KnE Social Sciences
INCLAR
3rd International Conference on Law Reform (3rd INCLAR)
Volume 2022

Conference Paper

The Urgency of Establishing Guidelines for Handling Cybercrime Cases in the Indonesian National Police Department

Cindy Monique[1], Isdian Anggraeny[2]*, Yohana Puspitasari Wardoyo[2], Aprilia Bhirini Slamet[2]

[1]Master of Law, Universitas Brawijaya, Malang, Indonesia
[2]Faculty of Law, University of Muhammadiyah Malang, Malang, Indonesia

ORCID
Cindy Monique: https://orcid.org/0000-0001-8735-0676
Isdain Anggraeny: https://orcid.org/0000-0002-1981-0412

Abstract.
Technological development has a strong influence on the development of criminals. In the past, crimes were carried out in conventional ways and tools, but now crimes are carried out in modern ways. Cybercrime is a borderless crime and requires special treatment when collecting digital evidence. Evidence in cyber crime allows criminals to hide or remove their tracks. Until now, Indonesian National Police (POLRI) does not have any case management guidelines for storing digital evidence using digital forensic methods. This research aims to determine what steps investigators take in obtaining digital evidence, whether these steps have been effective in law enforcement, or whether they are still unclear. The method in this writing is normative legal research based on a statute approach and a conceptual approach. The author offers to establish guidelines for handling cyber crime cases in the Indonesian National Police by relying on digital forensic methods by strengthening and choosing the right tools for handling cases.

Keywords: cybercrime, digital evidence, digital forensic

Corresponding Author: Isdian Anggraeny; email: isdian@umm.ac.id

Published: 4 October 2022

Publishing services provided by Knowledge E

Selection and Peer-review under the responsibility of the INCLAR Conference Committee.

1. INTRODUCTION

As social beings, humans certainly live in a particular group in a clump of society that interacts with each other to meet the needs of one another. Humans have primary and secondary needs, besides that, they also have needs in the form of social relationships with other humans. The scope of social relations between humans and other humans, along with the times, has also undergone significant changes. In the past, when we wanted to interact, we could only interact in a small area and were limited by space and time. After the development of the times, the way humans communicate and conduct social relations is not limited by region, distance, even space and time. This is due to the creation of a new dimension, namely information and communication technology

The widespread growth of cybercrime is hitting countries around the world. Cybercrimes have caused significant losses to the country's economy. With the development of humans in terms of socializing, it will more or less change the mindset of humans from simple things to unlimited. This information and communication technology emerged with discoveries related to the means to establish social relations, namely with the invention of the radio, television, the telephone, etc. In 1969, the United States Department of Defense through the ARPANET project (Advanced Research Project Agency Network) formed a computer network, namely with UNIX-based hardware and software (what does it stand for)? Humans could communicate within an infinite distance through telephone lines, which were later developed which was then developed until the end of the year. currently continuing to develop and we are familiar with the internet.[1]

Cyber crime utilizes several public and private communication systems, from satellite communications to wireless sensor networks, cellular networks, and the internet.[2]

The presence of the internet which is a connecting medium as well as a tool for humans to carry out social interactions and opens up new spaces that even penetrate borders between countries so quickly in capturing and sending electronic-based information which is of course very easy for humans to communicate with other humans. However, behind the convenience offered to the public for the emergence of this internet, of course, there are negative impacts, one of which will be in the spotlight in this paper is the existence of cyber crimes or cybercrime.

Before the advent of the internet, crimes were committed in conventional and limited ways and the space for movement could still be identified, but after the internet, crimes were committed in various ways and became unlimited, which means that crimes can be committed anytime, anywhere, and through any media as long as they are connected to a connection. existing internet. This conventional crime is complicated because it can be done in cyberspace or known as cyberspace.

