POSITION OF THE DIGITAL EVIDENCE BASED ON ARTICLE 184 & 185 CRIMINAL PROCEDURE CODE IN CYBER CRIMINAL INVESTIGATION IN THE COURT

R. Arie Febrianto
STMIK Sinar Nusantara Surakarta
E-mail: ariefebrianto337@gmail.com

ABSTRACT

Law made by government and legislator in order to establish order and regularity in public .Basically law made by legislators is the answer to the question of public at the time of the establishment of the law. The legal developments must be in line with the development of society, so that when people change or grow then the law should be changed to arrange all the developments taking place in an orderly manner in the growth of modern society, because globalization has been the driver of the birth of the Information Technology era. In cyber crime cases, knowing the position of digital evidence in cases of cyber crime. The theory used in this research is a progressive legal theory with empirical juridical methods using qualitative data analysis, kind of this research is a descriptive study. The conclusion of this study, System proofs and evidences under Article 184 and 185 Criminal Procedure Code evidence of unconventional tools such as witness testimony and expert witnesses, as well as letters and instructions shift from conventional towards electronic will be able to ensnare cybercriminals. Law Number 11 of 2008 on Information and Electronic Transactions, particularly Article 5 has been clearly stated that electronic information is a valid legal evidence in the form of electronic information and / or electronic documents and / or printout.

Keywords: Crime, Electronic Transactions, Cyber Crime.

A. INTRODUCTION

Basically law made by lawmakers is the legal answer to the question of society at the time of the formation of the law. Legal developments should be in line with the development of society, so that when society changes or develops then the law must change to organize all developments that occur in an orderly manner amid the growth of modern society4, because globalization has been the driver of the birth of the era of information technology (*B Suhariyanto, 2010*).

Along with the development needs of people in the world, information technology plays an important role, both in the present and in the future. There are at least two things that make information technology considered so important in spurring world economic growth. First, information technology encourages the demand for information technology products, the second is to facilitate business transactions, especially financial business in addition to other businesses (*B Suhariyanto, 2010*). Information technology by itself also changes people's behavior. The development of information technology has caused the world to be indefinitely and cause rapid social change. So it can be said that information technology today becomes a double-edged sword, In addition to contributing to the improvement of welfare, progress, and human civilization, as well as being an effective means of

unlawful acts (*B Suhariyanto, 2010*). Unlawful acts in Law Number 11 Year 2008 About Information and Electronic Transactions, a crime in information technology called Cyber Crime. Cyber crime is a type of crime associated with the utilization of an infinite information and communication technology, and has a strong characteristic with a technological engineering that relies on a high level of security, from information conveyed and accessed by Internet users (*Agus Tri PH 2010*).

In Article 35 of Law Number 11 Year 2008 on ITE has been explained that

"Any person who knowingly and without rights or against the law manipulates, creates, alters, omissions, destruction of Electronic Information and / or Electronic Documents in order to make Electronic Information and / or Electronic Documents considered as authentic data".

In Indonesia many cases related to cybercrime According to Deputy Chairman of Network Monitoring and Security SIRTII / CC, Muhammad Salahudin said the current cases of violations of cyber crime in 2014 to early April has reached about 1,000 cases. This number continues to increase every year to reach 100 percent. In 2010 only 100 cases a year, 2011 rose 200 cases, 2012 to 400 cases (*Jatimprov 2014*).

In practice in Indonesia, the crime by using computers since the first is a legal problem (Maskun 2013) which often encountered is when associated with the delivery of information, communication and / or transactions electronically, especially in the case of proof and things that teka with legal acts carried out Through electronic systems (Jatimprov go.id. 2014).

One example of cases of cyber crime that occurred in Surakarta, which in the proof of having an obstacle in the case of a password hacker email, which a person is suffering losses up to billions of dollars, because the email is a means of transactions in the company. This also happens in the case of e mail burglary that occurred in Jakarta, with the same method. However, this case did not arrive at the Court because the witnesses of the Reporting Parties, Victim and Defendant Witnesses had mediated and carried out the responsibility. Furthermore, a judge presented a witness but the expert witness of the reporter / victim could not prove it so the defendant was freed by the judge (Decision Number 20 / Pidsus /2011/PN.Ska).

Thus, in practice, proof of criminal law is a very vital role, considering that in the Criminal Procedure Code (KUHAP) the role of evidence is very influential on the judges' judgment. Every obstacle that arises makes law enforcement to be confused to conclude a case in the field of Information Technology, in which the form of evidence is digital

. B. **PROBLEM STATEMENTS**

1. How is Understanding and Position of Evidence in Cyber Crime case?

2. How is the position of Digital Evidence in the case of cyber crime based on article 184 and article 185 in the Criminal Procedure Code?

