Pakistan Journal of Criminology
Vol. 16, No. 04, October—December 2024 (255-268)

The Role of Digital Forensics in Criminal Investigations: An Analysis of Electronic Evidence in the Indonesian Legal System

Nasrullah[1], Judhariksawan[2],
Amir Ilyas[3] & Haeranah[4],

Abstract

Research on the use of digital forensic evidence in the process of investigating criminal acts, especially those carried out by the Police with their legal structure capabilities, aims to find out and analyze the extent to which evidence produced through digital forensics plays an important role in the process of proving criminal acts, the results of which become electronic evidence that has the strength of evidence in the applicable criminal procedural law. The type of research is normative (doctrinal), namely research that views law as building a system of norms. Digital forensics is an important instrument that helps investigators carry out research and investigation tasks, and it is an absolute requirement that must be met so that electronic documents can be used as evidence from the start of investigations, inquiries, prosecutions, and trials. The role of digital forensics in uncovering a criminal case starts from the preliminary stage, where investigators begin to collect evidence and electronic evidence assisted by one or more digital forensic experts. Digital forensics from the investigation stage is used to find material truth in every process of proving a criminal act.

Keywords: Digital forensics; investigation; criminal act

Introduction

Crimes in the field of information and communication technology have unique characteristics, namely: 1) they are global (cross national borders), making it difficult to determine which country's legal jurisdiction applies to them; 2) the nature of the crime, does not cause easily visible chaos (*non-violence*) so that fear of the crime does not easily arise; 3) criminals, the perpetrators are not easy to identify, but have special characteristics, namely that the perpetrators master the use of the internet/computer; 4) the crime mode, can only be understood by people who understand and master the field of information technology; 5) types of losses,

[1] Doctoral Student in Doctoral Program in Faculty of Law, Hasanuddin University, Indonesia. Nasrullahulla44@gmail.com
[2] Law lecturer, Department of Law, Hasanuddin University Makassar, Indonesia
[3] Law lecturer, Department of Law, Hasanuddin University Makassar, Indonesia
[4] Law lecturer, Department of Law, Hasanuddin University Makassar, Indonesia

the losses incurred are broader, including losses in the political, economic, social and cultural fields (Wahid & Labib, 2005).

Several types of cybercrime that are developing in this digital era include: 1) *unauthorized access*, namely a type of crime by infiltrating a computer system without permission and without the knowledge of the system owner. This way, perpetrators can steal the system owner's data to carry out piracy and system damage (*hacking* and cracking). 2) *illegal content*, namely a type of crime in the form of spreading something misleading or unethical that violates societal norms, such as spreading fake news (hoaxes) and pornographic content. 3) the spread of viruses, crimes to paralyzeaiming to paralyze the victim's device, theft and destruction of data by infiltrating viruses such as the well-known *trojans* and *ransomware* (Wahid & Labib, 2005).

Data from electronic Investigation Management (e-MP) Robinopsnal, Indonesian National Police Headquarters (from now on referred to as National Police Headquarters) states that from January 1 to December 22, 2022, the Police took action against 8,831 crime cases using information technology or cyber*crime*. All work units at Bareskrim Polri and Regional Police (from now on referred to as Polda) in Indonesia are taking action against this case. Polda Metro Jaya is the work unit with the highest number of prosecutions for cybercrime cases, namely 3,709 cases (Polri, 2023). Meanwhile, in the same period in 2021, the number of prosecutions was 612 throughout Indonesia. Only 26 work units took action.

By Law Number 2 of 2002 concerning the National Police of the Republic of Indonesia (from now on referred to as the Police Law) Article 15 paragraph (1) letter j, the National Police has the authority to organize a Criminal Information Center (Pusiknas). Pusiknas is under Bareskrim Polri and is based on the regulations of the Chief of the Republic of Indonesia National Police Regulation Number 15 of 2010 concerning the Implementation of a National Criminal Information Center within the National Police of the Republic of Indonesia (from now on referred to as Perkapolri No. 15 of 2010).

