Macrothink Institute™

International Journal of Culture and History
ISSN 2332-5518
2021, Vol. 8, No. 2

The Technology Revolution of The Criminal Jurisdiction Process Without Paper

Murshal Senjaya (Corresponding author)

Universitas Pasundan

Bandung, Indonesia

E-mail: socialscience897@gmail.com

Received: September 21, 2021 Accepted: October 31, 2021 Published: November 1, 2021

doi:10.5296/ijch.v8i2.19035 URL: https://doi.org /10.5296/ijch.v8i2.19035

Abstract

The technological revolution for the Paperless Criminal Court Process is that in the development of evidence as regulated in the Criminal Procedure Code, it can no longer accommodate developments in information technology; this creates new problems. This problem causes the form of printed media to be shifted to digital media (paperless). This shift makes a significant change in crime using computers because evidence of a crime that will lead to a criminal event is in electronic data. Either on the computer itself (hard disk/floppy disc) or printed out or in another form in the form of a trace (path) of a computer user activity. The judge is not related to the correctness of conformity embodied on the instructions as evidence because electronic evidence cannot stand alone to prove the defendant's guilt. Therefore, it needs to be supported by other evidence.

Keywords: technology revolution, criminal justice, paperless, Indonesia

1. Introduction

The rapid development of technology is changing various increasingly sophisticated and organized crimes, especially the regulation of electronic evidence in criminal procedural law in Indonesia, which is still limited. Even though it has been regulated in several laws, electronic evidence is still partial because it can only use electronic evidence in specific laws. However, the issuance of the ITE Law has accommodated electronic evidence that it can use in procedural law in Indonesia.

Article 5 paragraph (1) of the ITE Law states that electronic information or electronic documents or printouts are valid evidence. Furthermore, Article 5 paragraph (2) of the ITE

Law states that electronic information or electronic documents and printouts in paragraph (1) constitute an extension of valid evidence following the applicable procedural law in Indonesia.

However, in its development, the evidence as regulated in the Criminal Procedure Code can no longer accommodate developments in information technology; this raises new problems. This problem causes the form of printed media to be shifted to digital media (paperless). This shift makes a significant change in crime using computers because evidence of a crime that will lead to a criminal event is in electronic data. Either on the computer itself (hard disk/floppy disc) or printed out or in another form in the form of a trace (path) of a computer user activity (Makarim, 2005).

Of course, law enforcement efforts must not stop with the absence of laws regulating the use of evidence in the form of electronic information in settlement of a crime, especially general crimes, and corruption.

With the development of crimes using computers, investigators and public prosecutors and judges are faced with the existence of electronic evidence such as computer data, electronic documents, e-mails, and account transaction records (Harahap, 2005) so that evidence is not only limited to the testimony of witnesses, letters, experts, instructions, and statements of the defendant but includes information and documents stored electronically (Harahap, 2005).

Yahya Harahap revealed that the Judge was not related to the correctness of conformity embodied on the instructions as evidence because electronic evidence cannot stand alone to prove the defendant's guilt. Therefore, it needs to be supported by other evidence (Yuliearti, 2006).

Edmon Makarim presents electronic evidence as valid and independent evidence; of course, it must guarantee that a data recording is carried out following applicable procedures (calibrated and programmed) in such a way that the printout results are straightforward. data received in proving a case (Makarim, 2005).

The same thing was said by T. Nasrullah, who emphasized that electronic evidence such as SMS (short message service) only applies in special criminal law and does not apply to general criminal law. Meanwhile, a communication technology expert, Roy Suryo, stated that SMS could not be used as single evidence. The use of SMS as a means of evidence must be supported by expert statements (expertise) (Mansur, 2006).

In addition, the process of submitting and proving evidence in the form of digital data needs a separate discussion, considering that the evidence in the form of electronic information and the examination program files have gone through the digitization process with the process of typing checking, and storing by using a computer. However, the results are still printed on Paper (printing process). Therefore, it is necessary to have clarity on how to submit and carry out proving evidence in the form of digital data.

Proof of evidence in the form of digital data also concerns aspects of validation that are used as evidence because electronic evidence has unique characteristics compared to

non-electronic evidence; this unique characteristic is due to its form which is stored in electronic media, besides that electronic evidence can be easily engineered so that it is often its validity is doubtful (Volodino, 2003).