C. **RESEARCH METHODS**

Method Approach used by the author in this research is empirical juridical approach that is approach directly with plunge into field. Thus the empirical juridical research method can provide an overview of how the Position of Digital Evidence Instrument is linked to article 184 and article 185 of the Criminal Procedure Code (KUHAP) in the Cyber Crime case. The type of research used by the authors in this study is descriptive research that is to provide a complete picture of the proof of cyber crime, where this proof is associated with articles 184-185 Book of Criminal Procedure Law regarding the Letter as evidence in terms of This is an Electronic Letter. Descriptive research itself is intended to provide as much data as possible about humans, circumstances or other symptoms. The author in this study describes how the Proof in Cyber Crime case.

D. **RESEARCH RESULTS AND DISCUSSION**

1.Proving

Evidence is a decisive stage in the proceedings of the case, because the results of the evidence can be known whether or not an indictment or demands by pointing to the evidence. Evidence is anything that has to do with an action which, by means of such evidence, can be used as evidence to raise the judge's confidence in the truth of a crime committed by the defendant (Politikum blogspot 2013). The proof itself is the act of proving, proving means giving or showing evidence, doing something as truth, implementing, signifying, witnessing and convincing (Eddy O.S.Hiariej, 2012).

2. The setting of evidence in cyber crime is set forth in:

a.Book of Criminal Procedure Code.

b. Law Number 11 of 2008 on Information and Electronic Transactions

In the evidentiary system adopted in the Criminal Procedure Code 183 of the Criminal Procedure Code, "the judge shall not impose a penalty on a person except if with at least two valid evidences he / she is convinced that a crime is committed and that the defendant is guilty of doing so". This problem of proof plays an important role in dealing with cyber crime, it is necessary to note that electronic evidence has become a new medium for the execution of a crime (Khairul Anam, 2010).

And the subsequent evidentiary system in the Criminal Procedure Code (KUHAP), namely article 184, describes "legal evidence is:

a.) Description of witness d.) Directive

b.) Description of Evidence e.) Defendant's Statement

c.) Letter

3. Things that are generally known do not need to be proven In-Criminal Procedure Code Article 185 explained:

a) Description of the Witness as evidence is what the witness stated in court.

b) The description of a witness alone is not sufficient to prove that the defendant is guilty of the charges he or she is accused of

c) The provisions referred to in paragraph (2) shall not apply if accompanied by other legal evidence.

It is used as a valid proof if the witness's statements are related to each other in such a way as to justify the existence of a particular event or circumstance.

d) Neither opinion nor invention, derived from the results of thought alone, is not an expert description.

e) In assessing the truth of the testimony of a witness, the judge must seriously pay attention to:

i) The correspondence between witness testimony with each other;

ii) An appropriateness between witness testimony and other evidence;

iii)Reasons that might be used by witnesses to provide certain information;

iv)The way of life and morality of witnesses and everything that can generally affect whether or not the information can be trusted;

7) The statements of witnesses that are not sworn in alignment with each other, do not constitute

The evidence, however, if such information is in accordance with the statements of the witnesses sworn in may be used in addition to other legal evidence.

In the context of proof, the formulation of a offense in a law, in addition to the embodiment of the principle of legality, also has the function of evidence of evidence. That is, what the prosecutor has to prove in court is the elements in a delict formulation that is charged to the suspect. Here is a comparison of the Laws governing electronic evidence:

Law Number 8 of 2011 The Criminal Procedure Code (KUHAP) are :

a.Witness Written d. Guidance instructions

b.Exception of Expert e.Description of Defendant

c.Letters

Based on the Criminal Procedure Code and Law Number 11 of 2008 on Information and Electronic Transactions, in criminal acts cyber crime evidence that can be used are as follows:

a. Witness's Statement

Based on Article 1 Sub-Article 26 of the Criminal Procedure Code stated "The witness is a person who can provide information for the interest of investigation, prosecution and judicial hearing of criminal cases which he hears himself, he sees himself, and he experiences his own". Meanwhile the Statement of Witnesses according to Article 1 number 27 of the Criminal Procedure Code, "the witness's testimony is one of the evidence in a criminal case in the form of testimony from the witness concerning a criminal event which he heard himself, he himself sees, and he experienced by himself mentioning the reason of his knowledge ". Witnesses are required to provide actual or at least closer information from the events he / she sees, to provide an understanding of the judge in giving a decision to the offender.

While the witness in the cybercrime case involves the person who sees and controls the virtual world whose information can be used as the judge's consideration in disclosing the facts in the hearing, it is regulated in Article 7 of Law Number 11 of 2008 on Information and Electronic Transactions, which reads "Everyone who declares rights, reinforces existing rights, or refuses the rights of others based on Electronic Information and / or Electronic Documents shall ensure that eligible Electronic systems are in accordance with the laws and regulations ".

