RLJ Ratio Legis Journal
ISSN 2830-4624
published by
Master of Law, Faculty of Law
Universitas Islam Sultan Agung
Volume 3 No. 1, March 2024

The Urgency of Electronic Evidence Validation by Judges in Digital Forensic Examinations

Gatot Sarvadi
Faculty of Law, Sultan Agung Islamic University, Semarang, Indonesia, E-mail: Gatotsarwadi.std@unissula.ac.id

Abstract: *The aim of this research is to determine and analyze the judge's methods in carrying out digital forensic examinations in analyzing electronic evidence in court. In this writing the author uses a normative juridical method with research specifications in the form of descriptive analysis. The use of computers as a medium to commit crimes has its own level of difficulty in proving it. Handling often requires forensics, which is an activity to carry out investigations and determine facts related to criminal incidents and other legal issues. Digital forensics is the application of computer science and technology for the purposes of legal evidence, which in this case is to prove high-tech crimes scientifically so that digital evidence can be obtained that can be used to identify the perpetrator of the crime. The material requirements for electronic evidence are regulated in Article 6, Article 15 and Article 16 of the ITE Law, which in essence, electronic information and documents must be able to guarantee their authenticity, integrity and availability. To ensure the fulfillment of the material requirements referred to in many cases, digital forensics is needed.*

Keywords: *Digital; Electronics; Evidence; Forensics; Judge.*

1. Introduction

Indonesia is a country based on law, this statement is contained in the Explanation of the 1945 Constitution of the Republic of Indonesia which states that "The State of Indonesia is based on law (rechtstaat) and not based on mere power (machtstaat)."[1], as a country based on law, Indonesia has a series of regulations or laws so that the interests of the community can be protected.[2]Paragraph 4 of the Preamble to the 1945 Constitution of the Republic

[1]Anton Susanto, Ira Alia Maerani, and Maryanto, Legal Enforcement by the Police against Child of Criminal Doer of a Traffic Accident Who Caused Death (Case Study in Traffic Accident of Police Traffic Unit of Cirebon City Police Juridiction), Jurnal Daulat Hukum, 3 (1), (2020), p 21
[2]Asep Sunarsa, (2018), Attorney Role In Fighting Crimes Of Motorcycle Gang In Cirebon, Jurnal Daulat Hukum, 1. (2), p 453

of Indonesia, which is the constitutional basis of this country, states that one of the goals of the state is to create general welfare. So all efforts and development carried out by this country must be directed towards this goal so that people's welfare is created.[3]

The law that determines what must be done and what must not be done or is prohibited. The target of the law is not only people who actually act against the law, but also legal acts that are likely to occur, and to state apparatus to act according to the law. The working system of the law in this way applies one of the

forms of law enforcement that apply in Indonesia.

In the era of the Industrial Revolution 4.0, the law must be able to respond to the development of information technology, even though the law can hardly keep up with its speed. Satjipto Rahardjo, said that "the law is for humans, not humans for the law" meaning that if the law is no longer appropriate, then it is not humans who must be forced to adjust to the law, but the law that must be adjusted to the development of human needs.[4]

In the current era of globalization, information has placed Indonesia as part of the world's information society, thus requiring the establishment of regulations regarding the management of information and communication transactions at the national level so that the development of information technology can be carried out optimally, evenly, and spread to all levels of society in order to educate the life of the nation and state. Computers or mobile phones are one of the causes of social change in society, namely changing their behavior in interacting with other humans, which continues to spread to other parts of human life, so that new norms, new values, and so on emerge.[5]

The use of this technology is not limited to its use in society, but can also be used by law enforcement as a means of carrying out their duties. The technological approach has actually helped law enforcement in uncovering various cases. This electronic technology is used in providing evidence. The technological approach to evidence still needs to be studied as well as how to apply it to the legal mechanism in Indonesia.

