ACQUISITION AND PRESENTATION OF DIGITAL EVIDENCE IN CRIMINAL TRIAL IN INDONESIA

Dewa Gede Giri Santosa
Pengadilan Negeri Gedong Tataan
girisantosa@gmail.com

Karell Mawla Ibnu Kamali
Pengadilan Negeri Kalianda
karellmawla@gmail.com

Received 19-09-2020; Revised 19-07-2022; Accepted 25-07-2022
https://doi.org/10.25216/jhp.11.2.2022.195-218

ABSTRACT

Digital evidence is not defined in Article 184 paragraph (1) of the Criminal Procedure Code but regulated in Law No. 11 of 2008. However, in practice, digital evidence is submitted not only for electronic information and transactions crimes but also to prove crimes in general. Distinct characteristics of digital evidence require different acquisition and presentation methods. Hence, this research examines those methods and how judges evaluate digital evidence. This research is normative legal research, where data sources include research on legal principles, legal system, and legal comparison. The research concluded that Indonesia already has laws and regulations governing the expansion of evidence to include digital evidence. Indonesia also has rules regarding the method of acquisition and presentation of digital evidence in a criminal trial. Therefore, judges must be able to evaluate the validity of digital evidence by observing the method of acquisition and presentation of digital evidence.

Keywords: Criminal Procedural Law; Criminal Trial; Digital Evidence.

INTRODUCTION

Examining the evidence, commonly referred to as the process of proof, is one of Indonesia's most critical stages of a criminal trial. According to M. Yahya Harahap, the proof is a provision that regulates evidence justified by law and admissible evidence for the judge to prove the defendant's guilt. At this stage, a panel of judges who preside over the trial will examine all the evidence presented by the public prosecutor and the defendant or the lawyer in order to determine whether the defendant is guilty of committing the crime as charged or not.[1] Regarding the type of evidence provided by Article 184 paragraph (1) of the Criminal Procedure Code, not all can be used as evidence in the trial. This article states that the valid evidence is the witness testimony, expert testimony, document, circumstantial evidence, and defendant statement.

Although the types of evidence submitted in a criminal trial have been strictly regulated in Article 184 paragraph (1) of the Criminal Procedure Code, as time goes by, a new form of evidence outside of those mentioned in Article 184 emerges. Electronic devices in modern technology nowadays are able to generate or contain a lot of data and information. For example, with the internet, correspondence that used to be done conventionally can now be done by typing a letter via a computer, laptop, or smartphone. Similarly, the rise of social networks such as Facebook, Twitter, and Instagram created a virtual world where people around the world meet each other. Unarguably, technology plays a vital role in the present and the future.[2] Data and information on electronic devices transmitted online are evidence of a legal event. However, the current Criminal Procedure Code did not anticipate such evidence.

In order to fill the legal vacuum, digital evidence was regulated beyond the Criminal Procedure Code, such as on Law No. 31 of 1999

[1] M. Yahya Harahap, *Pembahasan Permasalahan dan Penerapan KUHAP Pemeriksaan Sidang Pengadilan, Banding Kasasi dan Peninjauan Kembali* (Jakarta: Sinar Grafika, 2005), p. 252.
[2] Budi Suhariyanto, *Tindak Pidana Teknologi Informasi (Cybercrime), Urgensi Pengaturan dan Celah Hukumnya* (Jakarta: RajaGrafindo Persada, 2013), p. 1.

concerning Eradication of Corruption as amended by Law No. 20 of 2001, Law No. 21 of 2007 concerning Eradication of the Crime of Human Trafficking, Law No. 11 of 2008 concerning Electronic Information and Transactions as amended by Law No. 19 of 2016, Law No. 35 of 2009 concerning Narcotics, Law No. 8 of 2010 concerning Prevention and Eradication of the Crime of Money Laundering and Law No. 9 of 2013 concerning Prevention and Eradication of Criminal Acts of Terrorism.

Apart from their different forms, the method of obtaining digital evidence shall differ from conventional evidence because digital evidence has different characteristics compared to conventional ones. Meanwhile, one of the fundamental rules is to accept evidence obtained only by means that do not violate the law, as Phyllis B. Gerstenfield argues, which is referred to as exclusionary rules. The exclusionary rule is a legal principle not to acknowledge nor accept evidence obtained against the law[3] Therefore investigators, public prosecutors, and lawyers are obliged to submit digital evidence by paying attention to the method of acquisition and presentation of their evidence. However, nowadays, not all digital evidence submitted on trial is based on lawful acquisition. Therefore judges must be able to measure the validity of every digital evidence on their own.

Based on all these backgrounds, the author is interested in exploring two problems. First, how is the method of acquisition and presentation of digital evidence in criminal trial? Second, how do judges evaluate the validity of digital evidence submitted in criminal trial?

