Digital Forensics in Online Fraud Crimes Investigation

Muhammad Alhadi Haq[1], Megawati Barthos[2], Zudan Arief Fakrulloh[3]
alhadisip50@gmail.com[1], megawati_barthos@borobudur.ac.id[2], cclsis@yahoo.com[3]

Universitas Borobudur[1,2,3]

Abstract. The rise of online fraud cases occurs in community. This study aims to find out the application of digital forensics in the investigation of online fraud crimes carried out by the Satreskrim Police Unit. To answer the questions posed, qualitative analysis methods were used to examine the quality of the collected data in order to construct a concise and pertinent picture of criminal policy regarding the police's role in combating online fraud. This included data from interviews and all other sources. The National Police have not done an adequate job of optimizing their use of social media to handle fraud cases. This condition is brought about by deficient HR capacities, both regarding information, abilities, financial plan, offices, and targets. There is currently only one person who has attended information technology vocational education, which has implications for investigator skills in cybercrime disclosure techniques and tactics that are still lacking. The budget that Satreskrim owns is the obstacle that prevents it from handling fraud cases through social media.

Keywords: Digital Forensics, Online Fraud, Crime

1. Introduction

The spread of information and communication technology has resulted in a world without borders, prompting significant social shifts. However, the creation of Information and Communication Technology produces positive benefits, but it turns out to be used for negative things. The rise of modern crimes is one of the negative effects of technological advancements. The quantity and complexity of crime, as well as variations in its methods, continue to rise alongside human civilization.[1] Defamation, pornography, gambling, account breaches, the destruction of cyber networks (hacking), and other crimes committed through electronic media are just a few examples of the many types of criminal acts that frequently occur.

Crimes caused by the development and progress of Information Technology and Telecommunications are crimes related to the internet, or in foreign terms, it is often called cybercrime.[2] Cybercrime is a type of crime that uses new technologies, especially the internet. The internet, which presents cyberspace as virtual reality, provides a number of hopes and conveniences; however, behind those hopes and conveniences are problems in the form of a crime known as cybercrime, which involves both the computer network system and the computer itself, which serves as the vehicle for committing crimes.

According to Selvik, there are various variations of digital fraud, such as phishing, lottery scams, video scams, identity theft, and scareware.[3] Meanwhile, Button mentioned other types of digital fraud, such as romance scams, malicious spam, employment scams, and investment scams. Various types of fraud are conveyed to victims or potential victims through various

ICLSSEE 2023, May 06, Salatiga, Indonesia

DOI 10.4108/eai.6-5-2023.2333408

channels such as short messages (SMS), messages through chat applications, and other social platforms including social media, email, telephone, websites, marketplaces, and various other digital platforms. [4][5]

One of the protection efforts is through Criminal Law, both by penal and non-penal means in Electronic Media.[6] The crime that often occurs is fraud in the name of buying and selling business using Electronic Media which offers various kinds of products that are sold below the average price. Online business has become a trend nowadays. However, it can harm other people if it is used by irresponsible parties. There are so many frauds in the real world, but in cyberspace, there are also cases of fraud.[7]

Several data and studies above show that digital fraud is a crime that seriously threatens the Indonesian people in this digital era, which not only causes financial and psychological losses but also breaches of personal data.[8] Various factors can be assumed to influence the number and variety of current digital fraud cases. First, the competence of media users in recognizing, preventing, and fighting digital fraud. Second, law enforcement and prevention regulations are not strong enough. Third, content moderation and community standards from various digital platforms have not been fully utilized to prevent and deal with digital fraud.

As law enforcement officers, the police have a responsibility to uphold the law and protect the community from the widespread fraud that is committed. This is demonstrated in Article 13 of Law No. regarding the Indonesian National Police, which states that the Indonesian National Police's primary responsibilities are as follows: 1. to preserve public safety and order; 2. Respect the law; and 3. Serve the community while offering shelter, protection, and assistance. [9]

Not only looking at the types and disadvantages of digital fraud but there is also a study on digital fraud from a legal perspective. For Indonesia, one of them was completed by Rahmanto in regards to policing criminal demonstrations of extortion in light of electronic exchanges which are as yet encountering numerous obstructions. Some of these obstacles are differences of opinion in interpreting regulations, the ability of investigators, public awareness and concern, limited expert personnel, weak government oversight, and procedural constraints on the Electronic Information and Transaction Law.