In judicial practice, the Judge's attitude in viewing evidence in criminal cases refers to the Criminal Procedure Code, while in civil cases it is guided by the HIR, RB and the Civil Code. However, after the enactment of Law Number 8 of 2011 concerning Electronic Information and Transactions (UU ITE), the Judge's attitude in viewing electronic document evidence can vary, namely some argue that

[3]Sri Praptini, Sri Kusriyah, and Aryani Witasari, (2019), Constitution and Constitutionalism of Indonesia, Journal of Legal Sovereignty, 2 (1), p 7

[4]Supandi, (2019). Modernization of State Administrative Courts in the Era of Industrial Revolution 4.0 to Encourage the Progress of Indonesian Legal Civilization, Semarang: Undip Press, p 17-18

[5]Dikdik M. Arif Mansyur, and Elisatris Gultom, (2005), CYBER LAW Legal Aspects of Information Technology, PT. Refika Aditama, Bandung, p 3.

electronic document evidence as valid evidence is as an additional conventional evidence in Procedural Law. However, there arealso those who are of the opinion that electronic documents are supporting evidence that must be supported by other evidence to increase the judge's confidence.

The Supreme Court itself is aware that electronic evidence is still unfamiliar to Judges, considering that many Judges, especially senior Judges, are not yet familiar with the use of information technology. Regarding electronic evidence, until now there has been no explicit obligation for Judges to ensure the authentication of electronic evidence with a certain mechanism, both in terms of procedural law and directions from the Supreme Court. The fundamental question regarding electronic evidence is to what extent Judges can ensure its authentication or authenticity. There are no provisions that provide guidelines for Judges on how Judges can authenticate electronic evidence from the beginning when it is obtained until it is submitted to the trial so that it can be accepted as valid evidence.

Based on the description of digital forensic evidence as mentioned above, the author conducted research related to digital forensic evidence as material for the trial process in court withresearch objectives forknowing and analyzing the urgency of validating electronic evidence by judges in implementing digital forensic examinations in analyzing electronic evidence in court.

2. Research Methods

The approach used in this study is normative juridical or written legal approach (statute approach). Given that the problems studied and reviewed adhere to the juridical aspect, namely based on norms, regulations, legislation, legal theories, opinions of legal experts. In normative legal research, law is conceptualized as a rule or norm that is the basis for human behavior that is considered appropriate. This research is categorized as normative research because it examines library materials against secondary data sourced from library materials.

3. Results and Discussion

3.1. Electronic Evidence

Along with the development of information and telecommunication technology, in its development now known electronic evidence such as electronic information, electronic data/documents, witness examination using teleconference, microfilm containing recordings of company documents in addition to other evidence such as radio cassette recordings, VCD/DVD, photos, facsimiles, CCTV recordings, even SMS/MMS.

Photos (portraits) and sound or image recordings (including CCTV recordings), based on literature, cannot be used as evidence because they may be the result of engineering so they cannot prove what actually happened. However, in today's development, with advances in technology in the field of information and

telecommunications, whether a photo and sound or image recording is genuine or not can be determined using certain techniques.

The Supreme Court of the Republic of Indonesia in its letter to the Minister of Justice dated January 14, 1988 No. 39/TU/88/102/Pid, expressed its opinion that microfilm or microfiche can be used as valid evidence in criminal cases in court, replacing written evidence, with the proviso that the microfilm's authenticity is previously guaranteed, which can be traced back from the registration or minutes. In terms of formal legality, the law of evidence in Indonesia (in this case procedural law as formal law) both HIR/Civil Code and Criminal Code have not accommodated electronic documents as evidence, while several new laws have regulated and recognized electronic evidence as valid evidence, namely in: Law No. 8 of 1997 concerning Company Documents, Law No. 36 of 1999 concerning Telecommunications, Law No. 40 of 1999 concerning the Press, Law No. 31 of 1999 in conjunction with Law No. 20 of 2001 concerning the Eradication of Criminal Acts of Corruption, Law No. 19 of 2002 concerning Copyright, Law No. 30 of 2002 concerning the Corruption Eradication Commission, Law No. 24 of 2003 concerning the Constitutional Court, and Law No. 11 of 2008 concerning Electronic Information and Transactions.[6]