This legal writing is normative legal research, where the data sources include research on legal principles, legal system, and legal comparison. In order to obtain accurate information and data on various issues related to this legal writing, writers use statute, comparative, and conceptual approaches. The statutory approach reviews all laws and regulations relating to digital evidence in procedural

[3] Phyllis B. Gerstenfield, *Crime & Punishment in the United States* (Pasadena California: Salem Press, Inc., 2008), p. 348.

law. This approach identifies and maps laws and regulations relating to digital evidence, as well as the coherence and consistency of its regulations. The comparative approach is carried out by comparing the laws on digital evidence in criminal procedural law in several countries in the world with the laws and regulations in Indonesia. A conceptual approach is needed to gain insight or ideas regarding obtaining and presenting digital evidence in criminal proceedings and how wise and prudent judges examine each digital evidence submitted.

This descriptive-analytic research describes and analyzes all the legal sources above, then identifies and finds the legal principles of several related regulations. The researcher will find a concept/legal principle relevant to the issue.

Digital Evidence in Indonesian Criminal Procedural Law

In general, the law can be divided into several fields. A. M. Bos and Lemaire divide the legal field into material and formal law. Material law contains relations between humans or regulates rights and obligations. In contrast, formal law is associated with the enforcement of material law, which regulates formal procedures or procedures to protect violated rights.[4] Likewise, material and formal criminal law are known in criminal law. The material criminal law regulates prohibited acts and their sanctions, and the formal criminal law regulates all matters related to the enforcement of material criminal law.

Formal criminal law in Indonesia is arranged in Law No. 8 of 1981 concerning the Criminal Procedure Code enacted on December 31, 1981.[5] The law regulates investigation, prosecution, trial, pretrial, court decision, legal remedies, confiscation, searches, detention, and others.[6] At the trial level, one of the stages that play an essential role is the proof stage. At this stage, the prosecutor will submit evidence that can prove

[4] Wahyu Sasongko, *Dasar-Dasar Ilmu Hukum* (Bandar Lampung: Universitas Lampung, 2010), p. 19.
[5] C. Djisman Samosir, *Hukum Acara Pidana* (Bandung: Nuansa Aulia, 2018), p. 1.
[6] Andi Hamzah, *Hukum Acara Pidana* (Jakarta: Sinar Grafika, 2008), p. 4.

the indictment. On the other hand, the defendant or the lawyer will submit adversary evidence that can refute the charges or at least lighten the defendant's sentence.

Evidence in a criminal trial in Indonesia has been regulated in a limitative manner in Article 184 paragraph (1) of the Criminal Procedure Code. Hence both the public prosecutor and the defendant or the lawyer cannot submit any evidence in a criminal trial but one already mentioned in Article 184. Any evidence other than that has no value before the judges and does not have binding evidentiary power.[7] Based on this Article, there are several types of evidence:

1. Witness testimony

Based on Article 1, number 27 of the Criminal Procedure Code, witness testimony is testimony from a witness regarding a criminal event that he/she has heard, seen, or experienced himself/herself by stating the reasons for his/her knowledge. The definition of witnesses through the Constitutional Court Decision No. 65/PUU-VIII/2010 was later expanded to include people who can provide information in the context of an investigation, prosecution, and trial of a criminal act which he/she did not always hear, see and experience himself/herself. According to the Constitutional Court, the significance of a witness does not lie in whether he/she saw, heard, or personally experienced a criminal event but in the relevance of his/her testimony to the criminal case proceeded.

2. Expert testimony

Arthur Best argues that expert testimony is testimony based on experience in general and knowledge based on his expertise on the facts of a case. Expert testimony is frequently necessary regarding information or analysis of a fact to convince the jury or judge at trial.[8] In Indonesia, expert testimony is defined in Articles 1 and 28 of the

[7] Syaiful Bakhri, *Hukum Pembuktian Dalam Praktik Peradilan Pidana* (Yogyakarta: Total Media, 2009), p. 46.
[8] Arthur Best, *Evidence: Examples and Explanations* (Boston-New York-Toronto-London: Little, Brown and Company, 1994), p. 157.

Criminal Procedure Code as information provided by a person with special expertise on particular matters to clarify a criminal case.

3. Document

Document as evidence is regulated in Article 187 of the Criminal Procedure Code. According to these provisions, documents that can be considered valid evidence if made officer under an oath or confirmed by an oath, namely:

a. minutes and other documents in an official form prepared by an authorized public official or before him, which contain information about events or conditions he has heard, seen, or experienced, accompanied by clear and emphatic reasons for the statement;
b. the document made under the provisions of laws and regulations or a document made by an officer regarding a matter which is included in the management which is his responsibility and which is intended to prove something;
c. an expert opinion based on his expertise regarding a matter or condition which has been formally requested from him;
d. another document that can only be valid if it is related to the contents of other means of proof.

4. Circumstantial evidence or eigen waarneming van den rechter

Article 188 paragraph (1) of the Criminal Procedure Code stipulates that circumstantial evidence is an act, event, or situation that, because of its compatibility, either between one another or with the criminal act itself, indicates that a criminal act has occurred and who the perpetrator is. Circumstantial evidence is fully authorized to the judge who presides over the trial. To conclude, circumstantial evidence must relate to other existing evidence. Therefore, circumstantial evidence is used if current evidence has unable to form the judge's conviction about the occurrence of a criminal act and the conviction that the defendant

committed it.[9] Circumstantial evidence can only be obtained from witness testimony, documents, and defendant statement.