The development of information technology and computers is rapidly bringing progress and influence on human life. At this time, humans have felt that it cannot separate their lives from the presence of technology (internet). This has resulted in the emergence of a virtual community (virtual community) which is formed through communication that is woven in a computer network (interconnected computer network) (Latifulhayat, 2000).

The rapid development of e-commerce activities has multidimensional legal implications, which will have implications for two sectors: economy and law. In the economic sector, e-commerce provides opportunities for businesspeople to transact more quickly, effectively, and efficiently.

On the other hand, e-commerce in the legal sector raises various fundamental legal problems. The main problem related to e-commerce transactions in Indonesia is not the technological aspect, but rather the regulatory aspect (Warta Ekonomi, 2010), wherein electronic trading transactions (e-commerce) is the use of a digital signature (digital signature) in sending messages/data/offers of goods and services which are often preceded by the existence of an electronic contract.

The existence of an electronic contract has a different legal consequence. The contract is not carried out conventionally (paper face to face) but has used electronic media, causing a sense of insecurity in the implementation of the contract.

To overcome this, application technology is used in the form of information encryption (cryptography). Cryptography as a form of data security / electronic messages provides several information securities functions, one of which is a digital signature that can be used as evidence in criminal justice (Purbo & Wahyudi, 2007).

A digital signature, better known as a digital signature, is defined by the author as a signature made with mathematical equations that participate in transferring data/messages that are also made electronically.

In general, several types of cryptography contain digital signatures: First, conventional cryptography, for example, IDEA (International Data Encryption Algorithm) and DES (Data Encryption Standard). Second, public-key cryptography, for example, Elgamal discovered by Taher Elgamal, Third, Diffie-Hellman, DSA, the inventor is David Kravits, and finally, RSA, which was discovered by Ron Rivest, Adi Shamir, and Leonard Adleman.

The presence of digital signatures in an electronic transaction activity is a direct result of a shift in the trading system, where trade in the past was more often paper-based. But now, it has turned into paperless (paperless); besides that, it can be used as evidence in procedural criminal law.

This shift has caused differences between the two, namely: paper-based criminal court evidence of various frauds is often encountered, where signatures can still be faked, and it

can change paper documents, even stamps, code impressions, stamp marks, and seals that should be safe can still be faked.

Even the conventional signature function is only as recognition and acceptance of the contents of the information with the signature, while on the other hand, in non-paper-based criminal justice, digital signatures cannot be faked; they can even have dual functions, namely guaranteeing the authenticity and integrity of data/message at the same time also briefly shows the contents of the data/message regarding the identity of the signer during the transmission process.

Legal problems arise when there is a criminal case involving the authenticity of data/messages, which are usually in the form of a digital signature in front of the court as evidence. Whereas in criminal law electronically, a digital signature is not in a written form (actual) as a conventional signature on a particular document/deed, but in a mathematical equation made digitally. Usually, when a case occurs, then in a criminal case trial, paper as a company document is written evidence as to the primary evidence. Because, in criminal law traffic, people deliberately provide evidence that they can use in a criminal case and the evidence provided is usually in the form of writing. The formulation of the problem in this research is how The Revolution of Paperless Criminal Court Process Technology?

2. Overview Theory

2.1 Digital Resolution

Digital Revolution is a change from mechanical technology and analog electronics into digital technology that has been happening since 1980 and continues to this day. Revolution was initially triggered by a generation of teenagers born in the 80s. Analogous to the agricultural revolution, the Industrial Revolution, the digital revolution marks the beginning of the Information age.

This digital revolution has changed the way a person looks at living a very worldly life today. A technology that is making significant changes to the whole world, from helping to simplify matters to creating problems because they cannot correctly and correctly use this increasingly sophisticated digital facility. The following is a brief history of the Digital Revolution in the development of world technology.

Technology was found in 1980 and became economical to be widely adopted after the invention of the Personal Computer. Previously converted digital revolution technology was analog into a digital format. For example, in digital communication, hardware repeats the ability to amplify a digital signal and pass it on without losing information in the signal.

Equally crucial as revolution is the ability to quickly transfer digital information between media and access or distribute it remotely. A computer is an electronic system for manipulating data quickly and precisely. It is designed and organized to receive and store input data automatically, process it, and produce output under the supervision of a program instruction step and stored in memory (program storage). Electronic data processing (PDE) or Electronic Data Processing (EDP), processing data using a computer. Data processing is

manipulating data into a more valuable and meaningful form of information using an electronic device, namely a computer.