3.2. Digital Forensics

Digital forensics is different from forensics in general. Digital forensics or computer forensics is the collection and analysis of data from various computer resources, including: Computer systems, computer networks, communication lines (including physical and wireless), and also various storage media that are considered worthy to be submitted in court. Digital Forensics is a field of science that combines two fields of science, law and computers.[7]

Definition according to HB Wolfre which explains that Digital Forensics is: "A methodological series of techniques and procedures for gathering evidence, from computing equipment and various storage devices and digital media, that can be presented in court of law in coherent and meaningful full format". If interpreted freely "A methodological series of techniques and procedures for gathering evidence, from computing equipment and various storage devices and digital media, that can be presented in court of law in a coherent and meaningful full format".

According to Noblett, digital forensics is the process of retrieving, preserving, returning, and presenting data that has been electronically processed and stored on computer media. Fourth, according to Judd Robin, it is the simple application of computer investigation and analysis techniques to determine possible legal

[6]Insan Pribadi, (2018), Legality of Electronic Evidence in the Criminal Justice System, Lex Renaissance, 1 (3), p 117

[7]Feri Sulianta, (2008), Computer Forensics, Elex Media Komputindo, Jakarta, p 3.

evidence.[8]According to Judd Robin, it is a simple application of computer investigation and analysis techniques to determine possible legal evidence. Fifth, according to Marcella, digital forensics is an activity related to the maintenance, identification, retrieval/filtering, and documentation of digital evidence in computer crimes. This term is relatively new in the field of computers and technology, but has emerged outside the term technology (related to the investigation of intelligence evidence in law enforcement and the military) since the mid-1980s.

3.3. Urgency of Validation of Electronic Evidence by Judges in the Implementation of Digital Forensic Examination in Analyzing Electronic Evidence in Trial

Even though the legal rules for a case are not legally binding or are unclear, the judge may not reject it. The judge must examine and try the case submitted to him, because the judge is considered to have sufficient legal knowledge. The judge must be able to interpret the law that is not legally binding or unclear in writing.

According to Muslihin Rais, "The judge's decision essentially contains all activities or judicial processes in the context of resolving a case that has been completed since the beginning of the case examination. From the series of judicial processes, not a single judicial decision can determine the rights of a party and the burden of obligations of another party, the validity of an action according to law and place obligations to be carried out by the parties in the case because among the judicial processes, only the decision has consequences for the parties.[9]

The judge can determine which evidence is prioritized for use in the proof and the strength of each piece of evidence submitted. Thus, the judge is bound by these provisions to determine that a legal fact is considered true. Without fulfilling the provisions of the minimum requirements for evidence, a fact must be set aside and considered irrelevant in deciding a case.

Current criminal acts also utilize sophisticated technology and information (cybercrime) in their criminal modus operandi, such as using email in communicating and using social media applications in sending documents related to a crime. The involvement of complex information technology as a mode of crime is often revealed in various trial processes. Thus, judges as law

[8]I Made Wiryana MSc, (2008), SAFFA-NG Forensic Case Management Architecture System. Indonesian Journal of Legal and Forensic Sciences, 1 (1), p 41

[9]H. Muslihin Rais, (2017), The Value of Justice in Judges' Decisions in Corruption Cases, Al-Daylah Journal, 6 (1), p 127.

enforcement elements are required to understand well the forms of cybercrime and how to anticipate them.[10]

In the process of proving a case, electronic evidence obtained or changed in an unlawful manner must be watched out for, because it has the potential to make the legal facts used as the basis for the decision unclear. Thus, it can be concluded that validation of electronic evidence is an absolute requirement that cannot be ignored in the process of proving considering the role of electronic evidence is very vital in determining the truth of the decision as the final product of the examination of a case.