In Law Number 11 of 2008 on Information and Electronic Transactions, a witness may use the electronic media to provide his information, so that it does not have to come directly to the court so that it can be through communication media based on Article 44 of Law Number 11 of 2008 on Information and Electronic Transactions states "Proof of investigation of prosecution and examination

of court trial according to the provisions of this law are as follows: evidence as referred to in the provisions of legislation, Evidence in the form of Electronic Information and / or Electronic Document as referred to in Article 1 number 1 and item 4 and Article 5 paragraph (1), paragraph (2), and paragraph (3) ".

In the investigation of the crime of cyber crime there are 3 (three) phases used by the investigator, eyewitness told to tell all the information he saw and other information related to the crime. Police are searching for suspects based on information obtained from eyewitnesses and seeking track records of potential police suspects directly by presenting the suspect (Eddy O S Hiariej 2012).

If the statements of several stand-alone witnesses of an event or circumstance may be used as a valid proof if the testimony of the witness has a relationship with each other in such a way as to justify a particular event or circumstance.

In the procedure of giving witness statements in court can be through teleconference by appointing Article 1 number 1 and number 4 of Act Number Number 11 of 2008 on Information and Electronic Transactions, which reads "number 1: Electronic information is one or a set of electronic data, including but not limited to writing, sound, images, maps, designs, photographs, electronic data interchange (EDI) Electronics, telegram, telex, telecopy or the like, 3. letterheads, signs, numbers, access codes, or perforations, which have been processed that have meaning or can be understood by those who are able to understand them, item 4: Electronic document is any Electronic Information Manufactured, forwarded, transmitted, received, or stored in analog, digital, electromagnetic, optical, or the like, which may be viewed, displayed and / or heard through computers or electronic systems, including but not limited to writing, sound, images , Maps, designs, photographs or the like, letters, signs, numbers, access codes, symbols or perforations that have meaning or meaning or can be understood by persons capable of m Understanding ". Although through the teleconference the witness's statements remain valid by law by appointing Article 5 paragraph (1) of Law Number 11 of 2008 "Electronic information and / or Electronic Documents and / or prints are valid evidence" (Cahyo Handoko, 2016).

Thus, based on the above discussion, gives an illustration that the testimony of witnesses in the Criminal Procedure Code set forth in Article 1 number 27 Criminal Procedure Code. It basically states that the testimony of a witness is an evidence in a criminal case in the form of information given directly by a witness, concerning a criminal incident which he heard himself, he saw himself, and he experienced his own by calling the reason of his knowledge ". The Witness shall, in giving his

statements, be present at a court hearing open to the public, as provided for in Article 160 of the Criminal Procedure Code.

b. Expert Commentary

The expert's information under article 1 number 28 of the Criminal Procedure Code is the information provided by a person who has specific expertise on what is necessary to make the light of a criminal matter in the interest of the examination. Expert information is related to the evidence to form a judge's conviction in deciding a cybercrime case, usually taken from a professor and a thinker. In Article 186 of the Criminal Procedure Code states that "an expert's statement is what an expert states in court". According to the explanation of Article 186 of the Criminal Procedure Code, it is made by recalling the oath at the time of accepting office or occupation. Referring to the provisions of the Criminal Procedure Code, the expertise of a person providing expert testimony is not only based on the knowledge he or she has through formal education, but the skill can also be gained on the basis of his experience. Or a particular academic.

Expert information is usually general in the form of an opinion on the subject of a criminal case that is being tried or relating to the principal matter of the case. Experts are not allowed to provide an assessment of the case being on trial (Eddy OS Hiariej 2012). Therefore, the question of the expert is usually hypothetical or statements of a general nature. The expert may not provide an assessment of whether or not the defendant is allegedly based on the fact of the trial being asked of him. Thus, in the case of cyber crime, an expert is required to give an understanding of the disclosure of case events occurring in cyberspace so far as his knowledge, because expert witness is competent in his field, this is explained in article 1 paragraph (1) of Law No . 11 Electronic Information is an electronic data set, including but not limited to writing, sound, images, maps, designs, photographs, electronic data interchange (EDI), electronic mail, telegram, telex , Telecopy, or the like, letters, marks, numbers, access codes, symbols or perforations that have been processed which have meaning or can be understood by those who are able to understand them. The term "understandable by a person who is capable of understanding" is a claim to expert witnesses to translate the events disclosed by witnesses and defendants, and expert statements in the form of reports recorded in the minutes of examination.

c. Letters

According to Article 187 of the Criminal Procedure Code, the Letter as referred to in Article 184 paragraph (1) letter c, made up of oath of office or reinforced by oath, the type of letter referred to is:

1) Official proceedings and other letters in the official form prepared by an authorized or competent public authority containing information concerning an event or circumstance heard, seen or experienced by itself, accompanied by a clear and unequivocal reason for his statement;

2) A letter made in accordance with the provisions of legislation or a letter made by an official recognizing matters that fall within the governance which is his responsibility and which is intended for the provision of a matter or situation.

