using the hard drive. When looking into computer crime and cases relating to computers, evidence is crucial, and tracing the movements of the criminals and apprehending them demands a comprehensive chronology. The forms of evidence are important for investigators and forensics to know because their location is highly strategic. He is able to identify the presence of evidence that requires more examination and analysis when he visits the crime scene of computer-related crimes.

Items used to commit crimes, products of crimes, or items connected to crimes that have already happened are all considered evidence (Kaligis, 2012).

The classification of digital evidence is divided into:

1) Electronic evidence

2) Digital evidence

Physical and visual evidence is easily identifiable. Consequently, when looking for evidence at the crime scene, detectives and forensics need to comprehend and then be able to identify each of these electronic pieces of evidence (Unik et al., 2019).

The types of electronic evidence are as follows:

a) PC, laptop/notebook, netbook, tablet
b) Mobile phone, smartphone
c) Flashdisk/thumb drive
d) Floppy disk
e) Harddisk
f) CD/DVD
g) Counters, switches, hubs
h) Video cameras, CCTV
i) Digital camera
j) Digital recorder
k) Music/video player.

According to the ITE Law, digital evidence is derived from other electronic evidence and is referred to as electronic information and electronic documents. Forensic search techniques must be used to find this kind of proof. Then, in order to identify cases of crimes involving electronic evidence, a thorough analysis of the relationships between each file is required. The admissibility of electronic evidence is contingent upon the utilization of an electronic system compliant with relevant Indonesian rules. Electronic evidence that can be verified for accuracy, accounted for, retrieved, and presented in a way that clarifies a situation is admissible in court.

Writings, sounds, images, maps, designs, photos, electronic data interchange (EDI), electronic mail (electronic mail), telegrams, telexes, telecopies, or the like, letters, signs, numbers, access codes, symbols, or perforations that have been processed and have meaning or can be understood by people who are able to understand them are all considered forms of electronic information, according to Article 1 Number 1 of the ITE Law (Koto, 2021). Any electronic information created, sent, received, delivered, or stored in analog, digital, electromagnetic, optical, or comparable forms that can be viewed, shown, or heard using a computer or electronic system is considered an electronic document, as defined by Article 1 Point 4 of the ITE Law. This description includes writings, sounds, images, maps, designs, photographs, and the like; it also includes letters, signs, numbers, access codes, symbols, and perforations that have meaning or that readers can decipher (Sulistyo & Ardjayeng, 2018).

To sum up, the ITE Law's presence is critical to preserving legal clarity in cyberspace, particularly in regards to issues pertaining to data and electronic transactions. The ITE Law states that electronic evidence is now legally recognized as admissible evidence in court. Given that procedural law serves as the foundation for court practice and is a legally binding formal rule, the Criminal Procedure Code's regulation of electronic evidence as admissible evidence is essential to achieving legal certainty in the ITE sector.

## CONCLUSION

Law Number 19 of 2016 Concerning Information and Electronic Transactions, specifically by quoting Article 184 of the Criminal Procedure Code, is the basis of evidence used in criminal cases involving information and electronic transactions. Because of the provisions of Article 184 of the Criminal Procedure Code, which include witness testimony, expert testimony, correspondence, and directions for the defendant's testimony, electronic evidence is essential to the prosecution of crimes involving information and transactions. Additionally, electronic information, electronic documents, and their prints are admissible forms of legal evidence according to Law Number 19 of 2016's Article 5 of the ITE Law.

## REFERENCES

Amajihono, K. D. (2022). Kekuatan Hukum Kontrak Elektronik. *Jurnal Panah Keadilan*, *1*(2), 128–139.
Amiruddin, H. Z. A. (2006). *Pengantar Metode Penelitian Hukum*.
Andi Sofyan, S. H. (2017). *Hukum Acara Pidana Suatu Pengantar*. Prenada Media.
Hamzah, A. (2005). *Pengantar Hukum Acara Pidana*.
Indonesia, P. R., & Indonesia, P. R. (1981). Undang Undang No. 8 Tahun 1981 Tentang: Kitab Undang Undang

Hukum Acara Pidana. *Sinar Grafika. Jakarta*.
Kaligis, O. C. (2012). *Penerapan Undang-Undang nomor 11 tahun 2008 tentang Informasi dan transaksi elektronik dalam prakteknya*. Yarsif Watampone.
Kawengian, T. A. (2016). Peranan Keterangan Saksi Sebagai Salah Satu Alat Bukti Dalam Proses Pidana Menurut KUHAP. *Lex Privatum*, *4*(4).
Koto, I. (2021). Hate Speech Dan Hoax Ditinjau Dari Undang-Undang Ite Dan Hukum Islam. *SOSEK: Jurnal Sosial Dan Ekonomi*, *2*(1), 48–56.
Marzuki, P. M. (2010). Penelitian Hukum, Kencana Prenada Group. *Jakarta. H*, *35*.
Raditio, R. (2014). *Aspek hukum transaksi elektronik: perikatan, pembuktian, dan penyelesaian sengketa*. Graha Ilmu.
Rintasari, D. N. (2020). *Keterangan Saksi Anak Sebagai Alat Bukti Dalam Perkara Pidana*. Skripsi, Universitas Muhammadiyah Magelang.
Samosir, C. D. (2013). A Handful of Criminal Procedure Law. *Nusa Aulia, Bandung*.
Samosir, D. (2013). *Segenggam tentang hukum acara pidana*. Segenggam tentang hukum acara pidana.
Soekanto, S. (2007). *Penelitian hukum normatif: Suatu tinjauan singkat*.
Sulistyo, H., & Ardjayeng, L. (2018). Tinjauan yuridis tentang perjudian online ditinjau dari undang-undang no 11 tahun 2008 tentang informasi dan transaksi elektronik. *Dinamika Hukum & Masyarakat*, *1*(2).
Unik, M., Larenda, V. G., & Mukhtar, H. (2019). Analisis Investigasi Android Forensik Short Message Service (SMS) Pada Smartphone. *JOISIE (Journal Of Information Systems And Informatics Engineering)*, *3*(1), 10–15.
Waluyo, B. (1992). *Sistem pembuktian dalam peradilan Indonesia*. Sinar Grafika.