In order to support the judge's role and duties in the evidentiary process at trial and to gain the judge's confidence regarding the evidence submitted, especially electronic evidence, knowledge and understanding of the process of obtaining it, examining it, storing it until submitting it is needed in its entirety and its validity is maintained so that can make a case clear so that it can be used as evidence in deciding the case.[11]

Judges cannot rely on invalid and invalid evidence, and judges cannot decide a case without sufficient evidence. So that the validation of electronic evidence is a vital stage and the first step in finding the truth of a disputed problem. This is where the process of validating electronic evidence finds its urgency.

Article 1 number 1 of the ITE Law states that electronic information is one or a collection of electronic data, including but not limited to writing, sound, map images, designs, photos, electronic data interchange (EDI), electronic mail (email), telegrams, telex, telecopy or the like, letters, signs, numbers, access codes, symbols or perforations that have been processed which have meaning or can be understood by people who understand them.

In order to be accepted in court, electronic evidence must meet the formal and material requirements as stipulated in the ITE Law. Regarding these requirements, Article 5 paragraph (4) of the ITE Law stipulates that the formal requirements of electronic information or electronic documents do not include documents or letters that according to the law must be in written form. Meanwhile, regarding the material requirements, the provisions of Articles 6, 15 and 16 of the ITE Law stipulate that electronic information or documents must be guaranteed for their authenticity, integrity and availability. To ensure that these material requirements are met, digital forensics are needed in many cases. By fulfilling these requirements, emails, chat recording files and various other documents can be used as valid evidence.

[10]Handrizal, Handrizal, (2017), Comparative Analysis of Puran File Recovery Toolkit, Glary Undelete and Recuva Data Recovery for Digital Forensics. J-SAKTI (Journal of Computer Science and Informatics), 1 (1), p 84

[11]Goddess Asimah. (2020), To Overcome The Constraints of Evidence in The Application of Electronic Evidence. Peratun Law Journal, 3(2), p 102

In fully digital evidence, of course, validation of evidence cannot be done in such a way as in conventional evidence. There are at least four principles that underlie the entire series of activities in handling electronic evidence so that the evidence can be valid to be submitted to court:

1) The principle of maintaining data integrity. Maintaining data integrity by maintaining every action taken on electronic evidence by not changing or damaging the data stored in it;
2) Principle of competent personnel. Personnel handling original electronic evidence must be competent, trained, and able to provide explanations for every decision made in the process of identifying, securing, and collecting electronic evidence.
3) Audit trail principle. An audit trail or chain of custody (CoC) must be maintained by recording every action taken on electronic evidence. This aims to ensure that the evidence will produce the same results as those obtained by the previous investigator/forensic analyst.
4) Principle of legal compliance. Personnel responsible for handling cases related to the collection, acquisition, examination and analysis of electronic evidence must be able to ensure that the ongoing process is in accordance with applicable laws and the previous basic principles.[12]

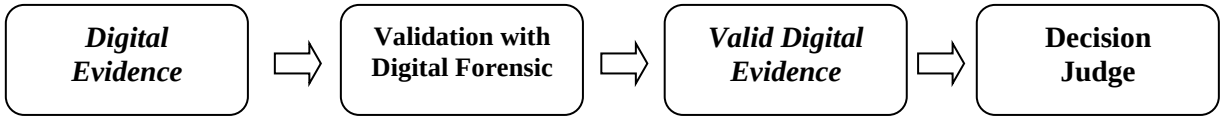
The issue of the validity of electronic evidence is a fundamental matter that needs to be considered in the presentation of electronic evidence in court. The judge is obliged to assess the authentication of the submitted electronic evidence by examining the evidence through:

a) Assess the condition of evidence and the integrity of electronic evidence;
b) Testing its relevance to the facts;
c) Checking conformity with the case report;
d) Assessing the role of electronic evidence in the chronology of the case (reconstruction);
e) The relationship of electronic evidence to other evidence and testimony;
f) The process of obtaining and handling electronic evidence can be accounted for professionally.