Cybercrime has various types which include: unauthorized access to computer systems and services, illegal contents, data forgery, cyber espionage, cyber sabotage and extortion, offense against intellectual property, infringements of privacy, cracking, and carding, etc.[3]

Cybercrime in Indonesia was identified as occurring in the span of 1983, which was the first time this had occurred in the banking sector. In later years, what has developed until now has become many kinds. Starting from piracy of computer programs, cracking, carding, bank fraud, pornography, and even domain names. In addition, other crimes are smuggling pornographic images or videos(cyber smuggling), page jacking, spam

(junk mail), intercepting, cybersquatting. Meanwhile, cybercrime cases against computer systems or networks include defacting, denial of service attack (DoS), distributed denial of service attack (DDoS), spread of viruses (worms), and installation of logic bombs.[4]

Electronic evidence and the existence of electronic evidence or digital evidence in cybercrime prior to Law Number 11 of 2008 concerning Information and Electronic Transactions which was later changed to several arrangements in Law Number 19 of 2016 concerning Amendments to Law Number 11 of 2008 Regarding Information and Electronic Transactions (UU ITE) it only relies on the provisions in the Criminal Procedure Code (KUHAP). It was felt that the provisions for handling cybercrime cases needed special handling, so the ITE Law was formed which is expected to become a regulation in the handling of cybercrime and no more individuals or institutions feel disadvantaged because of cybercrime.

The presence of the ITE Law is still not able to make a major contribution to cybercrime law enforcement because the regulations in the ITE Law are still considered general and do not explain in detail how the proper handling of cybercrime cases should be, considered and considering that cybercrime is an extraordinary crimethen extraordinary measures are needed (extra or special handling). Electronic information and/or electronic documents in the ITE Law are recognized as an extension of valid evidence in accordance with the applicable procedural law in Indonesia and valid when using an electronic system in accordance with the provisions stipulated in the ITE Law. Referring to the provisions of evidence as regulated in the Criminal Procedure Code, there must be reliable and adequate testing equipment on electronic evidence, so that the evidence can be legally recognized in the litigation process as well as other evidence, namely formal and material requirements must be met.[2]

Cybercrime generally leaves a trace or history of criminal activity which can then be used as evidence. Evidence in cybercrime is divided into 2 (two) namely electronic evidence and digital evidence. Electronic evidence is evidence in the physical form of an electronic device or storage device. While digital evidence is evidence in the form of document files, file histories, or log files containing data related to cybercrime cases obtained from file extraction on electronic evidence.[5]

Electronic evidence and digital evidence in cybercrime cases are susceptible to contamination or change so electronic evidence should be stored and treated properly in a safe place as well. Such conditions require special handling which cannot be equated with physical evidence in conventional crimes. This special handling of digital

evidence is known as the chain of custody.[6] Until now, there are no comprehensive and sophisticated tools or software to be able to apply the chain of custody concept.

The current tools are not sufficient so they are not able to handle digital evidence investigations properly. In addition, the orientation towards the implementation of the chain of custody concept has not been carried out optimally, even though the purpose of the chain of custody concept itself is so that the digital evidence obtained has a strong and potential position and can be maintained in the litigation process. Therefore, to realize this, it is necessary to select the right tools at each stage of the digital chain of custody.

Digital forensics is a newly developing field but is increasing in line with the rapid use of information technology. Various sciences and tools have been developed to facilitate investigators in collecting data and assembling it to prove crimes that have occurred. As a new science, it still takes time to reach maturity. One of the problems digital forensics faces is the rapid development of digital science and technology.[6]

Mastering this rapidly evolving technology is challenging for digital investigators and law enforcement. Efforts to increase understanding and capacity must continue to be improved.[6]

The Indonesian National Police (POLRI) is an important institution in a leading position in dealing with cybercrime reporting. The police act as an investigator in a criminal case, where he is authorized to seek and collect evidence with which evidence can make a criminal act clear. In this case, the police have formed a new force by forming cyber police or cyber police where cyber police are devoted to conducting cybercrime investigations. However, in carrying out their duties, so far the police do not have guidelines for handling cases dealing with cybercrime. Cybercrime has various types and of course, requires different special handling related to digital forensic tools and methods that must be used.

About the chosen investigative method, legality, and the process of controlling electronic evidence, the legal aspects at each stage of the established procedure and the investigator involved can be the main keys to the success of the digital forensic method so that the digital evidence obtained can be relied on in the litigation process.

Another reason is that, in contrast to conventional evidence, digital evidence has several characteristics: easy to duplicate and transmit, very susceptible to modification and removal, easily contaminated by new data and time-sensitive. It is also possible for digital evidence to be cross-country and legal jurisdictions. For this reason, according to Schatz, handling the chain of custody for digital evidence is more complicated than taking physical evidence.[7] In addition, the difficulty of proving cyber crimes

(cybercrime) is caused by electronic evidence that is quickly deleted, easily replaced and accessed by many people. Indonesia occupies the highest position as a country whose internet users are victims of cybercrime among 26 other countries; the second is occupied by Vietnam and India, with 25% and 24% of internet users being the target of crime, respectively. The survey also found that 48% of consumers were targeted by fraudulent acts designed to defraud and obtain sensitive information and financial data for criminal acts.[8]

This research is important to do considering that cybercrime requires special handling in collecting digital evidence because digital evidence is easy to change and even easy to lose. The investigation process carried out by the police is still not optimal in handling cybercrime because the cyber police institution does not yet have guidelines for handling cybercrime cases related to its digital forensic methods.

