Available online at JDR Website: http://journal.unublitar.ac.id/jdr

Journal Of Development Research, 7 (2), November 2023, Pages 264-271

DOI: https://doi.org/10.28926/jdr.v7i2.238

Digital Forensic Urgence in Analyzing Electronic Evidence for Evidence of Criminal Actions in Information and Electronic Transactions

Rivad Achmad Fahrezi Abdullah[(1)], Audyna Mayasari[(2)], Hijrah Adhyanti Mirzana[(3)]

Universitas Hasanuddin, Indonesia

E-mail: [(1)]rivadachmad@gmail.com

Received: 22 August 2022; Revised: 10 November 2023; Accepted: 20 November 2023

Abstract

This study aims to determine the position of digital examination results as electronic evidence for proving criminal acts of information and electronic transactions. This research was conducted using normative research methods. which is done by researching library materials and judges' decisions then analyzing the materials which are methods or methods used in a legal research to find answers which will later become a prescription for the legal problems faced. The results of this study indicate that digital evidence in the form of information and electronic documents and has passed the digital forensic process is legal evidence, as stated in Article 5 paragraphs (1) and (2) of Law Number 19 of 2016 concerning Electronic Information and Transactions. . So that the position of electronic evidence from the results of digital forensic examinations as evidence of expert testimony and documentary evidence at the stage of investigation and proof in the trial process.

Keywords: crime digital, evidence, forensics

Introduction

The development of globalization such as technology and information has made the Indonesian people part of the world's information society so that it requires the establishment of a regulation 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 (UU ITE, 2008).

Information technology has made the world borderless and caused significant social change to take place so quickly. It can be said that today's information technology has become a double-edged sword, because in addition to contributing to the improvement of human welfare, progress and civilization, it is also a means of stimulating the occurrence of unlawful acts.(Indra, 2017) According to statistical data from the Association of Indonesian Internet Service Providers out of a total population of 264 million people in Indonesia, 196.7 million people or around 72.8 percent are connected to the internet and it can also be said that the number of internet users in Indonesia has increased by 23.5 percent since 2019 (Data APJII, 2020-2021).

Achmad Ali revealed about the factors that drive changes in legal values, which are actually not laws but factors of population growth, changes in values, ideology, and advanced technology (Achmad Ali, 2015). Therefore, it has an impact on the increasing number of cases involving information technology crimes. Where offenses related to information technology are generally divided into two, namely offenses intended to attack systems or even damage computer networks and second offenses against computers and/or other digital devices that use the internet as a tool to commit crimes of use.

The obstacles to solving a crime case in the information technology scheme. These terms cause difficulties for evidence that is being processed, stored, or transmitted via electronic devices. Information or electronic documents that are slightly modified sometimes raise a question mark if they are related to the law regarding the authenticity of the information or electronic documents in question.

It is easy for someone to use any identity to carry out various types of electronic transactions anywhere, making it difficult for law enforcement to determine the identity and location of the real perpetrator. This effort is made to eliminate digital evidence that they believe can obscure the traces of the crimes they committed (Joua Sitompul, 2012). Such as information technology-based crimes, namely carding, dissemination of pornographic information and personal documents, and fraud in electronic media. Especially defamation through electronic media. Therefore, information technology is connected to the internet as an invisible medium, so that criminals can easily eliminate traces without being clearly identified.

Information technology-based crimes are connected to the internet as an invisible medium. As a result, criminals can easily erase their tracks without being identified, making it difficult for law enforcement officials to determine the authenticity of the evidence used.

Proving the digital evidence by knowing the authenticity or authentication of the sender and the location of the perpetrator. So we need a branch of discipline, namely Digital Forensics or computer forensics. Where Digital Forensics is a technique for obtaining digital evidence, namely the retrieval, maintenance and presentation of data that has been processed electronically and stored on computer-based electronic media that can be used in criminal case investigations that can be legally accounted for.

Digital Forensic Science is what law enforcers use in finding electronic evidence to be included in the law enforcement process, because in fact this evidence is the key to revealing the truth of a case in court in addition to other supporting evidence. Because in the investigation, documents deemed to be related to criminal acts must be analyzed for their history, when they were made, using what equipment and who made them.

The Criminal Procedure Code is not able to accommodate the development of information technology, especially electronic evidence. This was responded by the government with the enactment of the Law on Information and Electronic Transactions No. 19 of 2016 on the amendment to Law No. 11 of 2008. Therefore, this law is used in the law enforcement system regarding Information Technology Crimes.