This cybercrime comes in various forms. Police enforcement data during that period mapped 10 (ten) types of cases with the highest number of prosecutions. The ten types are authentic data manipulation (3,723 cases), fraud via electronic media (2,131 cases), *cybercrime* (1,098 cases), defamation through electronic media whi,ch also takes the form of persecution (835 cases), accessing the system unlawfully (38 cases); online gambling (164 cases); threats via electronic media/social media and also in the form of persecution (145 cases); pornography or prostitution via electronic media (143 cases); insults through electronic media and which also took the form of persecution (59 cases); and *hate speech* (43 cases) (Polri, 2023).

Collecting evidence of the crime by carrying out analysis using police digital forensics. Digital forensics is a science that discusses findings in the form of digital evidence after events related to computer security occur. Digital forensics is the application of science to recover digital evidence from a device, be it a computer or *smartphone,* using certain methods to collect data that the court can accept as evidence (Setiawan, 2005). The evidentiary system used in the criminal process is generally an evidentiary system according to the law, which does not abandon the judge's belief based on two (2) pieces of evidence (Khaerul et al., 2022). One of the digital forensic media is *mobile forensics*. Mobile forensics aims to restore data from mobile devices.

The digital forensic and mobile forensic processes are commonly used by the Police in conducting inquiries or inquiries in cases of alleged criminal abuse of information technology. Collecting material and data becomes evidence, and after being sorted according to needs, it becomes evidence that will be presented at trial. Evidence in criminal law is very important and primary. In Article 6 paragraph (2) of Law Number 48 of 2009 concerning Judicial Power (from now on referred to as the Judicial Power Law), it is stated that no one can be sentenced to a crime unless the court, because of legal evidence according to law, is convinced that the person who is deemed to be responsible, guilty of the act for which he is charged. In criminal cases, case evidence aims to find material truth, namely the true or actual truth (Harahap, 2006). This differs from civil cases, where evidence aims to find formal truth, which means that the judge must not exceed the limits proposed by the parties to the case. Judges seeking formal truth need to prove it with "preponderance of evidence", whereas, for criminal judges seeking material fact, the event must be proven (Harahap, 2006).

Difficulties can be raised; for example, in determining locus delicti, investigators can easily investigate by collecting evidence and clues and also call a forensic laboratory party to find fingerprints. Investigators also need help finding witnesses who were in the crime scene. Another area for improvement area for improvement arises in collecting evidence, which requires a lot of costs because it requires high technology. With these impacts towards the development of information technology and communication, cybercrime's scope is wider because it is unlimited to geographical location; this may occur locally, nationally, and even internationally. Victims can be from all over the world, and this causes difficulties in the law enforcement process (Maskun et al., 2016).

With the presence of Law Number 11 of 2008, as amended by Law Number 19 of 2016 concerning Electronic Information and Transactions (from now on referred to as the ITE Law), in such situations, digital forensics plays an important role in making things easier for investigators . To track the perpetrator or his

network, including the modus operandi used. The evidence collected is called electronic evidence. Through electronic evidence, the planning (motive) of a crime can be identified through various media such as e-mail, telephone, online chat applications, messages in images, sound, video and other media (Fakhira, 2008) .

Electronic evidence has an important role in revealing a criminal event . Electronic evidence is starting to be recognized by the public and its legal requirements are regulated in the ITE Law . Article 5, paragraph (1) of the ITE Law determines that electronic information and/or electronic documents and/or printouts are 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, in accordance with the procedural law in force in Indonesia. Article 5, paragraph (1) of the ITE Law can be grouped into two parts. First, electronic information and electronic documents. Second are printouts of electronic information and electronic documents (Sitompul, 2012). The electronic information and documents will become Electronic Evidence (*Digital Evidence*). Meanwhile, the printed results of electronic information and documents will become documentary evidence. Article 5, paragraph (2) of the ITE Law, regulates that electronic information, documents, and printed results are an extension of valid legal evidence by the procedural law in force in Indonesia.