3) A certificate from an expert containing opinions based on his or her expertise on a matter or something of the circumstances formally requested and thereof;

4) Other letters that may only apply if they relate to the contents of other evidence tools.

Based on Article 187 of the Criminal Procedure Code, it is described about letter proof consisting of 4 (four) items. Under the Electronic Information and Transaction Act, electronic information and / or electronic documents and / or prints are valid legal evidence.

Electronic Information and / or Electronic Documents and their prints are valid expansion of evidence according to procedural law. Electronic documents can not be used as evidence if a letter, the law determines to be made in writing, including notarial deeds or deeds made by the official deed. In the event that the letters do not meet the requirements to be declared as proof of the letter, the letters may be used as guidance. However, as to whether or not the letter should be used as evidence of evidence, it is left to the judge's judgment. So that the proof of the letter used in the proof of cyber crime is a valid evidence as long as it is in accordance with the electronic system set in the laws that regulate it, because the proof of the letter in the form of digital can be changed its authenticity in seconds and without having to hold the goods Evidence presented in the hearing. Thus it can be seen that the letter is a valid evidence in accordance with Article 5 paragraph (1) of Law Number 11 of 2008 on Information and Electronic Transactions And refer to the judges concerned considerations.

d. Instructions

Article 188 of the Criminal Procedure Code (1) which reads "A Directive is an action, event or circumstance, which, because of its correspondence, either between one another and the offense itself, signifies that there has been a crime and who did it." The evidence evidence is the full authority and subjectivity of the judge who examined the case. The judge in drawing conclusions about proof as a guidance must relate the evidence to one another. Assessment of the evidentiary power of a directive in any particular circumstance is performed by a judge after he or she has conducted an examination.

Strictly speaking, the guidance requirements as evidence must have correspondence with each other for the deeds that occur. In addition, these circumstances relate to each other with crimes that occurred and based on the observations of judges obtained from testimony of witnesses, letters and statements of the accused

1. Conformity, ie the correspondence between each act, the occurrence, and the circumstances of each other or the correspondence between the acts of the incident, or the circumstances of the indicted crime.

2. Such adaptation signifies or indicates the existence of two things, namely to show who the perpetrators. This element is the conclusion of the workings of the formation of evidence evidence, which is also the purpose of evidence evidence.

3. It can only be established through three evidences, namely witness testimony, letter, and statement of defendant. In accordance with the minimum principle of proof as in Article 183 of the Criminal Procedure Code, appropriate guidance should also result from at least two valid evidences.

Furthermore, in the proof mentioned at least there should be two guidelines to obtain valid evidence. The instructions found in the investigation are valid evidence in accordance with Article 5 paragraph (1) of Law Number 11 of 2008 on Information and Electronic Transactions, so that if the instructions are in digital form, it can be used as evidence in the hearing.

e. Defendant's Statement

The application of evidence of criminal cases set forth in the criminal procedure law is forever still required even if the defendant acknowledges the offense charged to him (Yahya Please accessed www.hukumonline.com on February 23, 2015). The Defendant in Article 1 Item 15 of the Criminal Procedure Code is a suspect charged with, examined, and tried in court. According to Article 189 paragraph (1) of the Criminal Procedure Code, "The defendant's description is what the defendant declares in the congregation about an act he has committed or knows or owns himself." The statement of the accused granted outside the congregation may be used to assist in finding evidence in the congrega- tion, provided that the information is supported by a valid evidence as long as it is accused of him. The defense of the defendant can only be used against himself, this refers to Article 189 paragraph 4) Criminal Procedure Code.

That a defendant is not burdened with an obligation in proof, so the statement of the defendant is a valid statement he declared in court. By referring to the meaning of the word proof, ie something that states the truth of an event, So the significance of proof is to seek the truth of an event. In the context of law, the significance of proof is to seek the truth of a legal event. Law events are events that have legal consequences.

It is understandable that the evidence is seen from the perspective of criminal procedural law, namely the provisions limiting the trial in seeking and maintaining the truth, whether by judge, prosecutor, defendant or legal counsel, all bound by the provisions and ordinances, In Law Number 11 of 2008 on Information and Electronic Transactions

2. Understanding of Cyber Crime

As it is known that one of the areas of science is growing very rapidly is a computer field where in a matter of days, weeks, months or years the status of science and computer technology will display a different face to the previous. These developments produce two different faces depending on their utilization, ie the positive and the negative sides. Positive side, these advances are used to help human life to be more interactive, efficient and effective with the support of advanced computer technology. Being from the negative side, the progress can be misused to do more sophisticated crime. When the perpetrator has a level of understanding of science and technology in the field of computer is high enough, it will be easier to find weaknesses weakness of an electronic or non electronic system because there is no perfect system (NO SYSTEM IS PERFECT), to then exploited by himself Or groups in order to commit crimes that could be financially motivated, security politics, and so on. This crime is known as Computer Crime or Cyber Crime (Muhammad Nuh Al Azhar 2012).