Based on this, it is clear that the Criminal Procedure Code as a criminal procedure law is based on the principle of legality. The implementation of the application comes from the starting point of the rule of law, that is, all actions must be carried out (Amir dan Haeranah, 2012) :

a) Based on the provisions of the law and the Act
b) Placing the interests of law and legislation above all else, so as to realize a life of the nation's people who are subject to the rule of law in harmony with the legislation and the feeling of justice of the Indonesian nation.

Legal evidence to be submitted before the trial as regulated in Article 184 of Law Number 8 of 1981 concerning the Criminal Procedure Code is (R. Soesilo, 1988) :

1. Witness testimony
2. Expert description
3. Letter
4. Instruction
5. Defendant's statement.

The latest breakthrough in the development of evidence can be seen in the Law on Information and Electronic Transactions Number 19 of 2016. This law is an answer to the main problem in the development of information technology-based crimes or cybercrimes. Where there is electronic evidence and electronic evidence in the form of electronic information and electronic documents, it is regulated in the law (Alcadini Wijayanti, 2012).

According to Paragraph 1 Article 5 of the Law of the Republic of Tajikistan Number 19 of 2016, electronic information and electronic documents are legal evidence. Then in paragraph (2) of the article it is emphasized that electronic information and electronic documents are extensions of legal evidence according to procedural law in force in Indonesia.

Electronic evidence is not regulated in the Criminal Procedure Code, but is found in criminal law practice and there are arrangements in various laws and specific legal instruments promulgated by the Supreme Court. The special law stipulates that electronic evidence can be used to prove criminal cases, both at the level of investigation, prosecution, and determination in court (Ramiyanto, 2017).

Digital forensics will determine the validity of electronic evidence in court. Based on the principle that any evidence can speak, anyone

who can make electronic evidence "talk" is a digital forensic expert. This explanation will be carried out later by reconstructing the electronic evidence so that the course of the trial becomes clear.

The problem is that the importance of the role of digital forensics in revealing electronic evidence where the evidence is vulnerable to be changed or manipulated by every perpetrator of information-based crimes and electronic transactions in order to be able to eliminate traces of the actions they have committed so that the authenticity of the evidence needs to be questioned, therefore make it difficult for law enforcement officers to prove before the court. Therefore, the author has an interest in answering the question, namely: How is the position of the results of digital forensic examinations as electronic evidence for proving information technology crimes in the Criminal Procedure Code.

Materials and Method

The research that will be conducted in this thesis is using the focus of normative research studies. This normative research is a type of legal literature research conducted by examining library materials and judges' decisions (Irwansyah, 2020). The approach in this study the author uses a conceptual approach which is carried out by examining the understandings that develop in the field of legal science that are related to the issue being handled or there has been an incarraht judge's decision (Peter, 2005). The form of material analysis is a method or method used in a legal research to find answers or solutions that will later become a prescription for the legal problems faced.

Results and Discussion

The Position of Forensic Digital Examination Results in the Criminal Procedure Code (KUHAP) for Proof of Information Crimes and Electronic Transactions

Electronic evidence is information and data that is stored and sent or collected electronically from a criminal who uses electronic media Electronic evidence basically has the characteristics of being invisible, very easy to change or damage, can move easily, so it requires a tool to see or read it. This is very different from conventional evidence which is generally the opposite.

The need for a digital forensic examination, where digital forensic examination is the science of analyzing electronic evidence so that it can be accounted for in the evidentiary process in court. This electronic evidence is used in committing criminal acts of all criminal acts using electronic media.

The principle of digital forensics is the process of collecting, acquiring, recovering, examining and storing information and electronic documents or electronic evidence contained in electronic media for the purpose of proving evidence in court.

In Law Number 19 of 2016 concerning Electronic Information and Transactions, the amendment to Law Number 11 of 2008 concerning Electronic Information and Transactions provides a legal basis for electronic evidence so that it can be accepted in court.

Law Number 19 of 2016 concerning Information and Electronic Transactions is divided into two parts. The first part concerns electronic information and/or electronic documents. and then print information and/or electronic documents. Computerized information and documents are electronic evidence (digital evidence). On the other hand, printed information and electronic documents are used as proof of letters.

Article 5 (1) of the law states that electronic information and documents or their paper copies are legal evidence in court. Article 5 (2) stipulates that electronic data and documents and/or their printed results are extensions of valid evidence according to the procedural law applicable in Indonesia.