The computers we use today did not just appear out of nowhere but went through a long process of evolution. The emergence of computers may be seen in historical flashbacks since their useAbacus - found in Babylon (Iraq) 5000 years ago - as the first manual calculation tool, both in schools and among traders, at that time.

In the next period, it found many similar mechanical calculating tools, namely Pascaline found by Blaine Pascal in the year 1642, Arithometer by Charles Xavier Thomas de Colmar in the year 1820, Babbage's Folly by Charles Babbage in the year 1822, and by Hollerith Herman Hollerith in the year of 1889. All of them are still entirely without electric power. The size and complexity of the structure are based on the level of operation of the calculations performed. Only in the years1940, the new era of electric computers begins with the invention of the electric computer that applied the Boolean algebra system.

In the decade 1980-an computers are becoming familiar machines to the public in developed countries, and millions of people buy computers for home use, including 17 million Commodore 64 myself between the years 1982 and 1994.

The more sophisticated digital technology present is making significant changes to the world. The more advanced the birth of various digital technology has emerged and pushed the shift known as digital transformation. Various groups have facilitated access to information in many ways and can enjoy the facilities of digital technology freely and under control. But it is unfortunate that with the development of technology, more crimes are detected.

Therefore, everything must have protection Copyright and control children and adolescents in particular. So many online games cause mental damage to the child, so pornography and copyright infringement are also violated.

2.2 Indonesian Criminal Justice System with Digital Technology

The South Jakarta District Court has conducted general criminal proceedings online or via teleconference using the zoom application with the defendant in the detention center. The implementation of E-Court is positive and progressive for the judiciary in Indonesia because it has begun to be established. "Fast, simple and low cost, this is a very positive concept for the future.

Another positive thing that it can learn from the digital trial is that it can save time because you don't have to wait for the accused to come to court. This must be continued by the Supreme Court so that it can continue in the future. Adjustments can be made other than in the District Court.

For example, in the legal process at the Police or the Corruption Eradication Commission (KPK), they have also conducted an E-Court before.

The digital justice system can be sustainable and integrated, not only in trials but all cases can apply an online system. However, the defendant had to attend the trial in person regarding

trials that needed further regulation and had heavy equipment that required specific evidence. "Of course, for example, in reading the charges or in the verification process, documents can still be digital, but if we present evidence, we must point out the implementation so that there is no distortion error.

The implementation of the trial by e-Court has a basis; the Supreme Court also has the authority to regulate the technical judicial process of the court. Second, in the development of the judicial system, there is currently a strong desire to reform the justice system into the short-term 2020 agenda. Implementing the SPPT (integrated criminal justice system) between the Police-Attorney-General's Office (KPK) -Justice -Institutions starting from administration in integrated handling of criminal cases, the broad framework already exists.

So, the Supreme Court needs to issue guidelines in what cases the trial can be carried out by E-Court and at any stage of the trial. "The prosecutor's office made prosecution guidelines following the judicial guidelines made by the Supreme Court, and so did the Police and the KPK. So, the judiciary will run orderly, and there will be no distortion in its implementation.

3. Discussion

Criminal Law is one of the means owned by the state in carrying out the obligation to protect the rights of every citizen to gain a sense of security, especially against the threat of crime. Compared to other laws, this criminal Law has unique characteristics that lie in stringent sanctions, namely sorrow.

Therefore, the criminal law system must always be evaluated, reconstructed, harmonized, and actualized carefully and precisely through a thorough understanding and thought so that, on the one hand, it is reliable in anticipating the development of crime. Still, on the other hand, it does not threaten human rights, dignity, and dignity (Wisnubroto, 2011)

As it is known that the criminal law system is based on a penal system that consists of three main pillars, namely, criminal acts (legality principle), criminal responsibility (principal guilt), and Criminalization.

In the Criminal Code, which applies as positive Law in Indonesia at this time (WvS), the three main pillars of the criminal system are still oriented towards the physical paradigm (hard reality). Even though the principles contained in the General Rules of the Criminal Code are very much needed as an operational basis in the application of regulations regarding offenses, both those contained in the Criminal Code and those scattered in various special criminal law laws, if they are not explicitly regulated.

As a result, the current positive criminal Law becomes challenging to reach the development of based crime cases Hight-tech which is increasing and has a non-physical paradigm (Wisnubroto, 2011).