2. METHODOLOGY/MATERIALS

The type of research used in this paper uses normative legal research based on the statute approach and conceptual approach. The technique of collecting legal materials used in this research is library research. If all the data has been collected, it will be processed using analytical methods using qualitative prescriptive which will be presented and describe and explain what this research finds.

3. RESULTS AND DISCUSSIONS

Digital forensics is essentially a science of computer technology that can be used for legal evidence, in this case, to prove high-tech crimes scientifically to obtain digital evidence that can be used to trap criminals; this is because in the search for digital evidence to ensnare perpetrators is often a highly complex job that makes a digital forensic analyst has to conduct a careful examination by following procedures recognized by national and international law.[9]

Based on the preceding, it can be seen that digital forensics is one of the fields of specialization in computer science and technology that has a significant position in investigating criminal cases with electronic evidence (computer crime) to find evidence for legal evidence purposes.[9]

Evidence in criminal cases, especially in cybercrime cases, certainly cannot be equated with conventional criminal cases. Because as we know that cybercrime cases are unlimited crimes that can be done anytime and anywhere with any method and tool

as long as there is a network called the internet that can help criminals to carry out their actions. Criminals can usually also be smarter to carry out their actions without being noticed by law enforcement, they are also good at protecting themselves and may even have thoughts of erasing or destroying evidence. To avoid this from happening, digital forensic experts are enforcing the law by securing evidence, reconstructing crimes, and ensuring that the collected evidence can be used in court later.

Digital forensic methods will certainly be needed in various interests. In general, digital forensic needs are classified as follows::

The need for investigation of violations of the law;

Reconstruction of computer security incident cases;

Efforts to restore system damage;

Troubleshooting involving hardware and software; and

The need to understand the system or various digital devices better.[10]

Definitions related to digital forensics according to several experts are as follows:

4. Budhisantoso

The combination of legal disciplines and computer knowledge in collecting and analyzing data from computer systems, networks, wireless communications, and fraudulent devices so that they are brought as evidence in law enforcement.

5. Marcella

Digital forensics is an activity related to the maintenance, identification, retrieval, screening, and documentation of digital evidence in computer crimes.

From the above definition, it can be concluded that digital forensics is a series of analytical and investigative methods used to identify, collect, examine and store evidence or information that is magnetically stored or encoded on a computer or digital storage media as evidence in uncovering cases of crimes or criminal acts committed. legally accountable.[11]

Forensic is identification work until an orderly hypothesis emerges and of course, to generate this hypothesis there must be internal research based on the available evidence. In this regard, it is known as the chain of custody. What is meant by the chain of custody is maintenance by minimizing the damage caused by the investigation. The purpose of this chain of custody is:

Guarantee that the evidence is authentic; At the time of trial, evidence can still be said to be like when it was found because usually, the distance between the investigation and trial is relatively long;

Storage and examination of existing evidence include protecting evidence from damage, alteration, and loss by irresponsible parties. Because digital evidence is temporary, easily damaged, easily lost and easily changed, the knowledge of a digital forensic expert is necessary. Minor errors that may arise in the handling of this digital evidence will be able to make the digital evidence not recognized in court.

Electronic evidence has begun to be recognized by the public, and new legal requirements are regulated in Law Number 11 of 2008 concerning Electronic Information and Transactions (called UU ITE). / or the printout is valid legal evidence. Then it is explained in Article 5 paragraph (2) of the ITE Law, which states that electronic evidence is an extension of legal evidence, following procedural law in force in Indonesia.[12]

Then the ITE Law also mentions the legal requirements for electronic evidence to be accepted as evidence, which is confirmed in Article 6 of the ITE Law, namely:[10].

Accessible. It can be displayed. Guaranteed integrity. It can be accounted for to explain a situation.