3. The position of digital evidence in a cyber crime case

In handling cases of cyber crime law enforcement officers should pay attention on The digital evidence used by the offender in committing his deeds. Because the digital evidence has a very important position in the process of verification in the Court of Justice. From digital evidence that will also determine whether the actions committed by the defendant are guilty according to law or innocence. Digital Goods or digital evidence are:

a) Logical files, ie files that are still there and recorded in the file system that is running (running) on a partition. The files can be application files, libraries, office, logs, multimedia, and others.

b) Deleted files, also known as unallocated clusters that refer to clusters and sectors where file storage has been deleted and not located again for the file marked in the file system as an area that can be used again for storage of new files. This means that files that have been deleted still remain in the cluster or sectors where the storage until stricken (overwritten) by the new files in the sector or cluster. In the condition where the deleted file has not been overwritten, then the whole recovery process of the file is very possible to happen.

c) Lost files, ie files that are not recorded in the file system that is running (running) from a partition, but the file is still in the storage sector. This can happen when for example a flash or hard drive or partition is done re-formatting process that produces a new file system, so the files that have been there before become unrecorded in the new file system. For the recovery process is based on the signature of the header and footer that depends on the type of file format.

d) Slack files, ie storage sectors located between End OF Files with End Of Cluster. This region is very possible there is information that may be important from the previous files have been deleted

e)Log files, ie files that record the activity (logging) of a particular situation, such as logs from the operating system, internet browser, b-application, internet traffic, and others.

f)Encrypted Files, ie files that have been encrypted by using complex cryptographic algorithms, so it can not be read or seen normally. The only way to read or view it again is to decrypt the file using the same algorithm. This is commonly used in the world of digital information security to secure important information. It is also a form of anti-forensic, a method for complicating forensic analysis or investigators getting information about traces of crime.

g) Steganography File, a file containing confidential information disispkan to another file, usually in the form of image files, video, or audio, so the files are carrier (messenger confidential) is seen normal and reasonable for others. But for people who know the methodology, the files have a deep meaning from the secret information. It is also regarded as one form of anti forensic.

h) Office Files, Ie the files that are the product of office applications, such as Microsoft office, open office, and so forth. These are usually in the form of document files, spreadsheets, databases, texts and presentations.

i) Audio File, which is a file that contains sound, music and others, which is usually formatted wav, mp3, and others. An audio file containing a voice recording of this person's conversation is usually

important in the investigation when the sound inside the audio file needs to be audited and analyzed by forensic audio to make sure the sound is the same as the voice of the perpetrator.

j) Video files, ie files loading video recordings, either from digital cameras, mobile phones, handycam, or CCTV. This video file is very possible to load the face of the perpetrators of crime so that this file needs to be analyzed in detail to ensure that the file is a criminal.

k)Image file, which is a digital image file that is very possible to contain important information related to the camera and time of manufacture (time stamps). These data are known as metadata exit (exchangeable image file). However, this exit metadata can be manipulated, so forensic analysts or investigators should be careful when examining and analyzing the metadata of the file.

l) E-Mail (Electronic mail), the letter-based electronic system using an online network system to send it or receive it. E-Mail becomes important in the investigation especially phishing (ie crimes that use fake e-mails equipped with false identities to deceive the recipient). The e-mail contains a header containing important information on the distribution path of the e-mail sending from the sender to the recipient. Therefore, the data in this header is often carefully analyzed to ensure the location of the sender based on the IP address. Even so, the data in the header is also very possible to be manipulated. Thus header inspection of e-mail must be done carefully and comprehensively.

m) User ID and Password, is a requirement to enter into an account online. If one of them is false, then access to the account will be rejected.

n) Short Message Service (SMS), which is the short message delivery and receiving service provided by the cellular operator to its customers. SMSs that can be incoming, out (sent), and draft can be indicative in Investigation to determine the linkage between the perpetrators with each other.

o) MultImedia Message Service (MMS), is a service provided by mobile operators in the form of sending and receiving multimedia messages that can be in the form of sound, image, or video.

p) Call Logs, which is the recorded call record on a mobile call number. These calls can be incoming, outgoing, and missed.

In this case the authors will conduct an analysis of 2 Decisions Surakarta District Court on the case of criminal acts cyber crime. From the analysis of decisions by the author, so it will be known about the position of digital evidence in the case of criminal acts cyber crime.