5. Defendant's statement

Article 189 paragraph (1) of the Criminal Procedure Code defines the defendant's statement as what the defendant stated at the hearing about the deeds he/she has done or what he/she knew or experienced by himself/herself. Article 189 paragraph (4) of the Criminal Procedure Code also stipulates that a defendant's statement alone is insufficient to prove that he/she is guilty of the act he/she is accused of but must be accompanied by other evidence. In other words, if, in a criminal case, a defendant has admitted that he/she is guilty and has committed the criminal offense charged, the judge cannot immediately issue a verdict regarding the defendant's guilt or innocence based solely on the defendant's admission. Defendant's statement must be supported by other evidence adhering to the principle of bewijs minimum.

Over time, the types of evidence presented in a criminal trial were not limited to the five types of evidence. The development of science encourages civilization to be more advanced than in previous times, and social interactions that occur conventionally gradually shift with the discovery of various electronic means that can facilitate life in interaction. Many legal actions occur through electronic means, and many criminal acts are closely related to cyberspace. For example, in the past, when someone wanted to communicate with people in other countries, they would use correspondence via mail post to share stories. However, these tools were considered to be time-consuming and inefficient. Nowadays, people can communicate across countries using e-mail.

Therefore, e-mail can be considered a legal act when it contains rights and obligations. E-mail can also violate the rights of others and even fall under criminal acts. For example, in Prita Mulyasari's case, she

[9] Eddy O.S Hiariej, *Teori dan Hukum Pembuktian* (Jakarta: Erlangga, 2012), p. 111.

sent a letter via e-mail and was later sentenced to defamation charges. Prita Mulyasari's trial was flooded with digital evidence, which was not accommodated in Article 184 paragraph (1) of the Criminal Procedure Code.

In various special criminal laws, digital evidence is formulated explicitly and has the power to act as valid evidence. However, those acts rule digital evidence status differently. Some acts recognize digital evidence as an extension of evidence, while others recognize it as a piece of stand-alone evidence.[10] For example, Article 26 A letter an of Law No. 20 of 2001 stated: 'Legal evidence in the form of circumstantial evidence as referred in Article 188 paragraph (2) Law No. 8 of 1981 concerning Criminal Procedure Code, specifically to corruption can also be obtained from: a. other evidence in the form of information uttered, sent, received, or stored electronically using optical devices or else'. Article 5 paragraph (2) of the Law on Information and Electronic Transactions regulates that 'Electronic Information and/or Electronic Documents and/or their printouts as referred to in paragraph (1) constitute an extension of legal evidence under the procedural law in Indonesia'. When referring to Article 26A letter a of Law No. 20 of 2001, digital evidence is circumstantial evidence, while in Article 5 paragraph (2) of Law No. 11 of 2008, digital evidence is a piece of stand-alone evidence and holus-bolus an extension of valid evidence as regulated in the criminal procedural law in Indonesia. There are several laws in Indonesia that regulate digital evidence:

Table 1. Status of Digital Evidence in some Laws and Regulations

NO	CONSTITUTION	STATUS
1	Article 15 paragraph (1) of Law No. 8 of 1997 concerning Company Documents	Evidence
2	Article 26 A of Law No. 20 of 2001 concerning Eradication of Corruption	Circumstantial evidence

[10] Sigid Suseno, *Yurisdiksi Tindak Pidaan Siber* (Bandung: Refika Aditama, 2012), p. 222.

3	Article 38 of Law No. 15 of 2002 concerning the Crime of Money Laundering	Evidence
4	Article 29 of Law No. 21 of 2007 concerning the Eradication of the Crime of Trafficking in Persons	Evidence
5	Article 5 Paragraph (2) and Article 44 of Law No. 11 of 2008 jo. Law No. 19 of 2016 concerning Electronic Information and Transactions	Evidence
6	Article 96 letter f of Law No. 32 of 2009 concerning Environmental Protection and Management	Evidence
7	Article 86 Paragraph (2) of Law No. 35 of 2009 concerning Narcotics	Evidence
8	Article 73 Law No. 8 of 2010 concerning the Prevention and Eradication of Money Laundering	Evidence
9	Article 38 of Law No. 9 of 2013 concerning Prevention and Eradication of Terrorism Financing Crimes	Evidence
10	Article 37 of Law No. 18 of 2013 concerning Prevention and Eradication of Forest Destruction	Evidence

Based on the table, it can be seen that there are differences in the regulation concerning the status of digital evidence in the respective laws. Meanwhile, the differences between the laws can be answered through a generally accepted legal principle: lex posterior derogat legi priori, which means that the latest law (lex posterior) overrides the old law (lex prior).[11] In this principle, lex prior (which starts from the Law on Criminal Acts of Money Laundering to the Law on the Prevention and Eradication of Forest Destruction) considers digital evidence as stand-alone evidence that extends existing evidence. Thus, digital

[11] Soedikno Mertokusumo, *Penemuan Hukum Sebuah Pengantar* (Yogyakarta: Liberty, 2009), p. 121.

evidence has been recognized as additional legal evidence in criminal law in Indonesia.