It should be noted that regarding Article 5 paragraphs (1) and (2) of the ITE Law, the Constitutional Court, through Decision Number 20/PUU-XIV/2016 ("MK Decision 20/2016") stated that the phrase "Electronic Information and Electronic Documents" is contradictory. The 1945 Constitution of the Republic of Indonesia does not have binding legal force as long as it is not interpreted, especially the phrase "Electronic Information and Electronic Documents" as evidence, carried out in the context of law enforcement at the request of the police, prosecutor's office and other designated law enforcement institutions. Based on the law specified in Article 31, paragraph (3) of the ITE Law.

Meanwhile, Article 31 paragraph (3) of the ITE Law itself stipulates that the provisions referred to in paragraph (1) and paragraph (2) do not apply to interception or wiretapping carried out in the context of law enforcement at the request of the police, prosecutor's office or other institutions whose authority is determined based on Constitution. Constitutional Court Decision 20/2016 above emphasizes that every interception must be carried out legally, especially in law enforcement.

However, handling electronic crimes using digital forensics is yet to be fully optimal, considering the limited number of investigators with expertise in information technology. Electronic crime has special characteristics, one of which is that this crime pattern uses information technology, which is difficult for people

who need help understanding the ins and outs of the cyber world. This certainly brings difficulties to the investigation process when this crime is handled by investigators who lack, or do not matter at all, information technology, especially digital forensics. Especially when the main perpetrator of the crime understands the ins and outs of information technology, it makes it easy to eliminate evidence that points to him just by using information technology devices and tampering with his network. This situation certainly becomes a major obstacle in collecting evidence of criminal acts at the investigation stage.

Internal regulations within the police force also do not support the effectiveness of handling electronic crimes. However, according to the data on handling electronic crimes above, the number of cases dealt with is quite large, with various patterns and a certain level of complexity. As a type of contemporary crime with special characteristics, it is necessary to strengthen law enforcement against electronic crimes through regulations within the police scope that cover the quantity and quality of investigative resources, infrastructure, budget, and other technical aspects deemed necessary to optimize police performance in handling this case.

Joint Decree of the Minister of Communication and Information of the Republic of Indonesia, the Attorney General of the Republic of Indonesia, and the Chief of Police of the Republic of Indonesia, Number 229 of 2021, Number 154 of 2021, and Number KB/2/VI/2021, concerning Implementation Guidelines for Certain Articles in the ITE Law, are not strong enough to support law enforcement in the field of electronic crime. This Joint Decree is very technical in regulating the implementation of offenses in the ITE Law and the Criminal Code, while what is needed is the ability and capacity of police investigators to handle electronic crimes. Another reason is that the SKB is not recognized in the legal hierarchy, so it is prone to be questioned by parties who feel disadvantaged if this is used as a reference in collecting evidence of electronic criminal acts.

Therefore, the author considers it important to research the use of digital forensic evidence in investigating criminal acts, especially those carried out by the Police with the capabilities of its legal structure. The extent to which evidence produced through digital forensics plays an important role in proving criminal acts, the results of which become electronic evidence that has evidentiary power in the applicable criminal procedural law.

Method

The type of research is normative (doctrinal), namely research that views law as building a system of norms. Peter Mahmud Marzuki defines the norm system, which is about the principles, standards, rules of legislation, court

decisions, agreements, and doctrines (teachings) (Marzuki, 2010). To support normative research, 3 (three) approaches are used: A philosophical approach used to study the nature of digital forensic analysis in electronic crime case investigation activities. The conceptual approach (*conceptual approach)* is used to test and analyze concepts related to digital forensics in electronic criminal case investigation activities. The *case* approach is used to study and analyze electronic crime cases investigated by the Makassar Police and South Sulawesi Regional Police using digital forensic analysis.

Results and Discussion

Along with modern science and technology development, the handling of criminal cases, especially in the inquiry and investigation process, has progressed and developed. Among them, it can be seen how the processes of resolving criminal cases are carried out by investigators applying other supporting knowledge with the appropriate competencies to facilitate the process of handling the case (Rachmie, 2020).

From the uniqueness contained in digital devices as evidence in a criminal case that uses information technology, investigators need other supporting knowledge to search for digital evidence stored on computers used by criminals, one of which is science. Digital forensics. It is necessary to apply digital forensic science to reveal facts or evidence related to the case so that a criminal act is clear and clear in the trial. In carrying out investigations through digital forensics, there are various applications as analytical aids circulating on the internet market, ranging from free applications to paid applications, including the well-known ones, namely *Encase*, FTK Data Access, *Belkasoft*, *Autopsy*, and so on to be able to search for evidence. In the law enforcement process (Rizki & Nursiti, 2018).