Thus, in order to fulfill the material requirements for electronic evidence

as determined by law, a digital forensic mechanism must be implemented for electronic evidence as part of the validation mechanism itself to make electronic evidence (digital evidence) into valid electronic evidence (valid digital evidence).

[12]Santhos Wachjoe P, (2016), Use of Electronic Information and Electronic Documents as Trial Evidence, Journal of Law and Justice, 5 (1), p 13



The components of digital forensics are generally almost the same as other fields. These components include people, equipment and protocols that are arranged, managed and empowered in such a way as to achieve the final goal with all feasibility and quality.[13]

The validation procedure for electronic evidence is largely determined by the type of electronic evidence submitted. The ITE Law groups these into two parts, 1) electronic information and/or electronic documents become electronic evidence (digital evidence), while printouts of electronic information and electronic documents become written evidence. The validation process through digital forensics is carried out through strict and thorough stages to ensure the validity and truth of the evidence. Judges may only base their legal considerations on validated electronic evidence (valid digital evidence). The validation process will ultimately be stated in the legal considerations of the decision as the core product and final product of the court. The description of the electronic evidence includes three main points, namely 1) the results of the validation of electronic evidence submitted by the parties and its conditions, 2) the relevance of electronic evidence to the facts (relevance principle), and 3) legal determination based on references to electronic evidence.

As for the preference of the stages through expert testimony in digital forensic evidence in terms of the judge's need to strengthen the analysis of his decision. The criteria for digital forensic experts in Indonesia are currently not detailed in the legislation. The provisions related to this expert are only found in the explanation of the ITE Law Article 43 paragraph (5) letter h which reads: "What is meant by "expert" is someone who has special expertise in the field of Information Technology who can be accounted for academically and practically regarding his knowledge."

The thing to note is that the expert opinion cannot stand alone, its function and quality add to other evidence, namely if the existing evidence has reached the minimum limit of proof and its evidentiary value is still not strong enough, in this case the Judge is allowed to take expert opinion to increase the value of the existing evidentiary strength. So that in terms of proving electronic evidence, when the Judge has not been able to determine the authenticity/originality of the evidence, an expert can be used to help prove it.

The results of a digital forensic test are the results of a forensic test. The results of a forensic test refer to a form of report on the results of a digital evidence analysis carried out by a digital forensic expert on digital evidence. Regarding the results of this digital forensic test, it is based on Article 46 of the Regulation of the Minister of Communication and Information Technology Number 7 of 2016 concerning the Administration of Investigation and Prosecution of Criminal Acts in the Field of Information Technology and Electronic Transactions. The results of

[13]Ruci, Meiyanti, and Ismaniah. (2015), Development of Digital Forensics. UBJ Scientific Study Journal, 15 (2), p 232

a digital forensic test according to doctrine are also included in the realm of experts, because they are the results of an expert's analysis based on formal education, expertise, and can be related to his position and field of service. The results of this forensic test will be presented in court by an expert. In the explanation of Article 186 of the Criminal Procedure Code, expert testimony can also be given during the examination by investigators or public prosecutors which is stated in the form of a report and made with the oath at the time he received the position or job. The results of the digital forensic test issued by the National Police forensic laboratory are in the form of a Criminalistic Laboratory BAP. The expert in court will explain the evidence analyzed and the Operational System and Procedures for analyzing the evidence. Regarding the digital evidence and forensic test reports presented, the testimony of a digital forensic expert is very important for evidence in court. This is because the digital forensic test report is difficult for lay people to understand and expert testimony in court will be able to better explain the results of the forensic test report.