The question is whether digital evidence is admissible as valid evidence in all criminal cases or only acknowledged for certain crimes regulated in special criminal laws such as corruption, human trafficking, narcotics, money laundering, terrorism, and criminal acts related to information and electronic transactions.

In Decision Number 20/PUU-XIV/2016, Constitutional Court create a landmark decision that an unauthorized interception and the recorded files are an infraction of human rights; therefore, it is illegal and shall only be authorized by an Act. If the files presented before the judge were obtained unlawfully, the judge should nullify and regard them as invalid evidence.

That decision was criticized because the Constitutional Judge barely considered the interception related to a certain corruption case. In contrast, corruption was an extraordinary crime and, as a result, needed extraordinary measures.[12] Regarding general crimes, this decision clarified that the acquisition method to obtain and evaluate electronic evidence should be conducted lawfully; hence it is admissible as valid evidence before the court.

Article 2 of the Criminal Procedure Code defines that this law applies to judicial procedures in trials at all levels. Furthermore, Article 3 demands that the trial shall be carried out in a manner regulated by this law. Based on these two articles, all procedures for enforcing criminal law in Indonesia must be conducted in accordance with Criminal Procedure Code and yet Criminal Procedure Code does not regulate the existence of digital evidence.

However, as previously described, digital evidence has been accepted and regulated in various special laws. Criminal Procedure Code as a general law shall follow lex specialis derogat legi generali principle,

[12] Ahmad Rifqi Hasbulloh, 2017, *Analisis Putusan Mahkamah Konstitusi Nomor 20/PUU-XIV/2016 Terhadap Kewenangan Penyadapan KPK*, Thesis, Universitas Islam Indonesia, Yogyakarta, p. 94-95.

which means special law overrides general law. Based on those arguments, Law No. 11 of 2008 juncto Law No. 19 of 2016 concerning Electronic Information and Transactions, which has regulated digital evidence as valid evidence, shall be used as a basis to measure digital evidence as valid evidence on trial.[13] Efa Laela Fakhriah argued that digital evidence regulation was not clear enough. Therefore, judges were tied to the principle of ius curia novit, which means the "court knows the law." The judges cannot refuse to decide the case even if the law is unclear or non-existent. Judges are obliged to explore values that grow within the society and decide justly.

Referring to Article 1, number 1 and 4, as well as Article 5, paragraph (1), (2), and (3) of the Law on Electronic Information and Transactions, this law generally applies and does not limit itself to certain cases. Furthermore, Article 5 paragraph (2) of Law No. 11 of 2008 confirms that Electronic Information and/or Electronic Documents and/or printouts thereof are an extension of valid evidence under the applicable procedural law in Indonesia. Based on this article, Law on Information and Electronic Transactions have provided the legal basis that digital evidence is admissible in procedural law in Indonesia, the procedural law is also not limited to the laws of a particular event. This rule can be a legal basis for accepting digital evidence as valid evidence in Indonesia's criminal procedure and civil procedural law.

[13] Efa Laela Fakhriah, *Kedudukan Bukti Elektronik sebagai Alat Bukti di Pengadilan Setelah Berlakunya Undang-Undang No. 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik*, the paper was presented at the Limited Seminar on the collaboration of the Research and Development and Education and Training Agency for Law and Justice of the Supreme Court of the Republic of Indonesia with universities with the theme: *Validitas Alat Bukti Transaksi Elektronik Perbankan Sebagai Alat Bukti Di Pengadilan Setelah Berlakunya Undang-Undang No. 11 Tahun 2008*, Grand Pasundan Hotel, Bandung, held on 25 Nov 2009, p. 15.

Acquisition and Presentation of Digital Evidence in Criminal Trial

Eddy OS Hiariej states that there are at least four things that need to be considered regarding the concept of proof, namely:[14]

1. Evidence must be relevant to the case;
2. Evidence must be admissible;
3. Un-acknowledgement of evidence obtained against the law;
4. The judge must evaluate any evidence that is relevant and admissible.

Based on these four points, the evidence submitted in a criminal trial must be relevant, meaning that the evidence is related to the facts that point to the truth of the incident. Furthermore, for evidence to be admissible, it must be obtained only by means that do not violate the law, as said by Phyllis B. Gerstenfield, referred to as exclusionary rules, namely legal principles that require the non-recognition of evidence obtained against the law[15] Therefore, for digital evidence to be admissible, the acquisition and presentation of digital evidence at a criminal trial must not violate the law.