The analysis will be described as follows:

1. Court Decisions

Number Verdict : 20 / Pid.Sus / 2011 / PN.Ska

Convicted : Syarif Bin Syech Salim

Crime : Email breaking / Accessing computer without permission

The indictment : Article 30 paragraph (1) Jo Article 46 paragraph (1) of Law of the Republic of Indonesia Number 11 of 2008 on Information and Electronic Transactions

Verdict : To impose criminal sanction on the defendant with 1 (one) year imprisonment is reduced during the period of arrest and duration of detention that the defendant has undergone, and a fine of Rp. 1.000.000, - (one million rupiah) subsidair 1 (one) month of confinement.

2. Judgment of the Court: 79 / Pid.Sus / 2013 / PN.Ska Anthon Wahjupramono, S.H, M.Hum. Spreading threat via Instant Messaging (SMS) Article 29 Jo Article 45 paragraph (3) of the Law of the Republic of Indonesia Number 11 of 2008 on Information and Electronic Transactions; Criminalize the defendant by imprisonment for 5 (five) years minus the period of detention that the defendant has undergone by order of the Defendant to remain in custody

After reading the 2 (two) decisions above, the three crimes can be categorized in cyber crime because these three decisions violate Law Number 11 of 2008 on Information and Electronic Transactions, the first decision Number 20 / Pid.Sus / 2011 / PN.Ska who was indicted

With Article 30 paragraph (1) Jo Article 46 paragraph (1) of Law of the Republic of Indonesia Number 11 of 2008 on Information and Electronic Transactions, the second of Decisions Number 79 / Pid.Sus / 2013 / PN.Ska indicted by Article 29 Jo Article 45 paragraph (3) of RI Law Number 11 of 2008 on Information and Electronic Transactions, and lastly Decision Number 476 / Pid.B / 2013 / PN. Sleman who was accused of Article 45 paragraph (1) Jo Article 27 paragraph (1) of RI Law Number 11 of 2008 on Information and Electronic Transactions. Furthermore, pursuant to articles 184 and 185 of the Criminal Procedure Code concerning legal evidence in the form of witness statements, expert statements, letters, guides, and statements of defendants and on the testimony of interrelated witnesses in which there is in this case SMS which is a digital evidence as evidence Strengthening and functioning as the main evidence that has been clearly stated in the ITE Act concluded that digital evidence has a prime position as evidence that plays a role in the judge's decision given to the defendant. The judge's judgment in disclosing the facts in the trial by using digital evidence Is in Article 5 paragraph (1) of Law Number 11 of 2008 on Information and Electronic Transactions

explains "Electronic Information and / or Electronic Documents and / or prints are legal legal evidence". To disclose digital evidence then the judge requires an expert witness in explaining such evidence as mentioned in Article 1 number 1 and item 4 explaining "number 1: Electronic Information

An electronic data set, electronic data, telegram, telex, telecopy or the like, letters, marks, Numbers, Access Code, symbols or perforations that have been processed that have meaning or can be understood by those who are able to understand them, item 4: Electronic Document is any Electronic Information created, forwarded, transmitted, received or stored in analog, digital, Electromagnetic, optical, or the like, which may be viewed, displayed and / or heard via Computer or Electronic System, including but not limited to writing, sound, images, maps, designs, photographs or the like, letters, , Symbols or perforations that have meaning or meaning or can be understood by people who are able to understand it ". So we can know the position of digital evidence in both decisions Above is that in the disclosure of facts in the hearing in order to find material truth, the Panel of Judges requires digital evidence in the case of cyber crime and the role of expert witness in strengthening the role of the digital evidence, because in Article 1 number 1 and number 4 of Act No . 11 year 2008 explains that Electronic Information and Electronic Document can only be understood by people who are able to understand it, the person who is able to understand it means having expertise in the field of Information and Electronic Transaction, in this case called expert witness, in the verdict above the expert witness is instructed to explain the position Digital evidence to the judges. Because the position of digital evidence in the above decision affects the judge's judgment to make a decision. This is associated with digital forensic explanation, the more assertive it is to say that digital evidence has a strong and important position in judgment by the judge against the defendant in violation of the Information and Transaction Electronic Law Based on 2 (two) Cyber crime Decisions above can be known tool The above digital evidence used is:

1. Laptop
2. Email
3. CD
4. Software (Uniblue Spyerasser)
5. Smartphone
6. CPU (Central Processing Unit)
7. Flashdisk
8. Data
9. Porno Film Content
10. CCTV Recording
11. SMS