In accordance with Article 184 paragraph 1 of the Criminal Procedure Code, valid evidence is witness testimony, expert testimony, letters, instructions and statements of the defendant. to prove the evidence in the crime of Information and Electronic Transactions.

In Law Number 19 of 2016 concerning Information and Electronic Transactions on the amendment of Law Number 11 of 2008 concerning Information and Electronic Transactions which regulates a crime committed through the use of information technology or computer networks is called cyber crime, including applications and software that is on the computer. Various kinds of crimes in a sense such as pornography, online prostitution, fraud, trafficking in persons and defamation.

Based on the results of the author's research regarding the urgency of the digital forensic

process carried out at the investigation stage in the police to the stage of proving evidence in court.

Digital Forensic Examination Results Used as Evidence of Expert Statements for Proof of Information Crimes and Electronic Transactions

Proof is a very important process to find material facts that exist in a judicial process because it is a judge's consideration in deciding a case. In a trial of evidence, it is very important for someone to prove whether the defendant's actions are substantially determined by the findings of the case evidence.

In Law Number 19 of 2016 concerning Information and Electronic Transactions on the amendment of Law Number 11 of 2008 concerning Information and Electronic Transactions which regulates a crime committed by utilizing information technology or computer networks known as cyber crime, including applications and software on the computer. Various kinds of crimes in a sense such as pornography, online prostitution, fraud, trafficking in persons and defamation.

The proof system for cyber crimes is subject to the opposite mechanism of proof, namely a proof by the guilt of the defendant is determined by a minimum of two valid pieces of evidence and a judge's conviction, because this cyber crime is related to electronic media, the proof is also needed by an expert in the field. technology too.

Expert testimony for evidence in cybercrime cases is very necessary because the process of proof in cybercrime cases is evidence from electronic data, so experts in certain fields are asked to give their opinions to explain something to cases that are currently in the process of proving before the Court. to check, namely digital data legal experts.

In this component letter, what is meant is a person who is skilled in part in spying on the fairy of an event. For later, the recorded component will examine, research, analyze, issue opinions based on the environment it has in order to establish explicitly whether or not the detainee actually practices a cyber crime structure.

The strength of the evidence in the expert's statement is as follows:

a) The evidence in the expert copy is free because it does not force the judge to use it, and if it contradicts the judge's decision, the judge is free to use it as evidence in the expert copy according to Article 186 of the Criminal Procedure Code to consider the judge's right in sentencing the defendant.
b) Expert opinion has the same evidential value. Article 184 of the Criminal Procedure Code.
c) The expert opinion is compiled by an expert who has special expertise in the criminal justice process being examined.

So a digital forensics expert who has an expertise in the field of information technology or in the cyber field should be responsible scientifically or academically as well as practically account for the knowledge he has to analyze electronic evidence in criminal acts of information and electronic transactions.

Information crime and electronic transactions or cybercrime in the period 2020 to 2021. In the case of cybercrime, which article can be explained, violated and listed in the table column. There are three decisions regarding cyber crime, and all three are criminal acts of defamation through electronic media. The three cases presented evidence in the form of expert statements, experts who were present to explain and provide their statements in the process of proving every crime of Information and Electronic Transactions. And not all cases in the decision are in the process of proving the existence of information from digital forensic experts, but only language experts.

Cases with permanent legal force in the table are criminal acts that use electronic media. According to the data above, it is also clear that quantitative human resources are limited, in this case, digital forensic expert information, especially at the district level. So there are still many cybercrime case reports that have not yet reached the trial stage.

Crimes related to information and electronic transactions or cybercriminals go to the trial stage, they must go through the investigation and settlement stage within the police. However, in the case of cybercrime, as with any computer system in cyberspace, finding digital evidence is quite difficult. Therefore, we need tools and experts in the field of information and electronic transactions because they are experts in the field of digital forensics who are able to explain the possibility of crime, how it occurred, what tools were used, and how cyber crimes were committed.

According to Nasrul Kadir, S.H as the

Judge of the Maros District Court, as stipulated in Article 184 paragraph (1) of the Criminal Procedure Code, what is meant by the expert here is a digital forensic expert, where this digital forensic expert provides a statement relating to digital evidence at the proof stage. at trial and is domiciled as evidence of expert testimony so that the judge is able to consider in his belief to decide the guilt of the defendant in accordance with the article charged by the public prosecutor (Interview, Nasrul Kadir, 2022).