The exclusionary rules also emphasized in Constitutional Court Decision Number 20/PUU-XIV/2016 that an unauthorized interception and the recorded files are an infraction of human rights; therefore, it is illegal and shall only be authorized by an Act. As the Decision was written, there has been no Act to regulate how a lawful interception is taken. Therefore, to fill the status quo, The Constitutional Court decided that the "electronic information and/or electronic document" phrase in Article 5 and 44 of the ITE Act and Article 26A of the Crime of Corruption Act must be defined as "electronic information and/or electronic document" as evidence of law enforcement per requested by the police, attorney, and/or other law enforcer unit stated by an Act."

In comparison, Title III of the Omnibus Crime and Safe Street Act 1968 in America determined that all wiretapping must be carried

[14] Eddy O.S Hiariej, *Teori dan Hukum Pembuktian*…, p. 10-12.
[15] Phyllis B. Gerstenfield, *Crime & Punishment in the United States*…, p. 348.

out with the local court's permission. However, with the court's permission, there are exceptions if eavesdropping is done on communications within urgent circumstances that endanger the safety of the lives of others. With this, a conclusion can be drawn from the statement of Title III, The Omnibus Crime and Safe Street Act 1968, concerning wiretapping and recording; both activities must be carried out with the court's permission (law enforcement officers). New provisions regarding this electronic evidence poured into Law Number 19 of 2016 concerning Amendments to Law Number 11 of 2008 concerning Information and Electronic Transactions result from the Constitutional Court Decision Number 20/PUU-XIV/2016.

The method of acquisition and presentation of digital evidence is closely related to the search and seizure. The Law on Information and Electronic Transactions also regulates the search and seizure of digital evidence by Article 43 paragraph (3). In this article, 'search and/or seizure of Electronic Systems related to suspected criminal acts in the Information Technology and Electronic Transactions field are carried out under the provisions of criminal procedural law. Unfortunately, the law does not explain further the provisions of the criminal procedural law in question. Referring to this article, search and seizure of digital evidence are carried out using the same method as the search and seizure of conventional evidence regulated in the Criminal Procedure Code. However, the acquisition of digital evidence cannot be equated to the acquisition of evidence in a conventional manner, considering their distinct characteristics. Digital evidence has volatile properties and is easily modified, manipulated, or destroyed. Furthermore, accessing digital evidence frequently requires special tools and skills.

For example, other countries such as the UK and the United States. Both countries have standard rules regarding the search and seizure of digital evidence. These standard rules are listed in the Good Practice Guide for Computer-Based Digital evidence, Association of Chief Police (ACPO) in the UK, and Electronic Crime Scene Investigation: A Guide for First Responders, Second Edition, US

Department of Justice, in the United States. In the ACPO, to ensure that the digital evidence submitted is relevant to criminal cases being processed, Section 4.3.1 clarifies that a device should only be seized if it is likely to hold evidence and the police have reasonable grounds to do so. Additionally, officers are warned that 'digital devices and media should not be seized just because they are there.'[16]

Besides search and seizure, examining and reporting digital evidence are also essential for a judge to evaluate whether the digital evidence is admissible. Max M. Houck stated that evidence obtained illegally or tainted evidence shall not be used and cannot substantiate a case.[17]

Although the Law on Electronic Information and Transactions does not thoroughly regulate the procedures of seizure, examination, and reporting of digital evidence in criminal proceedings, the Law on Electronic Information and Transactions contains principles that law enforcers must follow. This is regulated in Article 43 paragraph (2), which states 'Investigations in the field of Information Technology and Electronic Transactions as referred to in paragraph (1) shall be carried out with due observance of the protection of privacy, confidentiality, public interest, data integrity, or data wholeness under the provisions of the Laws and Regulations. That means investigations in information technology and electronic transactions must pay attention to protect privacy, confidentiality, public interest, data integrity, and data wholeness.

In fact, in Indonesia, there are regulations regarding the procedures for seizure, examination, and reporting of digital evidence, namely in the Regulation of the Minister of Communication and Information Technology No. 7 of 2016 concerning Administration of Criminal Investigation and Enforcement in the Field of Information

[16] Association of Chief Police Officers, "Good Practice Guide for Digital Evidence" (March 2012), http://www.digital-detective.net/digital-forensics-documents/ACPO_Good_Practice_Guide_for_Digital_Evidence_v5.pdf, accessed July 6, 2020.
[17] Max M. Houck, *Essentials of Forensic Science: Trace Evidence* (New York: An Imprint of Infobase Publishing, 2009), p. 3.

Technology and Electronic Transactions. In Article 40 paragraph (2) of this Ministerial Regulation, it is stipulated that those subject to seizure are:

1. Objects or claims that all or part of it are suspected to be obtained from a criminal act or as a result of a criminal act;
2. Objects that have been directly used to commit a crime or to prepare it;
3. Objects that are used to obstruct a criminal investigation;
4. Objects specially made or intended to commit a criminal act;
5. Other objects that have a direct relationship with the criminal act committed;
6. Electronic Systems, Electronic Information, or Electronic Documents obtained through a forensic process against the Electronic Systems being searched.