Digital Forensics is a scientific discipline derived from computer security that discusses discovering digital evidence after an event occurs. Digital forensics activities identify, maintain, analyze, and use digital evidence according to applicable law (Asrizal, 2022). Digital forensics states that computer science is applied to search for legal certainty for criminal acts and the like. Digital forensics science has basic principles. The basic principles of digital forensics according to ACPO include: (Yudha, 2015)

1. Legal institutions and their officers are prohibited from changing digital data stored in storage media, which is then brought to court.
2. A person who needs to access digital data stored in evidence storage media must be clear about the competence, relevance, and implications of the actions taken with the evidence.

3. Technical and practical notes regarding the steps taken on storage media during the inspection and analysis process if a third party investigates the storage media and gets the same results.

Digital forensics is a science that discusses findings in the form of digital evidence after events related to computer security occur. Digital forensics is the application of science to recover digital evidence from a device, be it a computer or *smartphone*, using certain methods to collect data that the court can accept as evidence (Setiawan, 2005). One of the digital forensic media is *mobile forensics*. Mobile forensics aims to restore data from *mobile devices*.

In cybercrime, contact can occur when two computers contact each other in a network, as stated in the " *Cyber Exchange* " theory (Horiyah, 2023). The meaning of the *Cyber Exchange theory* is that contact with electronic devices does not cause physical traces because humans do not come directly and do not make physical contact with the crime scene. However, the contact that occurs is "virtual" contact. So, the traces left on the contact are called digital evidence. To search for digital evidence stored on computers used by criminals, digital forensic methods are needed, namely scientific methods for collecting and analyzing data and traces from computer systems, networks, and storage devices.

Handling digital forensics generally refers to *the National Institute of Justice* (NIJ), which is a research and evaluation institution of the United States Department of Justice that provides standard digital forensic models in the book "Forensic Computing Models: Technical Overview", with the following stages: (Shrivastava et al ., 2012)

1. Identification Stages and Procedures

The identification stage refers to the identification standard in handling ISO 27037 of 2012, which includes 4 stage elements, namely:

a. The process of identifying media or what is usually called Electronically Stored Information (ESI), which is considered to be a data source;

b. Collection activities;

c. Data acquisition activities; And

d. The process of preserving (security) electronic devices/evidence

The identification stage is the initial handling of electronic evidence at the crime scene (TKP), which is volatile (easily changed, lost, and damaged). In the identification process, it is necessary to identify several data storage media (such as hard disks, flash drives, CDs, memory cards, etc.), electronic devices (computers, gadgets, cameras, etc.), and network activity logs from internet providers that are relevant to the action. Criminal. Therefore, digital forensic personnel who are competent in mapping electronic evidence and its owner are

needed to coordinate with investigators to confiscate electronic evidence related to criminal acts.

2. Examination Stages and Procedures

Once electronic devices containing relevant electronic evidence have been identified, personnel must decide whether to collect or acquire them later. Several factors determine this choice, including the surrounding conditions and the condition of electronic devices (Zakariya, 2019). Collection is the process of handling electronic evidence in which devices containing electronic evidence are moved from their original location to a forensic laboratory or other controlled environment for subsequent acquisition and analysis. Meanwhile, acquisition is transferring electronic evidence from the original electronic device to the storage of personnel/investigators for further analysis (Zakariya, 2019). In the process of collecting electronic devices, things that personnel need to pay attention to include: (Zakariya, 2019)

a. Verify data integrity to prove that the data collected has not been altered or tampered with.

b. Equipment in the electronic device collection process, such as using gloves to avoid tampering with latent evidence (fingerprints, DNA, etc.).

c. Packaging electronic devices in tamper-evident bags and labels, numbered according to the evidence label, FR name, collection date, and evidence specifications. Avoid extreme temperatures, large magnets, water, moisture, and other conditions affecting electronic evidence.

d. Record the details of the electronic devices collected, then document them in the chain of custody and explain the reasons for the collection.