In the field of criminal Law, an analogy is not part of the interpretation because it is known that in criminal Law, there are fundamental principles that reflect the primary nature of criminal Law philosophically, namely: the principle of legality/legalism (Principle of Legality) which is also known as Nullum Delictum Principle (Nullum Crimen), namely the principle

that determines that no act is prohibited and is punishable by punishment if it is not determined in advance in the legislation.

Anselm von Feuerbach formulated the legality principle, which is arranged in one sentence: "Nullum crimen, nulla poena sine praevia lege" (There is no criminal act, no punishment without prior statutory provisions) (Wisnubroto, 2011). Regarding the legality principle in technology, criminal law, this is like what Moeljatno said, which said that the fundamental basis for imposing a criminal on a person who has committed a criminal act is an unwritten norm. And people are acquitted if there is no mistake. This primary matter is about the responsibility of a person for the actions he has done. So, regarding criminal responsibility or criminal liability.

Usually, this legality principle is meant to contain three definitions (Moeljato, 2008): no act is prohibited and punishable by punishment if it has not previously been stated in law, it cannot use an analogy to determine the existence of a criminal act. The rules of criminal Law are not retroactive.

In general, the function of Law is to realize an orderly coexistence in such a way that this condition can support the development of the individual human being in achieving his life goals. In essence, the function of Law is to maintain public interests in society, protect human rights, and create justice in living together in society (Huijbers, 2008).

In connection with the function of Law, Lawrence M. Friedman argues that the function of Law is as a means of social supervision or control (social control), dexterous settlement (dispute settlement), and social engineering (social engineering, redistributive, innovation) (Abidin, 2007).

Meanwhile, according to Soerjono Soekanto, the function of Law is to provide guidance to the community on how they should behave and behave, maintain the integrity of society, provide guidance on society to exercise social control (Soekanto, 2003).

Based on Article 1 of the Criminal Code, it can be concluded that there is a legality principle in criminal Law in Indonesia. The legality principle is a general principle that prioritizes the qualification of a criminal act which must be stated in the legislation beforehand. If the act has been determined, then every person who fulfills the elements stipulated in the statutory regulations then the act can qualify as a criminal act and can be sentenced.

The principle of legality, which is fully formulated in Latin is nullum crimen sine lege and Nulla poena sine lege recognized as a basic principle of criminal Law in liberal capitalist and socialist countries, including by the Indonesian Criminal Code (Abidin, 2007).

According to Moeljatno, it has been said that the basic basis for punishing a person who has committed a criminal act is an unwritten norm. Not sentenced if there is no mistake. This basis is about someone's responsibility for the actions he has done.

Regarding the prohibition and threat of an act, namely regarding his own criminal act, concerning criminal act, there is also a main basis, namely, the principle of legality (principle of legality), the principle which determines that no act is prohibited and punishable if it is not

determined in advance in the legislation (Moeljatno, 2008).

The principle of legality means demanding that the provisions of statutory regulations be legally stipulated. After that, an act committed by a human being proven to fulfill the elements of a criminal act can be punished. Thus, in this principle it can be concluded that statutory regulations cannot be applied retroactively, so that this becomes a guarantee of legal certainty (Kartanegara, 2006).

The ITE Law also adheres to the legality principle (as a fundamental principle in criminal Law), namely as seen in Article 54 paragraph (1) that this Law comes into force on the date of promulgation. This means that the criminal provisions contained in the ITE Law will be implemented after they come into effect since April 21, 2008 (Widodo, 2013).

The principle of legality is very crucial in determining whether an act is categorized as a criminal act or not, especially in a technology crime whether it is a legal problem or an ethical problem. So, the role of the legality principle as an initial basis in determining the conduct of a criminal act is needed.

Article 184 of the Criminal Procedure Code regulates valid evidence, namely:

a) Witness statements

b) Expert statement

c) Letter

d) Instructions

e) Statement of the defendant

The arrangement of electronic evidence must be based on the system and principles of proof of criminal procedure law in effect in Indonesia. The legal definition of proof is a part of the criminal procedure law which regulates various types of evidence which are valid according to Law, the system adopted in the evidence, the requirements, and procedures for submitting the evidence and the judge's authority to accept, reject and judge evidence (Sasangka & Rosita, 2003).