Then, in the Ministerial Regulation, it is also stipulated that digital forensics consists of identification, acquisition, examination, analysis, documentation, and reporting. Regarding implementing those procedures, Article 46 paragraph (5) of the Regulation of the Minister of Communications and Information Technology No. 7 of 2016 demands a technical guideline laid by the director general, but none to be found. The procedures of identification, acquisition, examination, analysis, documentation and reporting are based on the ISO 27037:2014 regarding Security techniques - Guidelines for the Identification, Collection, Acquisition, and Preservation of Digital Evidence.[18]

There are at least four steps that must be taken to obtain digital evidence, namely:

1. Identification

   The identification process in ISO 27037 consists of:

[18] Dedy Hariyadi, et al.., "Analisis Barang Bukti Digital Aplikasi Paziim pada Ponsel Cerdas Android dengan Pendekatan Logical Acquisition", *Cyber Security dan Forensik Digital*, Vol. 2, No. 2 (2019), p. 53-54.

a. The Identification stage involves identifying several media but is not limited to data storage media, electronic devices, and network activity logs from internet providers.
b. The collection stage is collecting as much data as possible to support the investigation process in the search for evidence.
c. The preservation stage is a series of activities to ensure that the data that has been determined as potential data contains evidence that is not damaged or changed and considers incidents that may occur due to external influences so that appropriate preventive measures must be taken.
d. The acquisition stage is taking data from a device using forensic tools.

2. Data Examination

The examination or inspection stage involves analyzing the data contained in the media. This stage must be carried out by personnel who understand specific forensic data analysis techniques. The analysis method consists of identifying electronic documents containing certain keywords, analysis of operating systems, compressed and encrypted data, analysis of computer and network activity logs, and other analyses that can reduce the number of documents that may become evidence of criminal acts. The data is then extracted for further analysis.

3. Analysis

The analysis process is carried out by making a mapping from the extracted data. The analysis results can show the parties involved, the location, objects likely to be the result of a criminal act, and a series of events. The results of the digital data analysis are hereinafter referred to as digital evidence, which must be accounted for technically and legally in front of the trial.

4. Reporting

The entire series of activities and outputs obtained from the previous processes is written as a report.

5. Evidence Management

After the entire process is completed, the evidence must be managed to avoid change or damage, considering that digital evidence has special properties and characteristics, different from conventional evidence in general.

Article 46 paragraph (4) Regulation of the Minister of Communication and Information Technology No. 7 of 2016 underlines that the identification, acquisition, examination, analysis, documentation, and reporting of digital evidence shall maintain privacy, confidentiality, public interest, and data integrity, or data wholeness.

Regulation of the Minister of Communication and Information Technology No. 7 of 2016 has provided a legal basis for seizure procedures, examination, and reporting of digital evidence on criminal trials. However, this ministerial regulation applied exclusively to crimes regulated in the Law concerning electronic information and Transactions. In other words, it does not cover common criminal offenses or specific crimes outside of Law on Electronic Information and Transactions.

The absence of clear rules regarding the procedures for seizure, examination, and reporting of digital evidence for criminal acts outside of those regulated in the Law on Electronic Information and Transactions has led investigators to ignore forensic principles of digital evidence. This condition can lead to some negative impacts, such as:

1. Vulnerability of violations of the privacy rights held by electronic device owners because of insufficient legal protection for personal data within the device;
2. Legal uncertainty for investigators who seize the suspected devices;
3. Judges who examine criminal cases find evaluating the integrity of electronic data/documents presented at trial challenging.

Hence, to address those problems, the government is urged to regulate the clear procedure of digital evidence acquisition and presentation for criminal offenses outside of Law on Information and Electronic Transactions.

Judge's Evaluation of Digital Evidence in Criminal Trial

Defendant has a right to proof of guilt beyond a reasonable doubt. Evidence in criminal procedural law in Indonesia aims to seek the material truth, unlike civil procedural law, which only seeks formal truth.[19] The criminal proof system in Indonesia itself adopts a system of proof based on negatief wettelijk bewijstheori.[20] Therefore, a judge must consider the evidence regulated in law, and the judge's conviction is obtained from the evidence.

As Law on Electronic Information and Transactions was established, digital evidence has become a type of evidence that is legal and acceptable in criminal procedural law in Indonesia. However, it is still the judge's duty to examine whether the digital evidence presented in trial is relevant, admissible, and obtained based on a law-compliant procedure.

In case of submission of digital evidence for crimes regulated in the Law on Information and Electronic Transactions, Judges shall observe the method of its acquisition and presentation by referring to the Law on Information and Electronic Transactions and the Regulation of the Minister of Communication and Information Technology No. 7 of 2016. Judges can evaluate the method of acquisition and presentation of digital evidence by examining documents at the investigation level, such as Search and Seizure Warrants, Search and Seizure Permits or Approval, and Information Technology Expert Examination Minutes, Digital Forensic Examination Minutes, or Computer Forensic Examination Minutes.

Whereas to examine digital evidence on criminal offenses outside of the Law on Information and Electronic Transactions, judges may refer to the material and formal requirements stipulated in the Law on Information and Electronic Transactions. Formal requirements are regulated in Article 5 paragraph (4) of the Law on Electronic

[19] Subekti, *Hukum Pembuktian* (Jakarta: Praniya Paramita, 2005), p. 9.
[20] Hari Sasangka, *Hukum Pembuktian dalam Acara Pidana* (Bandung: Mandar Maju, 2003), p. 16.