Digital evidence is Electronic Information and / or Electronic Documents that meet the formal requirements and material requirements set forth in Law Number 11 of 2008 on Information and Electronic Transactions. Evidence can be said as digital evidence because of Electronic Information

and / or Electronic Document in accordance with the criteria in Article 1 number 1 and number 4 of Act Number Law Number 11 of 2008 covering writing, sound, images, maps, designs, photographs, electronic data interchange (EDI), electronic mail, telegram, telex, telecopy or equivalent, letters, signs, numbers, access codes, symbols, Or processed perforations that are meaningful or understandable to those who are able to understand them and their analog, digital, electromagnetic, optical, or similar forms which can be seen, displayed and / or heard through the Computer or Electronic System, including but not limited to Writing, sound, images, maps, designs, photographs or the like, letters, signs, numbers, access codes, symbols or perforations that have meaning or meaning or can be understood by people who are able to understand it, To explain a cyber crime that might be done by the suspect, so that this digital evidence clarifies the facts that occur with the support of other evidence. Can be known the types of digital evidence that has been described in article 1 number 1 and number 4 of Law Number 11 of 2008 is covering: Tool Type

Electronic Information; Electronic Document: Digital Evidence; Forms of Tools; Sound; Picture ;

Map; Design; Photos; Electronik Data Interchange (EDI); Electronic Mail (E-mail); Telegram;

Telex; Telecopy; Letters; Alerts; Access Code; Symbol; Perforation; Analog; Digital; Electromagnetic; Optica

What distinguishes Electronic Information and Electronic Documents is the means used in the proof of digital evidence, in accordance with Article 1 number 1, Electronic Information is limited to a person capable of understanding Information which may further define the Electronic Information, whereas in Article 1 number 4 Using the computer and / or electronic system to translate the Information contained in the Electronic Document. Understanding Electronic Systems is a set of electronic devices and procedures that function to prepare, collect, process, analyze, store, display, publish, transmit, and / or disseminate Electronic Information (Elucidation of Article 1 number 5 of Law Number 11 of 2008 on Information and Electronic Transactions). So in the fact disclosure of the above three decisions must be able to distinguish Electronic Information and Electronic Documents to minimize the multiple interpretations that may occur by court judges. In Article 183 of the Criminal Procedure Code "Judge shall not impose a penalty on an individual except where, with at least two valid evidences, he / she obtains the conviction that a crime is actually committed and that the defendant is guilty of doing so". Proof of using digital evidence, the judge must be able to uncover the facts and get at least 2 evidences to obtain the conviction that a crime really happened and that the defendant did it. Surakarta District Court Judge Kun Maryoso, SH, MH explains cyber crime is a cyber crime, the disclosure using digital evidence and expert witnesses who are really experts in the field to

provide understanding of the events according to expert glasses, this is to minimize multi interpretation with the judge The other because, the position of this digital evidence as a guide or letter and / or electronic document described in Law Number (Kun Maryoso SH, Personal interview dated 28 August 2014 11.30 wib) The position of the digital evidence of the two decisions as instructions or letters and / or electronic documents as described in Law Number 11 of 2008 on Information and Electronic Transactions, so that required expert witness to understand it as described in Article 1 number 1 and number 4 of Act Number 11 of 2008 on Information and Electronic Transactions.

The third cyber crime case of the above verdict requires proof to know the facts that occur, in the disclosure of the evidence, Law enforcers shall comply with the procedures and provisions of the Criminal Procedure Code and the provisions in Law Number 11 of 2008 on Electronic Transactions and Information and the provisions contained in the Digital Forensics review, especially the basic principles of Digital Forensics. In Law Number 11 of 2008 in Article 5 paragraph 1 "Electronic Information and / or Electronic Documents constitute valid evidence". So in terms of determining the proofing procedure of digital evidence Bhudhi Kuswanto, S.H describes as follows:

1. Expert witnesses are instructed to explain their knowledge of the case on trial.

2.Then the Investigator of the Police shall copy / copy or electronic information in a new device, then the digital evidence is presented before the court.

3. Furthermore, expert witnesses make an analysis of the digital evidence to be judge's consideration.

To maintain the authenticity of digital evidence law enforcers have their own procedures in handling digital evidence that is evidence in the Court, the procedure used is as follows:

1.Acquiring and Imaging Process

After the investigator receives the digital evidence, it must be done the process of acquiring and imaging that copy (clone / duplicate) precisely and precision 1: 1 from the result of the coffee then a digital forensic expert can do the analysis because the analysis should not be done from digital evidence Original because it is feared will change the evidence.

2. Conducting Analysis

After doing the Acquiring and imaging process, it can be continued to analyze the contents of the data, especially those that have been deleted, hidden, encrypted, and abandoned log traces. The results of such digital evidence analysis will be delegated to the prosecutor to be brought to the Court.

According to Bhudhi Kuswanto, SH, Judge at the Surakarta District Court (Kun Maryoso, SH interview on August 28, 2014 at 11.30 Wib) in proving the digital evidence in the Court must pay attention to the authenticity or originality of the digital evidence, because this digital instrument can be changed Any time in a matter of minutes, so that investigators in the Surakarta Court's jurisdiction are expected to pay attention to it (Bhudhi Kuswanto personal interview January 10, 2015).