The opinion of Teguh Adiyanto Muriono S.H as an investigator for the South Sulawesi Police Ditsiber explained that this is a digital forensic specialist who will handle electronic evidence directly, from crime scenes to the lab. forensics. in accordance with article 43 paragraph (5) of Law Number 19 of 2016 concerning Information and Electronic Transactions, it has been mentioned that investigators may request expert assistance during the investigation process. In the explanation of the article, it is only stated that the criteria for experts must be accountable both academically and practically. However, there is no further explanation of what is meant by academic and practical.

So that the digital forensic expert During the processing of evidence, the data obtained comes from the source, so there is no manipulation of the form, content, and quality of digital data. In accordance with Article 3 (2) of the Electronic Information and Transaction Law Number 11 of 2008, which stipulates that the conduct of investigations in the field of information and electronic transactions must be carried out in connection with the protection of privacy, confidentiality, as well as the functioning of public services and data integrity by good according to law (Interview Teguh, 2022).

So the author concludes that to find out the authentication or authenticity of digital evidence collected by the police at the investigation stage, it is better to pass a digital forensic examination where this examination is analyzed by a digital forensic expert. After passing through the digital forensic process, the digital forensic expert provides information about his analysis of the examination, so that his statement is used as evidence for expert testimony in the evidentiary process and strengthens the judge's confidence in deciding cases of Information and Electronic Transaction Crimes as in decision number three in the table above with decision number 193/Pid.Sus/2020/ Pn.Mrs

Digital Forensic Examination Results Used as Letters of Evidence for Proof of Information Crimes and Electronic Transactions

Legal evidence is a tool related to a crime that can be used as evidence that leads to the judge's belief in the truth of the crime committed by the defendant in the field of information and electronic transactions.

The system of evidence and evidence based on article 184 of the Criminal Procedure Code is able to reach evidence for cybercrime which is classified as a new crime. Searching for conventional evidence such as witness statements and expert statements, as well as shifting letters and instructions from conventional to electronic will be able to ensnare cybercrime perpetrators. Law No. 11 of 2008 Jo Law no. 19 of 2016 concerning criminal acts of information and electronic transactions, which is stated in Article 1 paragraph 1 which reads: "Electronic information is one or a set of electronic data, including but not limited to writing, sound, images, maps, designs, photographs, electronic data interchange. , electronic mail (electronic mail), telegram, telex, telecopy or the like, letters, signs, numbers, access codes, symbols, or perforations that have been processed that have meaning or can be understood by people who are able to understand them.

Meanwhile, in Article 1 paragraph 4 of Law Number 11 of 2008 in conjunction with Law Number 19 of 2016 which reads that electronic documents are any electronic information that is created, forwarded, sent, received, or stored in analog, digital, electromagnetic, optical, or the like, which can be seen, displayed, and/or heard through a computer or electronic system, including but not limited to writing, sound, pictures, maps, designs, photos or the like, letters, signs, numbers, access codes, symbols or perforations that has meaning or meaning or can be understood by people who are able to understand it.

The form of defamation is contained in the Criminal Code and there is also a form of defamation in the internet world or through electronic media and is contained in several articles in Law Number 19 of 2016 on the amendment to Law Number 11 of 2008 concerning Information and Electronic Transactions.

There are three cases that have been decided and have permanent legal force which include the crime of Information and Electronic Transactions regarding defamation through electronic media. And the three decisions that have permanent legal force are proven by one of them being documentary evidence.

However, there is only one case in which the digital evidence has gone through a digital forensic process and a paper report is made as the medium and is proven through the minutes of the examination of digital evidence, namely in decision number 193/Pid.Sus/2020/Pn.Mrs.

It is well known that in criminal prosecution, apart from errors and criminal acts, it is hoped that the factor of proving the strength of evidence in the Criminal Procedure Code is also an important issue. Law Number 8 of 1981 concerning the Criminal Procedure Code stipulates that in Article 18, valid evidence is witness testimony, letters, expert testimony, instructions and statements. defendant. said to consist of.

Especially in the Evidence letter is the evidence most relevant to computer material. According to experts, letters are writing that is interpreted as descriptive punctuation to express what is in your heart. The problem is that not everyone can read and understand written computer code. Therefore, finding existing evidence requires a scientific mechanism called forensics.