Information and Transactions, namely that Electronic Information or Documents are not documents or letters that, according to the law, must be written. Meanwhile, the material requirements are regulated in Article 6, Article 15, and Article 16 of the Law on Electronic Information and Transactions, in short, Electronic Information and Documents must be guaranteed their authenticity, integrity, and availability.[21] Although the procedures for seizure, examination, and reporting of digital evidence for criminal acts outside of those stipulated in the Law on Electronic Information and Transactions do not yet have clear legal rules, judges are obliged to explore legal values that grow and develop in society, one of which is also can make the Minister of Communication and Information Technology Regulation No. 7 of 2016 as a means for legal discovery.

There are several things that a judge can do in evaluating digital evidence regarding the method of its acquisition and presentation in the criminal trial, namely:

First, if the digital evidence presented is relevant, admissible, and the procedure of acquisition and presentation is carried out regarding the principles and procedures as regulated in Law on Information and Electronic Transactions and also the Regulation of the Minister of Communication and Information Technology No. 7 of 2016, the digital evidence can be accepted as valid evidence, and the judge can use the digital evidence to strengthen whether or not a criminal act is proven.

Second, if the digital evidence submitted at trial is relevant but the acquisition and presentation violate the principles stipulated in the Law on Electronic Information and Transactions or violate the seizure, examination, and reporting procedures stated in the Regulation of the Minister of Communication and Information Technology No. 7 of 2016, judges can set aside those evidence as it does not have the power/value of proof. Moreover, even though the digital evidence is relevant and admissible, judges may ignore the evidence if it was not

[21] Josua Sitompul, *Cyberspace, Cybercrimes, Cyberlaw : Tinjauan Aspek Hukum Pidana* (Jakarta: Tatanusa, 2012), p. 275.

obtained according to the rules.[22] At a more extreme level, for countries that use the due process model, the pretrial hearings often acquit a suspect because the evidence is obtained by illegal means or what is known as unlawful legal evidence.[23] However, in Indonesia, there have not been any cases of suspects released in pretrial due to unlawful legal evidence. The Criminal Procedure Code does not authorize pretrial to decide on the illegality of obtaining evidence.

Third, suppose the decisive digital evidence is obtained illegally so that it cannot be accepted as evidence. In that case, it turns out that not accepting the digital evidence means that the minimum evidence required in the proof is not fulfilled (bewijs minimum), and the judge can release the defendant from charges because the public prosecutor has failed to prove the charges.

Fourth, suppose the method of acquisition and presentation of digital evidence submitted at the trial are not following the principles stipulated in the Law on Electronic Information and Transactions nor the Regulation of the Minister of Communication and Information Technology No. 7 of 2016. Meanwhile, the digital evidence corresponds to the witness's testimony, defendant's statement, or documents. In that case, this can be used as an indication to strengthen the judge's conviction, for example, in a criminal act of theft that involved several people who collaborated using the Whatsapp chat media. Later, prosecutors presented those chats as evidence in the form of a printed screenshot which investigators obtained by taking screenshots directly from the defendant's smartphone without going through forensic measures. Meanwhile, in the trial, neither the witnesses nor the defendant denies and even confirms the truth about the Whatsapp chat. In such a case, even though the printout of the Whatsapp chat screenshot was rendered inadmissible because it was obtained through invalid acquisition, those printouts can be used by the judge as a tool to strengthen the judge's conviction about the defendant's guilt by

[22] Eddy O.S Hiariej, *Teori dan Hukum Pembuktian*…, p. 11.
[23] Eddy O.S Hiariej, "Kinerja Polisi", *Kompas* (6 November 2003), p. 37.

correlating the printout with the witnesses testimony, defendant statement, and other evidence available.

Conclusion

Evidence in a criminal trial in Indonesia has been strictly regulated in Article 184 paragraph (1) of the Criminal Procedure Code. However, as time goes by, it is not uncommon for evidence to be found in electronic devices or stored in cyberspace. The development of this type of evidence has led to the establishment of a particular law regulating the expansion of evidence to include digital evidence, one of which is Law No. 11 of 2008 concerning Electronic Information and Transactions as amended by Law No. 19 of 2016. These laws have provided a legal basis that digital evidence is acceptable as legal evidence in Indonesian criminal procedure law.

Besides their different forms, obtaining digital evidence also needs a special measure. Therefore, the Minister of Communication and Information Technology Regulation No. 7 of 2016 issued a legal basis for the acquisition and presentation of digital evidence to be submitted in the criminal trial. However, the criminal acts referred to in this ministerial regulation are limited to criminal acts stipulated in the Law on Electronic Information and Transactions. This result in the absence of clear rules regarding the method of acquisition and presentation of digital evidence for criminal acts outside of those stipulated in the Law on Electronic Information and Transactions. Hence, to address this problem, the government is urged to regulate clear procedures of digital evidence acquisition and presentation for criminal offenses outside of the Law on Information and Electronic Transactions.