Where the legal sources of proof in this case are laws, doctrine, or teachings, as well as jurisprudence. And what is meant by evidence is everything that has to do with an act, where the evidence can be used as evidence to give the judge confidence in the truth of a criminal act that has been committed by the defendant (Sasangka & Rosita, 2003).

KUHAP has not explicitly regulated valid electronic evidence. However, about the legality of electronic evidence in the criminal justice system, this is related to the existence of a legality principle which states that in Law Number 11 of 2008 concerning Electronic Information and Transactions included in Article 54 paragraph (1), data is used. electronics can be used as valid evidence.

The ITE Law legally regulates this matter. This is indicated in the Letter of the Supreme Court to the Minister of Justice Number 39 / TU / 88/102 / Pid dated January 14, 1988,

stating "microfilm or microfiche can be used as valid evidence in a criminal case in court to replace documentary evidence, provided that the authenticity of the microfilm is previously guaranteed which can be traced back from registration or minutes (Sitompul, 2012).

The legality of electronic evidence in the ITE Law is regulated in CHAPTER III concerning Information, Documents and Electronic Signatures, as well as Article 44 of the ITE Law. Article 5 of the ITE Law is stated, namely:

Electronic Information and or Electronic Documents or printouts thereof are valid legal evidence. (2) Electronic Information and / or Electronic Documents and their printouts as intended in paragraph (1) are extensions of valid evidence in accordance with the applicable Procedural Laws in Indonesia.

Electronic Information and Electronic Documents are declared valid if using Electronic Systems in accordance with provisions regulated in this Law.

Provisions regarding Electronic Information and Electronic Documents as intended in paragraph (1) do not apply to: 1) Letters which according to the Law must be in writing, and 2) Letters and documents which according to the Law must be made in the form of a notarial deed or a deed by the deed-making official.

In the Criminal Justice System, especially electronic evidence, this is very important and very much needed to become evidence of a crime committed by the perpetrator and proven in the Criminal Court. The relationship between this electronic evidence and the Criminal Justice System, especially in the function of the Criminal Justice System, has two major goals, namely, to protect the public and enforce the Law.

Looking at the functions of the criminal justice system above, electronic evidence is very useful and useful, to review the legality of measures of prevention and prosecution and to provide court decisions that determine the guilt or innocence of the defendant at trial, using the electronic evidence as evidence that the defendant committed the crime that was prosecuted by the law enforcement apparatus.

It is stated that one of the material requirements of electronic evidence to be accepted in court is that an electronic information or document must be guaranteed its availability, integrity, authenticity. In an electronic transaction, there will be so much information that is recorded or recorded on many tools and devices. Electronic information or electronic documents, if not handled properly, can be changed, damaged, or lost.

Association of Chief Police Officers (ACPO) provides four principles in handling electronic evidence, namely: First, all handling of electronic evidence (i.e., data obtained from computers or storage media, or other electronic tools and devices) by law enforcement officials must not result in changes or damage to the data so that it can be accepted in court.

Second, in circumstances where someone must access original data that contained in a computer or storage media, the person in question must have the competence to do so and must be able to provide an explanation of the relevance of his actions to the data and the consequences of his actions.

Third, that there must be clear procedures and processes in place for collecting and analyzing electronic evidence. The procedure referred to includes handling of electronic evidence starting from the discovery of evidence containing electronic evidence, wrapping of evidence, examination, analysis, and reporting.

Fourth, a party or official must ensure that the implementation of activities follows the laws and regulations and all the processes and procedures referred to another thing that needs to be considered in collecting evidence that stores electronic evidence is that many types of tools and media store information.

Given that there are so many information storage media and technology types, their handling also has their respective characteristics. In general, digital forensics is divided into (Al-Azhar, 2004):

Computer forensics is carried out on computers, laptops, or hard drives, and similar storage media.

- Mobile forensics, namely forensics carried out on cell phones.
- Network forensics, namely forensics carried out on computer networks.
- Audio forensics, namely forensics that is carried out on sound.
- Image forensics, namely forensics that is carried out on images.

Video forensics, namely forensics carried out on video and CCTV. Based on the ACPO principles mentioned above. The principle of digital forensics is divided into three stages, namely (US Department of Justice taking, 2004) (acquisition), examination and analysis, and documents and presentations. Regarding retrieval, given its nature that cannot be changed, destroyed, or eliminated if not appropriately handled, information retrieval of electronic document data must be carried out by maintaining and protecting its integrity or integrity.