It turns out that it's hard for the police to find crimes involving information technology. In Indonesia, the Criminal Code's provisions (KUHP) and the provisions of the Criminal Code outside of the Criminal Code serve as a legal foundation for dealing with cybercrime.[5] The crook arrangements for the people who commit extortion through electronic media are totally managed in Article 28 passage (1) of Regulation Number 11 of 2008, which manages Data and Electronic Exchanges. Each individual deliberately and without defense spreads bogus and misdirecting data, which makes clients lose cash through electronic exchanges. [6]

The difficulty in uncovering cases of online fraud is due to several factors, including perpetrators taking advantage of the knowledge of victims who are usually unfamiliar with certain mechanisms; evidence and evidence of online fraud crimes are easy to manipulate, delete or eliminate so that the traces of the crime are not detected; the evidence is often confiscated not from the perpetrator, but from other people so that its authenticity is questioned; Victims can be anyone, either detectable or not or in other words transnational in nature.[10]

Based on the facts above, an important element in solving security problems from online fraud is the use of science and technology itself. In this case, science and technology can be used by law enforcement officials to identify suspected criminals. This is where the importance of instruments to explore the process of proving crimes is commonly known as digital forensics. Proof in cyberspace has its own characteristics, which are different from proving conventional crimes.

Online fraud knows no geographical boundaries, this activity can be carried out at a close

range, or from thousands of kilometers away with similar results. Criminals are usually one step ahead of law enforcement officials, in protecting themselves and destroying evidence. Subsequently, computerized criminology is fundamental for implementing the law by defending proof, remaking violations, and guaranteeing that the proof accumulated will be helpful in court. So online misrepresentation can be uncovered and safeguard the interests of casualties. Because so far there have been many cases of online fraud that have not been resolved properly.

2. Method

Based on the definition of Soerjono Soekanto, this study employs the normative juridical approach. [11] The creator of this legitimate review tries to analyze the regulations and guidelines relating to the current subject, explicitly cybercrime, as illustrated in the Republic of Indonesia's 1945 Constitution; Regulation No. 19 of 2016 on Electronic and Educational Exchanges.

Optional information sources are utilized in regularizing juridical exploration. Information got from lawful materials, including essential, auxiliary, and tertiary legitimate materials, comprise optional information in regularizing juridical examination. [12]

Legitimate materials as auxiliary information used to break down lawful issues in this proposition are as per the following:

a. Primary Lawful Materials, explicitly authoritative records overseeing on the web exchanges and virtual entertainment use. [13] This concentrate essentially depended on authoritative records like:
    1) The 1945 Constitution of the Republic of Indonesia
    2) Law Number 19 of 2016 concerning Data and Electronic Exchanges
b. Secondary Legitimate Materials, explicitly those that make sense of essential legitimate materials like draft regulations, research discoveries, or well-qualified sentiments. [9]
c. Tertiary Legitimate Materials are legitimate materials like word references (in English, Indonesian, and regulation) and reference books that give guidelines and clarifications to essential and auxiliary lawful materials. [14]

3. Result and Discussion

3.1. Digital Forensics in Criminal Cases

The role of digital forensics in helping to prove a crime digitally is very important, but digital forensics can not only be used to uncover digital crime evidence but conventional crimes that have electronic/digital evidence. Of course, digital forensics is important for analyzing electronic evidence of computer crimes and/or computer-related crimes. Traditional crimes like theft, robbery, murder, corruption, drug trafficking, and others all fall under the category of computer-related crimes. Defacement (illegally changing a website's pages), denial of service (making a system not work or function as it should), keylogging (recording each composing action on the console and applications that show up on the screen), fraud (robbery of significant information from the objective), intrusion (illegal entry into a system), and other forms of computer crime are examples of computer crime.[15]

In criminal cases, digital forensics aids in digital case proof. Following Article 5 segment (1) of the Law of the Republic of Indonesia Number 11 of 2008 Guideline No. 19 of 2016 on

Data and Electronic Exchanges expresses that electronic records, reports, and prints are lawful confirmation. Digital forensic expert, Christopher revealed that in the digital and electronic world, the original evidence is not analyzed, that's why the evidence must be preserved, this is different from dissecting the victim's body. [14]

Offenders in computer crimes can, of course, destroy evidence and try to avoid criminal liability. Criminals are usually one step ahead of law enforcement, in protecting themselves and destroying evidence. In the world of digital forensics, this is called anti-forensics. Hence, the errand of advanced scientific specialists is to uphold the law by getting proof, reconsidering wrongdoings, and guaranteeing that the proof will be helpful in court.

3.2 Consumer Protection Act

First and foremost, society is viewed as a system of institutionalized trust, so it is essential to safeguard crime victims. This belief is incorporated by the standards that are exhibited in institutional structures like the police, prosecutors, and courts, among other things. The event of a wrongdoing against the casualty can mean the obliteration of the conviction framework so the guideline of criminal regulation and different regulations connecting with the casualty will work for the purpose of reestablishing this conviction framework.