Even though it has been accepted as valid evidence, judges must still evaluate whether the digital evidence presented in the criminal trial is relevant, admissible, and obtained based on a law-compliant procedure. Suppose there is a submission of digital evidence for criminal acts regulated in the Law on Electronic Information and Transactions. In that case, judges are obliged to pay attention to the

method of acquisition and presentation of digital evidence based on the Law on Electronic Information and Transactions and the Minister of Communication and Information Technology Regulation No. 7 of 2016. Judges can evaluate the method of acquisition and presentation of digital evidence by examining documents at the level of investigation, such as Search and Seizure Warrants, Search and Seizure Permits or Approval, and Information Technology Expert Examination Minutes, Digital Forensic Examination Minutes, or Computer Forensic Examination Minutes.

While there is no rule to provide judges a clear legal basis to address those problems, judges by law are obliged to explore legal values that grow and develop in society. Meanwhile, to examine digital evidence in criminal offenses other than those regulated in the Law on Electronic Information and Transactions, as long as it is not ruled clearly, judges may refer to the principles stipulated in the Law on Electronic Information and Transactions. Judges may also explore the legal values contained in the Law on Electronic Information and Transactions and Regulation of the Minister of Communication and Information Technology No. 7 of 2016.

Bibliography

Association of Chief Police Officers, "Good Practice Guide for Digital Evidence" (March 2012), http://www.digital-detective.net/digital-forensics-documents/ACPO_Good_Practice_Guide_for_Digital_Evidence_v5.pdf, accessed July 6, 2020.

Bakhri, Syaiful, Hukum Pembuktian Dalam Praktik Peradilan Pidana, Yogyakarta: Total Media, 2009.

Best, Arthur, Evidence: Examples and Explanations, Boston-New York-Toronto-London: Little, Brown and Company, 1994.

Fakhriah, Efa Laela, Kedudukan Bukti Elektronik sebagai Alat Bukti di Pengadilan Setelah Berlakunya Undang-Undang No. 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik, the paper was presented at the Limited Seminar on the collaboration of the

Research and Development and Education and Training Agency for Law and Justice of the Supreme Court of the Republic of Indonesia with universities with the theme: Validitas Alat Bukti Transaksi Elektronik Perbankan Sebagai Alat Bukti Di Pengadilan Setelah Berlakunya Undang-Undang No. 11 Tahun 2008, Grand Pasundan Hotel, Bandung, held on 25 Nov 2009.

Gerstenfield, Phyllis B., Crime & Punishment in the United States, Pasadena California: Salem Press, Inc., 2008.

Hamzah, Andi, Hukum Acara Pidana, Jakarta: Sinar Grafika, 2008.

Harahap, M. Yahya, Pembahasan Permasalahan dan Penerapan KUHAP Pemeriksaan Sidang Pengadilan, Banding Kasasi dan Peninjauan Kembali, Jakarta: Sinar Grafika, 2005.

Hariyadi, Dedy, et al.., "Analisis Barang Bukti Digital Aplikasi Paziim pada Ponsel Cerdas Android dengan Pendekatan Logical Acquisition", Cyber Security dan Forensik Digital, Vol. 2, No. 2 (2019), p. 52-56.

Hasbulloh, Ahmad Rifqi, 2017, Analisis Putusan Mahkamah Konstitusi Nomor 20/PUU-XIV/2016 Terhadap Kewenangan Penyadapan KPK, Thesis, Universitas Islam Indonesia, Yogyakarta.

Hiariej, Eddy O.S, "Kinerja Polisi", Kompas (6 November 2003).

Hiariej, Eddy O.S, Teori dan Hukum Pembuktian, Jakarta: Erlangga, 2012.

Houck, Max M., Essentials of Forensic Science: Trace Evidence, New York: An Imprint of Infobase Publishing, 2009.

Mertokusumo, Soedikno, Penemuan Hukum Sebuah Pengantar, Yogyakarta: Liberty, 2009.

Samosir, C. Djisman, Hukum Acara Pidana, Bandung: Nuansa Aulia, 2018.

Sasangka, Hari, Hukum Pembuktian dalam Acara Pidana, Bandung: Mandar Maju, 2003.

Sasongko, Wahyu, Dasar-Dasar Ilmu Hukum, Bandar Lampung: Universitas Lampung, 2010.

Sitompul, Josua, Cyberspace, Cybercrimes, Cyberlaw : Tinjauan Aspek Hukum Pidana, Jakarta: Tatanusa, 2012.

Subekti, Hukum Pembuktian, Jakarta: Praniya Paramita, 2005.

Suhariyanto, Budi, Tindak Pidana Teknologi Informasi (Cybercrime), Urgensi Pengaturan dan Celah Hukumnya, Jakarta: RajaGrafindo Persada, 2013.

Suseno, Sigid, Yurisdiksi Tindak Pidaan Siber, Bandung: Refika Aditama, 2012.