The obligation to fulfil the requirements for the validity of electronic evidence is absolute, as confirmed by Article 5 paragraph (3) of the ITE Law. So if one of them is not fulfilled, then the electronic evidence becomes invalid as evidence in court. As a reason for the requirement, electronic evidence has different characteristics from non-electronic evidence difference is:[13]

Electronic evidence is fragile (volatile) or easy to change, so there is a risk of damaging the integrity of the electronic evidence.

Contains electronic traces that record who, what, where, and when information from documents or information was created, deleted or modified

Vulnerable to the surrounding physical environment.

Based on these characteristics, law enforcers, when handling electronic evidence, must be careful and according to handling procedures so as not to change the integrity of the electronic evidence. Technical arrangements regarding procedures for handling electronic evidence by law enforcement officers in Indonesia currently refer to the National Police Chief Regulation No. 10 of 2009 concerning Procedures and Requirements for Requests for a Criminal Technical Examination at the Place of Case Incident and a Criminalistic Evidence Laboratory to a Forensic Laboratory (called PERKAP 10/2009).[12] However, in PERKAP 10/2009, there are several shortcomings; namely,

it is not comprehensive in regulating the handling of electronic evidence to maintain its integrity and can be said to be incomplete in retaining the integrity of electronic evidence.

Digital evidence found at the scene of the case will be confiscated which will then be further investigated by the evidence management officer. Handling of digital evidence must be done properly by taking into account 5 (five) aspects, namely: acceptable, authentic, complete, reliable, and believable.[14] Several things that can cause digital evidence to be unacceptable are when the extraction process is unprofessional, there is no match between the case and the evidence displayed, or not properly documented between the cases handled and the evidence obtained at the scene of the case.

Digital forensics uses four phases: arrest, storage, analysis, and presentation to trace digital evidence to court disclosure processes. In addition to broadening and expanding the research theme and scope of digital forensics, digital forensics is certainly needed further. With the development of technology, the research themes and scope of digital forensics will be further expanded, and the expertise of digital forensics will be further expanded. Of course, more will be needed.

Currently, the Indonesian National Police does not have any guidelines regarding the handling of cybercrime cases. Given that cybercrime has various types and of course, the digital evidence storage model is also different, maybe it can be stored on flash drives, software, hardware, or other devices. The handling of cases in managing digital evidence is of course different, depending on where the digital evidence is stored. The purpose of the establishment of this case handling guideline is so that the cyber police can determine their attitude to manage the digital evidence using the most appropriate method. Because of the method of handling digital evidence when using digital forensics, of course, you have to choose what kind of digital forensic model will be used for the digital evidence. Making guidelines for handling cases is useful to avoid the occurrence of a ”wrong choice of method” in handling digital evidence.

In addition to the selection of handling methods related to digital evidence with available tools based on the concept of digital chain of custody, another important thing that must be considered in the development of handling cybercrime cases, especially in Indonesia itself is maximizing the role of the authorized institution. in terms of analyzing concepts, digital forensic investigation projects, tools, and legal support in the field of cybercrime.

Asri Agung Putra, Head of the DKI Jakarta High Prosecutor’s Office, said that in the current digital era, the trend of criminal crimes tends to use electronic devices. Asri Agung Putra also proposed a strict standard operating procedure (SOP) that applies

to all law enforcement officers in handling electronic evidence so that the handling of electronic evidence can be responsive and accountable in the seminar "The Urgency of the Legal Framework for Electronic Evidence Regulation in Indonesia" held Partnership Institute, Wednesday (8 July 2020).[15]

In addition, synchronization between institutions is needed so that the SOP runs in one understanding. This is where the importance of regulation can be used as a standard reference so that there is an understanding from upstream and downstream; this is what is essential for us to realize in the context of electronic evidence management.[15]

The regulations made must cover things such as how to collect, manage, store, and available evidence at trial. That way, all law enforcement officers can acknowledge the existence and authenticity of the data. Reliable and qualified human resources must also support these things, both in quality and quantity, to carry out the function of digital evidence first responder (DEFR). In addition, it is necessary to form a data manager or data examiner, data analyst, report maker, and electronic evidence manager. Infrastructure support for handling electronic evidence, namely a digital forensic laboratory centre, is very much needed. [15]

With the inclusion of strict regulations on electronic evidence in the new civil procedural law, it is hoped that judges can examine cases (which use electronic evidence as evidence) to completion and then make a decision so that legal certainty can be obtained through judge decisions to provide a sense of justice for all parties. Public. Because justice can be achieved based on legal certainty that is applied to specific events or vice versa, legal certainty is performed based on justice.[16]

6. CONCLUSION ANDRECOMMENDATION

Digital forensics methods are used in dealing with digital evidence that is easily lost, easily damaged, easily changed, or even easily deleted at any time by criminals. To store digital evidence requires special handling and cannot be equated with evidence in conventional criminal acts that can be seen and dista then can be investigated at any time, because of its tangible form. Handling this digital evidence must use the right digital forensic method so that this digital evidence can be accounted for and "on display" and even acknowledged in court.