As a normative letter in criminal procedural law, a criminal procedural law system which is negative by law with the aim of punishing the defendant or defendant requires the minimum amount of evidence determined by law. However, even if the evidence accumulates and exceeds the minimum required by law, if the judge is not satisfied with the defendant's guilt, he cannot accept it and convict the accused.

In the research at the South Sulawesi Regional Police located in the city of Makassar, the authors interviewed investigators on behalf of Teguh Adiyanto Muriono with the position of Ba Unit Sub-Directorate V of Special Cyber Crimes.

According to Teguh Adiyanto Muriono's explanation as an investigator for the Criminal Directorate of Cybercrime, specifically for the South Sulawesi regional police, that because people have never met in person and have no physical contact with the crime scene, electronic devices do not leave physical traces. However, the contact made is a virtual contact. That's why the traces left on your contacts are called digital evidence. Therefore, finding digital evidence stored on computers and cell phones used by criminals requires digital forensics techniques—techniques that collect and analyze data and traces from computer systems, networks, and storage devices.

The investigator said considering the characteristics of digital evidence that has a high risk of being damaged, so that it can be damaged by criminals of information and electronic transactions with the intention of avoiding legal entanglements (Interview Teguh, 2022).

As for the digital forensic process, the first is the collection where you get supporting evidence at the investigation stage, the second is maintenance, namely maintaining and preparing digital evidence. In the explanation of the investigators of the Directorate of Cybercrime, specifically for the South Sulawesi regional police, this maintenance process is very important because at this stage it protects the evidence from damage, alteration and disappearance by certain parties. Because the evidence must be truly original which has not undergone any process.

This is done by copying the data bitstream image to a secure location. Bitstream images are a digital storage method that copies every bit of the original data, including hidden files. That is, the files are completely copied to the new media. And in this process it is called cloning technique. Third, enter the process of in-depth analysis of the evidence that has gone through the cloning process without changing from the original to be analyzed. The last is the reporting process, at this final stage the reporting is carried out by a digital forensic analyst regarding the findings in the form of evidence in the form of whatever is in the device used, when it happened, how to do it and the file is original or not.

After going through several stages or the digital forensic process, it is proven that there is a report made by a digital forensic expert in the form of a letter. And later the letter will be used as legal evidence in court in accordance with article 182 paragraph 1 of the Criminal Procedure Code. Then the evidence of the letter is used to prove criminal acts of information and electronic transactions.

Evidence at trial in accordance with article 183 of the Criminal Procedure Code stipulates that in order to determine a sentence for a defendant for his guilt, it must be proven by at least two valid pieces of evidence.

Therefore, with the enactment of this article, documentary evidence from the results of a digital forensic examination is one of the considerations by the judge to determine whether or not the defendant committed a crime of information and electronic transactions.

Article 187 of the Criminal Procedure Code requires that it be through an oath of office or strengthened by an oath so that a letter can be used as evidence.

So this is very different from electronic evidence which cannot be sworn in as evidence. Because even if an oath is required, it will be unclear how the procedure for taking an oath will be for electronic evidence, such as videos or photos. Therefore, for the electronic evidence, a letter from an expert is needed that explains according to his expertise what he found in the electronic evidence.

According to Rubianti, S.H., M.H as Judge at the Maros District Court, he said that on the other hand, the results of the digital forensic examination which had two interpretations in their position were used as evidence in the evidentiary process at trial. This may include evidence of a digital forensic expert statement in the form of an expert report, which can also be used as documentary evidence in accordance with Section 18(1)(c) of the Criminal Code. Information from digital forensic experts is provided during the investigation process. In addition, if the expert is unable to attend the session, he can give his opinion in the form of a letter which will be read out at the trial (Interview Rubianti, 2022).

The author is of the opinion that the minutes that explain where the electronic evidence was obtained and examined by experts who explain the electronic evidence as outlined in the results of the analysis of the digital evidence through the digital forensic process and serve as documentary evidence as referred to in article 187 letter c of the Criminal Procedure Code. However, digital evidence must meet a requirement so that the digital evidence can be declared valid and can be used in the evidentiary process at trial. Fulfillment of the requirements for digital evidence can be done by collecting or confiscation of electronic data which is from the original form of the computer system so that it turns into digital evidence that is printed in the form of paper. Examples of electronic data or electronic documents that can be used as digital evidence are screenshots of posts taken from social media that are stored in a flash drive and then printed out so that they become letter evidence to be used in proving criminal acts of Information and Electronic Transactions.