When this stage is complete, the electronic device is then taken by the personnel/investigator to the laboratory for acquisition and analysis. This acquisition requires special competencies other than authority, such as using physical or logical acquisition methods. After being acquired, the electronic evidence does not change (message digest or hashing) between the original evidence at the crime scene and the copied evidence. (Zakariya, 2019).

3. Analysis Stages and Procedures

After obtaining electronic data related to criminal acts, the data is then analyzed. However, before that, the data is indexed first. Indexing is the process of categorizing each word in electronic data so that it becomes searchable. The analysis stages must be carried out by competent personnel who understand the chronology of the case events. Therefore coordination is needed with investigators who understand the case's beginnings. This analysis identifies the parties involved,

location, sequence of events, mode, and so on. These results are from now on referred to as electronic evidence, which must be technically and scientifically accountable to the court (Zakariya, 2019).

4. Reporting Stages and Procedures

After certain facts related to criminal acts are known through digital forensic analysis, the analysis results are then reported in a forensic report. Next, the report is submitted to investigators to prove a criminal act. The reporting is also accompanied by *a chain of custody*, which contains records of each stage of electronic evidence handling carried out by personnel (Zakariya, 2019).

The involvement of digital forensics in supporting crime evidence in the digital realm plays a very significant role. This involves analyzing electronic evidence related to computer and computer-related *crime* . The four key elements in computer forensics that are legally acceptable are as follows: (Noffezar et al., 2019)

1. The identification of digital evidence is the earliest discovery of computer forensics. Find out what digital evidence exists, where, and how it is stored so you can know how to handle and recover it.
2. Storing digital evidence is a critical process in disclosing digital evidence related to computer forensics. Digital evidence is very fragile evidence. Every detail that is carried out must be accountable and explained because there are circumstances where changes cannot be avoided in digital evidence; this applies to changes to the data itself and physical changes that may be made to electronic devices to access the data itself.
3. Digital Evidence Analysis: is the extraction, processing and interpretation of digital data, generally considered the main element of forensic computing. After the extraction process, digital evidence requires processing before it can be read.
4. Presentation of Digital Evidence: is the final process in digital forensics, namely presenting the results of digital evidence analysis before the trial. The presentation of digital evidence is related to the legal standards for presenting evidence before a trial, including the standard qualifications of the skilled profession presenting the evidence, the process of proving digital evidence that is appropriate and not defective in the eyes of the law due to digital evidence that is invalid or contaminated during the process. the analysis is carried out.

Digital forensics is an important instrument that assists investigators in carrying out investigation and investigation tasks as regulated in Law Number 19 of 2016 concerning amendments to Law Number 11 of 2008 concerning

Information and Electronic Transactions, which is in synergy with the Criminal Procedure Code. (Criminal Code). Explicitly in Article 6, Article 15, and Article 16 of the ITE Law, electronic information and documents must be able to guarantee their authenticity, integrity, and availability. To ensure the fulfillment of this, digital forensics is needed (Sitompul, 2012).

Implementing digital forensic science in the investigation process requires an in-depth understanding of technology, apart from the legal aspects, which are a routine part of the criminal court process (Awaluddin et al., 2024). The application of digital forensic science is divided into 4 (four), namely: (Raharjo, 2013)

1. Computer forensics, namely investigations carried out regarding the data and applications on the computer, which are recorded in various log files;
2. Network/Internet forensics, namely investigations carried out on data obtained based on observations on the network;
3. Application Forensics is an investigation carried out using certain applications. This application has an audit function because the application has a feature to leave traces of a device;
4. Device Forensics is an investigation to obtain and collect data and traces of certain activities on a digital device.

Digital forensics is an absolute requirement that must be carried out so that electronic documents can be used as evidence from investigations, inquiries, prosecutions, and trials. Without digital forensics, an electronic document cannot be used as evidence because the validity of the electronic document cannot be guaranteed. Electronic evidence can be grouped into two parts. First, electronic information and electronic documents. Second, printouts of electronic information and printouts of electronic documents. Electronic information and electronic documents will become electronic evidence (*digital evidence*).