As of now, the Indonesian National Police has not issued or made a guideline for handling cases related to digital evidence and how to properly manage digital evidence and what use of digital forensic methods is appropriate to handle the digital evidence, because the digital evidence storage is in various possible places. there will also be

different procedures for handling the digital evidence. POLRI must make guidelines for handling cases related to digital evidence as well as institutional strengthening, in this case the understanding of competent and reliable POLRI human resources to become an investigator investigating digital evidence using digital forensic methods which will later be seleted as assistance in digital management evidence.

References

[1] Ilham Y. "Sejarah Internet di Dunia dan Perkembangannya di Indonesia," 2015. https://yusufilham.web.ugm.ac.id/2015/09/12/sejarah-internet-di-dunia-dan-perkembangannya-di-indonesia/ (accessed Jun. 28, 2022).

[2] Handoko, "Kedudukan Alat Bukti Digital dalam Pembuktian Cybercrime di Pengadilan,". Jurisprudence. 2016;6(1):1–15.

[3] "Jenis Cybercrime Berdasarkan Motif dan Aktivitasnya," Bapenda Jabar, 2017.

[4] Widodo, Sistem Pemidanaan Dalam Cyber Crime. Malang: Laksbang Mediatama; 2009.

[5] Riadi U, Umar R, Nasrulloh IM. ANALISIS FORENSIK DIGITAL PADA FROZEN SOLID STATE DRIVE DENGAN METODE NATIONAL INSTITUTE OF JUSTICE (NIJ). Elinvo. 2018;3(1):70–82.

[6] Rahardjo B. "Sekilas Mengenai Forensik Digital," J. Sosioteknologi, no. Agustus; 2013. pp. 384–7.

[7] J. T. Informatika, F. T. Industri, and U. I. Indonesia, "PROBLEMA DAN SOLUSI DIGITAL CHAIN OF CUSTODY Yudi Prayudi Abstract," no. 2011, 2014.

[8] N. Maharani, A. Zakaria, F. Hukum, and U. Brawijaya, "Urgensi pengaturan tata cara pembuktian tindak pidana siber (," no. 11, 2008.

[9] Wijanarko AA, Prakarsa A. PAMPAS: Journal Of Criminal Peran Digital Forensik dalam Pembuktian Tempus Delicti Sebagai Upaya Pertanggungjawaban Pidana Pelaku Pembuat Video Pornografi pengaruhnya bagi kehidupan manusia karena perkembangan teknologi sejalan dengan Gadget memiliki pen. PAMPAS J. Crim. 2021;2(2):68–88.

[10] Djati Nugroho P, Al-Azhar N. IT: Digital Forensic. Volume 5. IPSIKOM; 2017.

[11] Prayudi L, Pratama AM. "Pendekatan Model Ontologi Untuk Merepresentasikan Body of Knowledge Digital Chain of Custody," 2, 2014.

[12] Pengaturan R, Bukti P, Proses D, Pidana P, Indonesia DI. Rizki Zakariya 1, Yogi Prastia 2. Siti Ismaya. 2016;3:134–50.

[13] Gintin M. “Menata Regulasi Bukti Elektronik,” Tempo.com, 2019. https://kolom.tempo.co/read/1213817/menata-regulasi-bukti-elektronik

[14] Prayudi and Azhari. Digital Chain of Custody: state of the Art. Int J Comput Appl. 2015;114(5).

[15] Gobel T. “Perlunya Pusat Laboratorium Forensik Digital untuk Kelola Bukti Elektronik,” Cyberheart.id, 2020. https://cyberthreat.id/read/7482/Perlunya-Pusat-Laboratorium-Forensik-Digital-untuk-Kelola-Bukti-Elektronik

[16] Asimah D. To Overcome the Constraints of Proof in the Application of Electronic Evidence. J. Huk. Peratun. 2021;3(2):97–110.