The judge's consideration is one of the most important aspects in determining the realization of the value of a judge's decision that contains justice (ex aequo et bono) and contains legal certainty, in addition to also containing benefits for the parties concerned so that the judge's consideration must be addressed carefully, well, and carefully. If the judge's consideration is not careful, good, and careful, then the judge's decision derived from the judge's consideration will be canceled by the High Court of the Supreme Court. In examining a case, evidence is also needed, where the results of the evidence will be used as consideration in deciding the case. Evidence is the most important stage in the examination at trial. Evidence aims to obtain certainty that an event / fact that is submitted actually occurred, in order to obtain a true and fair judge's decision. The judge cannot make a decision before it is clear to him that the event / fact actually occurred, namely its truth is proven, so that there is a legal relationship between the parties.

4. Conclusion

The validation procedure for electronic evidence is largely determined by the type of electronic evidence submitted. The ITE Law groups these into two parts, electronic information and/or electronic documents become electronic evidence (digital evidence), while the printed results of electronic information and electronic documents become written evidence. The validation process through digital forensics is carried out through strict and thorough stages to ensure the validity and accuracy of the evidence. Judges may only base their legal considerations on validated electronic evidence (valid digital evidence). The validation process will ultimately be stated in the legal considerations of the verdict as the core product and final product of the court. The description of the electronic evidence includes three main things, namely 1) the results of the validation of electronic evidence submitted by the parties and its conditions, 2) the relevance of electronic evidence to the facts (relevance principle), and 3) the

determination of the law based on references to electronic evidence. The preference for stages through expert testimony in digital forensic evidence in terms of the judge's need to strengthen the analysis of his decision. The criteria for digital forensic experts in Indonesia are currently not detailed in the laws and regulations.

5. References

Books:

Dikdik M. Arif Mansyur, and Elisatris Gultom, (2005), CYBER LAW Legal Aspects of Information Technology, PT. Refika Aditama, Bandung

Ferry Sulianta, (2008),*Computer Forensics*, Elex Media Computindo, Jakarta

Supandi, (2019). Modernization of State Administrative Courts in the Era of Industrial Revolution 4.0 to Encourage the Progress of Indonesian Legal Civilization, Semarang: Undip Press

Journals:

Anton Susanto, Ira Alia Maerani, and Maryanto, (2020), Legal Enforcement by the Police against Child of Criminal Doer of a Traffic Accident Who Caused Death (Case Study in Traffic Accident of Police Traffic Unit of Cirebon City Police Juridiction), Jurnal Daulat Law, 3 (1)

Asep Sunarsa, (2018), Attorney Role In Fighting Crimes Of Motorcycle Gang In Cirebon, Jurnal Daulat Hukum, 1. (2)

Goddess Asimah. (2020), To Overcome The Constraints of Evidence in The Application of Electronic Evidence. Peratun Law Journal, 3 (2)

H. Muslihin Rais, (2017), The Value of Justice of Judges' Decisions in Corruption Cases, Al-Daylah Journal, 6 (1)

Handrizal, Handrizal, (2017), Comparative Analysis of Puran File Recovery Toolkit, Glary Undelete and Recuva Data Recovery for Digital Forensics. J-SAKTI (Journal of Computer Science and Informatics), 1 (1)

I Made Wiryana MSc, (2008), SAFFA-NG Forensic Case Management Architecture System. Indonesian Journal of Legal and Forensic Sciences, 1 (1)

Insan Pribadi, (2018), Legality of Electronic Evidence in the Criminal Justice System, Lex Renaissance, 1 (3)

Ruci, Meiyanti, and Ismaniah. (2015), Development of Digital Forensics. UBJ Scientific Study Journal, 15 (2)

Santhos Wachjoe P, (2016), Use of Electronic Information and Electronic Documents as Trial Evidence, Journal of Law and Justice, 5 (1)

Sri Praptini, Sri Kusriyah, and Aryani Witasari, (2019), Constitution and Constitutionalism of Indonesia, Journal of Legal Sovereignty, 2 (1)