Meanwhile, the printed results of electronic information and documents will become documentary evidence. Printouts of electronic information and electronic documents will become documentary evidence. Documentary evidence (faxes, e-mails) that are found can be used as a basis for prosecuting the defendant if it can be ascertained that a computer system is working properly. Its objectivity can be proven (Makarim, 2003).

Requirements for fulfilling electronic information and documents as valid evidence. In the process of retrieving digital *evidence* or *electronic evidence* (electronic evidence) in the form of information and electronic documents, namely numbers and information codes called *product keys* from computer programs that have been installed on the computer, physically the files containing *the product key* have been stored on a CD which can be displayed at any time and witnesses

have signed the printed results, then the CD and printed documents can also be used as documentary evidence which strengthens other evidence, namely in the form of Minutes of Computer Examination Results through digital forensics or *computer forensics* (Noffezar et al. al., 2019) .

The role of digital forensics in uncovering a criminal case starts from the preliminary stage, where investigators begin to collect evidence and electronic evidence assisted by one or more digital forensic experts. In practice, these digital forensic experts often also assist prosecutors in prosecution efforts and in court hearings to assist judges in analyzing concrete cases (Tatumpe, 2019) .

Ideally, every time a cybercrime case is proven, digital forensics experts need to be involved, either at the case investigation stage or at the trial level. In the event that investigators do not include digital forensic experts in investigating cases that occur in cyberspace, then the prosecutor's office cannot accept the case. (Medeline et al., 2023) . In terms of carrying out investigations, investigators need the application of digital forensic science; if viewed from the crimes committed, one of the ways that digital forensic science is carried out is through network forensics, which is the process of capturing, recording, and analyzing network activity in a digital device to obtain digital evidence. *Evidence*) of crimes committed against or using the computer network (Rachmie, 2020).

The presence of a digital forensics expert to assist the judge in adjudicating a case being tried plays a very important role. Becauseinvestigators, prosecutors, and judges are law enforcers withwith limited knowledge. On average, judges in Indonesia do not/do not understand computer technology and its applications; this is the main problem faced by judges in examining criminal cases using computer media, both about determining the case (by judex factie) and in terms of implementation. law (Tatumpe, 2019) .

Every case of cyber crime or general crime where digital or electronic evidence is found during the investigation must start from collecting evidence and using digital forensics to the next stage. The use of digital forensics from the investigation stage is to try to find material truth in every process of proving a criminal act, so that it can realize the principle of *due process of law* (Medeline et al., 2023) .

Digital forensic examination of evidence will guide investigators from the initial examination stage to finding the suspect who committed the crime . Digital forensics will play a role in finding perpetrators and reconstructing behavior. Digital forensics in the forensic process will be more responsible because it is a form of applying scientific techniques and analyzing existing evidence (Medeline et al., 2023) .

Conclusion

Digital forensics is an important instrument that helps investigators in carrying out research and investigation tasks, as well as an absolute requirement that must be met so that electronic documents can be used as evidence from the start of investigations, inquiries, prosecutions, and trials. The role of digital forensics in uncovering a criminal case starts from the preliminary stage, where investigators begin to collect evidence and electronic evidence assisted by one or more digital forensic experts. If investigators do not involve digital forensic experts in investigating cases that occur in cyberspace, then the prosecutor's office cannot accept the case.

The involvement of digital forensics in supporting crime evidence in the digital realm plays a very significant role. This involves analysis of electronic evidence related to computer crimes *and* computer-related *crimes.* Every case of cyber crime or general crime where digital evidence or electronic evidence is found during the investigation must start from the stage of collecting evidence and using digital forensics to the next stage. The use of digital forensics from the investigation stage is to try to find material truth in every process of proving a criminal act. Digital forensic examination of evidence will guide investigators from the initial examination stage to finding the suspect who committed the crime. Therefore, it is hoped that agencies, especially the Indonesian National Police, can further develop human resources within these agencies so that more investigators can use digital forensic technology to collect and review evidence during the investigation stage.