In the procedure of substantiation of digital evidence in the court affirmed in Article 43 paragraph (2) of Law Number 11 of 2008 on Information and Electronic Transactions stating "Investigations in the field of Information Technology and Electronic Transactions as intended, shall be conducted with due regard to protection of privacy, confidentiality, smooth public services, data integrity, or data integrity in accordance with the Laws and Regulations", Enforcers The law has not fully considered the prescribed procedures, such as for example in the above three decisions, which on average gives freedom for expert witnesses to directly explore the contents of digital evidence in the form of laptops, should law enforcement before presenting digital evidence must copy the data from laptop To a new device, in accordance with the Acquiring and imaging procedures, thereby minimizing the evolution of the evidence being presented at the Court and not reducing the value of the authenticity of the evidence. Bhudhi Kuswanto explains that this digital evidence is very vulnerable to change, it can be changed in minutes without anyone knowing it, so it is unfortunate if the existing procedures are not implemented in this proof of digital evidence. (Bhudhi Kuswanto SH personal interview January 10, 2015)

It was concluded that the processing of digital evidence under Article 184 and Article 185 of the Criminal Procedure Code of the two decisions has not fully complied with the procedures already in use, it is possible to change the authenticity of digital evidence presented in court, it can not be denied that the suspect may be subject to a decision , Is not proven to do any particular thing because its evidences have been changed because, this position of digital evidence affects judge's consideration in taking decision.

Of the two Decisions obtained by the authors in the field, there is no process of evidence according to the procedure, the digital evidence presented in the trial has been explored by previous expert witnesses, thereby reducing the authenticity of a proof instrument itself, whereas in Law Number 11 of 2008 in Article 43 paragraph (2) has been explained about the implementation of investigation procedures in the field of Information Technology and Electronic Transactions. One judge of the Surakarta District Court Explains that in the handling of evidence, a judge only hears information from the parties, one of which is the testimony of expert witness who becomes the judge's

judgment in making the verdict so that the processing of the instrument is fully authorized by the investigator (*Kun Maryoso SH interview Private August 28, 2014)*

Of the three decisions above, not yet fully using the correct evidence processing procedures of investigators, thereby reducing the authenticity of digital evidence, because the position of evidence of both cases is crucial to determine the judge's decision. In Law Number 11 of 2008 on Electronic Transactions and Information in Article 5 paragraph (1) explains that "Electronic Information and / or Electronic Documents and / or prints are valid evidence". Therefore, in processing of such evidence must pay attention to the procedures in accordance with Article 43 paragraph (2) of Law Number 11 of 2008 on Information and Electronic Transactions.

E. **CLOSING**

Evidence and evidence system based on Article 184 KUHAP, Article 185 KUHAP and Digital forensic provisions are able to reach the proof for the crime of cybercrime which is classified as a new crime. Tracing conventional evidence such as witness testimonies and expert witnesses, as well as shifts of letters and instructions from conventional to electronics will be able to ensnare cyber crime. Law Number 11 of 2008 on Information and Electronic Transactions on Article 5 has clearly stated that Electronic Information is a legal legal proof of electronic information and / or electronic documents and / or prints.

This position of digital evidence affects judges' judgment in making decisions. As well as complementary letter proof as described in Law Number 11 Year 2008 About Information and Electronic Transactions. So in the processing of digital evidence must be kept in the authenticity of such evidence to minimize the changing of digital evidence because, it can affect the trial process. From the results of the second study Verdict obtained authors in the field, there is no processing of evidence in accordance with procedures and procedures for Digital Forensics, instrument digital evidence presented at the trial had been in explore by expert witnesses earlier, thus reducing the authenticity of an evidence itself, whereas In Law Number 11 of 2008 on Article 43 paragraph (2) has been explained about the implementation of investigation procedures in the field of Information Technology and Electronic Transactions. Digital proofing tools must be kept in the authenticity of such evidence to minimize the changing of digital evidence because, it can affect the trial process.

BIBLIOGRAPHY:

Al-Azhar Muhammad Nuh, 2012, *Digital Forensic Practical Guide Computer Investigation*, Jakarta: Salemba Infotek

Handoko Cahyo, Position of Digital Evidence in Proof of Cyber Crime in Court, Surakarta: UMS *Jurisprudence Vol 6 Number 1 March 2016*

Hiariej, O.S Eddy, 2012. *Theory & Legal Proof*, Jakarta: Erland.

Maskun, 2013. *Cyber Crime Crime*, Jakarta: Kencana Prenada Media Group.

Suhariyanto, Budi. 2012. *Crime Information Technology (Cybercrime) Urgency Arrangement*

And the Legal Gap, Yogyakarta: Genta Publishing

Understanding-tool-proof-the-legitimate-in.html. Accessed on November 21, 2014