Electronic evidence that has passed the digital forensic process in the decision Number 193/Pid.Sus/2020/Pn.Mrs, which stipulates digital evidence in the form of printouts, screenshots of chat and Facebook social media walls. In Law Number 19 of 2016 concerning Information and Electronic Transactions, digital evidence is referred to as Electronic Information and Electronic Documents as stated in Article 5 paragraph (1) and paragraph (2) which states that (1) Electronic Information and/or Electronic Documents and / or the printed result is a valid legal evidence. (2) Electronic Information and / or Electronic Document and / or its printout as referred to in paragraph (1) is an extension of valid evidence in accordance with the procedural law in force in Indonesia.

The meaning of the section in Article reservoir paragraph (reservoir) that Electronic Information is one or a group of electronic information, calculated but not hindered by the threshold of writing, sound, pictures, plans, designs, pictures, electronic intercharge information, electronic certificates, telegram, telex, telecopy or the like of letters, signs, access instructions, emblems, or perforations that are intuitively touchable that hold meaning or can be understood by those who are able to understand them.

Meanwhile, the threshold of Article reservoir paragraph (2) explains that Electronic Documents are any electronic information that is made, forwarded, sent, received, or stored in analog, digital, electromagnetic, optical, or similar forms, which can be seen, displayed, helped or heard. tracing a computer or electronic order including but not obstructed by the threshold of writing, sound, drawings, plans, drawings or the like, letters, signs, numbers, access instructions, emblems or perforations that hold lessons or meanings and can be understood by residents who understand them.

The author analyzes that according to the explanation above regarding Electronic Documents and Electronic Information, the evidence in the form of screenshots of chat sheets and screenshots of the walls of Facebook social media pages is Electronic Information in the form of letters and its position as legal evidence in the evidentiary process at trial and convinces the judge that it

is the defendant who is proven and determined to have committed a crime of Information and Electronic Transactions through electronic media. And according to the theory of negative evidence Negative wettelijke Bewijstheorie where this proof system refers to the law and the judge's conviction so that the judge can determine that the defendant is guilty and receive sanctions according to the mandate of the law.

Conclusion

Based on the series of discussions above and in accordance with the results of the author's research, it can be concluded that digital evidence in the form of information and electronic documents and has passed the digital forensic process is legal evidence, as stated in Article 5 paragraphs (1) and (2) of the Law. - Law Number 19 of 2016 concerning Information and Electronic Transactions. So that the position of electronic evidence from the results of digital forensic examinations as evidence of expert testimony and documentary evidence at the stage of investigation and proof in the trial process.

Suggestion

Departing from the results of the research conducted, as well as the reality of the problems encountered, the authors suggest the need for clear rules regarding the position of electronic evidence if it has become legal evidence. The existing laws in Indonesia regulate the position of electronic evidence differently, both as evidence and as other evidence, of course, making it unclear for law enforcers in practice.

References

Achmad Ali, (2015) *Menguak Tabir Hukum; Edisi kedua,* Jakarta: Penerbit Kencana Prenada Media Group.

Alcadini Wijayanti, *Perkembangan Alat Bukti Dalam Pembuktian Tindak Pidana Berdasarkan Undang-Undang Khusus dan Implikasi Yuridis Terhadap KUHAP,* Dipenogoro Law Review Vol. 1

Amir Ilyas dan Haeranah dkk, (2012), Asas-Asas Hukum Pidana II, Yogyakarta:Rangkang Education

Irwansyah dan Ahsan Yunus, (2020), *Penelitian Hukum, Pilihan Metode & Praktik Penulisan Artikel,* Yogyakarta: Penerbit Mitra Buana Media.

Josua sitompul, (2012), *Cyberspace, Cybercrime, Cyberlaw, Tinjauan Aspek Hukum Pidana.* Jakarta: Tatanusa.

Peter Mahmud Marzuki, (2005), Penelitian Hukum, Jakarta:Kencana Prenada Media Group

Ramiyanto, *Bukti Elektronik Sebagai Alat Bukti Yang Sah Dalam Hukum Acara Pidana,* Jurnal Fakultas Hukum Universitas Sjakhyakirti Palembang. 2017.

Soesilo R, (2013), *Kitab Undang-Undang Hukum Pidana (KUHP) serta komentar-komentarnya lengkap pasal demi pasal,* Bogor: Politeia.