References

Asrizal. (2022). *Digital Forensics What and How* . Ministry of Religion. https://e-document.kemenag.go.id/cgi-sys/suspendedpage.cgi

Awaluddin, F., Amsori, & Mulyana, M. (2024). Challenges and Role of Digital Forensics in Law Enforcement against Crime in the Digital Realm. *Humaniorum , 2* (1), 14–19. https://doi.org/10.37010/hmr.v2i1.35

Fakhira, E.L. (2008). *The Position of Electronic Evidence as Evidence in Court* . Bandung: Art Press.

Harahap, Y. (2006). *Discussion of Problems and Application of the Criminal Procedure Code for Investigation and Prosecution* . Jakarta: Sinar Graphics.

Horiyah. (2023). Locard's Exchange Principles and Their Relation to Digital Forensics. *Journal of Informatics Engineering Online E-Journal* . www.academia.edu

Khaerul, M., Ilyas, A., & Muin, AM (2022). Document Forgery System in Indonesia's Election Crime. *Living Law Journal , 14* (1), 59–74.

Makarim, E. (2003). *Telematics Law Compilation* . Jakarta: Rajagrafindo Persada.

Marzuki, PM (2010). *Legal Research* . Jakarta: Kencana.

Maskun, Khairunnisa, & Fitriani., M. (2016). The Nature of Article 27 the Law on Information and Electronic Transactions in Indonesia Practice. *JL Pol'y & Globalization , 47* .

Medeline, F., Rusmiati, E., & Ramadhani, RH (2023). Digital Forensics in Proving Crimes of Hate Speech on Social Media. *PAMPAS: Journal of Criminal Law , 3* (3), 310–325. https://doi.org/10.22437/pampas.v3i3.19691

Noffezar, Fitriati, & Faniyah, I. (2019). Use of Digital Evidence in Computer Forensics in Mayantara Crime Investigations at the Special Crime Directorate of the West Sumatra Police. *UNES Journal of Swara Justice (UJSJ)* , *2* (4), 411–419.

Polri, P. (2023). *Cybercrime in Indonesia Increases Many Times* . Pusiknas Bareskrim Polri. https://pusiknas.polri.go.id/detail_article/kejahatan_siber_di_indonesia_naik_berkali-kali_lipat

Rachmie, S. (2020). The Role of Digital Forensic Science in Investigating Website Hacking Cases. *Litigation , 21* (21), 104–127. https://doi.org/10.23969/litigation.v21i1.2388

Raharjo, B. (2013). A Glimpse into Digital Forensics. *Journal of Sociotechnology , 12* (29).

Rizki, S., & Nursiti, N. (2018). Digital Forensic Analysis in Revealing Cyber Crimes at the Evidence Stage. *Student Scientific Journal in the Field of*

Criminal Law , 2 (November), 780–787. http://jim.unsyiah.ac.id/pidana/article/view/14618

Setiawan, D. (2005). *Computer Security Systems* . Jakarta: PT Elex Media Komputindo.

Shrivastava, G., Sharma, K., & Dwivedi, A. (2012). Forensic Computing Models:Technical Overview. *CCSEA, SEA, CLOUD, DKMP, CS & IT* , *5* , 207–216.

Sitompul, J. (2012). *Cyberspace, Cybercrimes, Cyberlaw: An Overview of Aspects of Criminal Law* . Jakarta: Tatanusa.

Tatumpe, A. (2019). Juridical Analysis of Digital Forensics in Proving Crimes in Indonesia. *Journal Scientia De Lex , 7* , 1–9. https://www.ejournal.unpi.ac.id/index.php/scientia/article/view/42%0Ahttps://www.ejournal.unpi.ac.id/index.php/scientia/article/download/ 42/35

Wahid, A., & Labib, M. (2005). *Mayantara Crime (Cyber Crime)* . Bandung: Refika Aditama.

Yudha, F. (2015). USB Analysis Tool for Digital Forensics Investigation. *Technoin , 21* (4). https://doi.org/10.20885/teknoin.vol21.iss4.art6

Zakariya, R. (2019). *Utilization of Digital Forensics in Handling Election Crime Cases* . Jakarta: General Election Commission.