In terms of examination and analysis, examining actual electronic evidence generally uses hardware and software specifically made for digital forensic purposes. Examination performs extraction, which takes all data from the media data stored, including data that has been previously deleted.

The examiner also uses a write blocker, namely a tool used to prevent writing to original data. Examination of the copy of the original electronic evidence can also make a copy of the electronic evidence as work material. Finally, concerning documents and presentations, it must document every action taken in collecting and examining electronic evidence accurately and thoroughly.

Not only actions in carrying out digital forensics, but also actions related to it, for example, receiving a computer from the officer who took the goods at the case scene to the forensic examiner. The report can contain the processes and stages carried out in the inspection, including the tools and equipment used. In addition, the report also needs to contain information about all data obtained and data relevant to a criminal act.

Improper handling of a running computer can lose volatile electronic information. Not being labeled when removing cables attached to the computer will make it difficult for digital forensics to conduct examinations and analyses.

In collecting electronic evidence, investigators will find a variety of information, both relevant and irrelevant. Investigators must maintain the confidentiality of information, especially information related to someone's privacy that is not relevant to a criminal act.

4. Conclusion

The Revolution in the Technology of the Paperless Criminal Court Process is that in the development of evidence as regulated in the Criminal Procedure Code, it can no longer accommodate developments in information technology; this raises new problems. This problem causes the form of printed media to be shifted to digital media (paperless). This shift makes a very significant change in crime using computers because evidence of a crime that will lead to a criminal event is in the form of electronic data, either on the computer itself (hard disk/floppy disc) or printed out or in another form in the form of a trace (path) of a computer user activity. The judge is not related to the correctness of the conformity embodied on the instructions as evidence because electronic evidence cannot stand alone to prove the defendant's guilt. Therefore, it needs to be supported by other evidence.

References

Ahsan, D. M. (2006). SMS as Evidence, Merapi Newspaper, April 13.

Aloysius, W. (2011). *Telematics Criminal Law Concept.* Atma Jaya University, Yogyakarta.

Andi, Z. A. (2007). *Criminal Law Part One.* Alumni, Bandung.

Arie, E. Y. (2006). Electronic Evidence in Computer Crime: A Study on Corruption Crime and Indonesian Criminal Law Reform, Regular Postgraduate Thesis, Faculty of Law, University of Indonesia, Jakarta.

Atip, L. "Cyber Law is Urgency for Indonesia", Paper presented in a Day Seminar on Cyber Law 2000, Organized by the Cipta Bangsa Foundation Grand Hotel Preangef, Bandung, 29 July 2000, See also AW Branscomb, "Common Law for the electronic frontier", Scientific American, Vol. 165, 1991.

Edmom, M. (2005). *Introduction to Telematics Law: A Compilation of Studies.* PT Raja Grafindo Persada, Jakarta.

Harahap, M. Y. (2005). *Discussion of Problems and Application of the Criminal Procedure Code: Court Session Examination, Appeal, Cassation, and Review.* Sinar Grafika, Jakarta.

Hari, S., & Lily, R. (2003). *Law of Evidence in Criminal Cases.* Mandar Maju, Bandung.

Josua, S. (2012). *Cyberspace Cybercrime Cyberlaw Aspects of Criminal Law.* Tata Nusa, Jakarta.

Lawrence, M. F. (2004). American Law, WW Norton & Co, New York.

Moeljatno, Principles of Criminal Law, Revised Edition, Rineka Cipta.

Muhammad Nuh Al-Azhar, Digital Forensic Practical Guide to Computer Investigation.

Ono, W. P., & Aang, A. W. (2007). Getting to Know E-Commerce, PT. Elex Media Computindo, Jakarta.

Satochid Kartanegara. (2006). Criminal Law, Student Literature Hall, Bandung.

Soerjono Soekanto. (2003). Principles of Legal Sociology, Raja Grafindo Persada, Jakarta.

The Huijbers. (2008). Philosophy of Law in Historical Trajectory, Kanisius, Jakarta.

US Department of Justice. (2004, April). Forensic Examination of Digital Evidence: Guide for Law Enforcement.

Volodino, L. (2003). Electronic Evidence and Computer Forensic. *Communication of AIS, 12.*

Widodo, Apek Mayantara Crime Law, Aswaja Pressindo, Yogyakarta, 2013.

Copyrights