Second, there are a common agreement and fortitude contentions on the grounds that the state can be said to have a syndication on all friendly responses against violations that restrict private activities. Consequently, the state must prioritize all victims of crime by enhancing services and regulating rights. Thirdly, victim protection is frequently linked to conflict resolution, one of the goals of punishment. Society's equilibrium and sense of peace will be restored by resolving conflicts brought on by criminal acts.

Regarding the implementation of the protection of the rights of crime victims, including internet fraud victims, as a result of human rights violations, several theories provide the foundation for protecting crime victims, including the following [16]:

i. The hypothesis of utility spotlights on giving the best advantage to the best number of individuals. However long it gives more prominent advantages than not making a difference the idea, safeguarding survivors of wrongdoing, including extortion casualties, online can be carried out. This applies not exclusively to survivors of wrongdoing yet additionally to criminal policing an entirety.
ii. Responsibility Hypothesis, Legitimate subjects are basically liable for all lawful activities they carry out so that assuming somebody perpetrates a wrongdoing and makes somebody endure, a misfortune (from a wide perspective), that individual should be liable for the misfortunes caused except if there is an explanation that liberates him. With respect to culprits of criminal demonstrations of extortion through the web, in view of the hypothesis of obligation, the culprits should be considered responsible for the legitimate activities they have carried out, except if there is motivation to clear the culprits.
iii. Compensation Hypothesis, as an epitome of obligation, in view of their errors towards others, the culprits of criminal demonstrations are troubled with the commitment to give misfortunes to individuals or their main beneficiaries. With respect to by means of the web, in light of the hypothesis of pay, the culprit should make up for misfortunes assuming the casualty claims pay. This remuneration can be made by joining common cases and criminal cases under the arrangements of articles 98 to 101 of the Criminal System Code.

Casualties of the event of a wrongdoing in electronic exchanges, one of which is the

casualty of extortion through the web, are the party that experiences the most and is burdened, thusly having security from the state is vital. Casualties' freedoms should be viewed as a type of equivalent treatment for everybody under the steady gaze of the law (uniformity under the steady gaze of the law).

There is a sale and purchase agreement for buying and selling goods online, which issuing an agreement, namely an agreement that originates from an agreement or commonly referred to as a named agreement. Buying and selling goods online should adhere to existing regulations. Instagram, Facebook, and online buying and selling shops like Zalora and Shopee are currently widely used for sale and purchase transactions. Every business deal comes with risks and problems. One example was when a customer felt let down because he didn't get the goods he bought, so he complained that an online store with a Facebook account tricked him. Another thing that happens when people buy and sell things online is when they buy something and the condition isn't right.

The imposed article in Law No. 19 of 2016 on Amendments to Law No. 11 of 2008 on Information and Electronic Transactions is Article 28 paragraph (1), which reads as follows: 1) Everybody utilizes deliberately and without freedoms share bogus and misdirecting data that causes shopper misfortunes in Electronic Exchanges. According to Article 45 paragraph [2] of the ITE Law, the penalty for violating this article is either a fine of up to IDR 1 billion or imprisonment for a maximum of six (six) years. As per Article 5 section 2 of Regulation Number 19 of 2016 Concerning Changes to Regulation Number 11 of 2008 Concerning Data and Electronic Exchanges, you can utilize electronic proof or potentially printed results as an augmentation of proof for verification notwithstanding other traditional proof as per the Book Criminal Strategy Code (KUHAP).

The privileges of casualties in the Criminal System Code that are pertinent to the freedoms of survivors of criminal demonstrations of misrepresentation through the web are as per the following:

a) Right to Report (Article 108 Section (1) of the Criminal System Code)
b) Right to practice command over examiners and public investigators (article 77 jo 80 KUHAP)
c) The Right to Guarantee Remuneration Because of a Lawbreaker Act by Consolidating Common Cases with Criminal Cases (Article 98 to Article 101 of the Criminal Method Code)

The principle of online transactions dictates that sellers and buyers typically place a higher priority on the issue of "trust." The standard of online exchange security has not yet turned into a main pressing issue, particularly when exchanges are completed on a little or medium scale with an ostensible exchange that is little or not excessively huge. One of the reasons for the many fraudulent transactions is through online/internet media or other telecommunication media. With so many frauds that have occurred, it would be better if you are more selective in making online transactions and be more careful to reduce fraud, as a consideration if you are going to make buying and selling transactions online.

Not only large amounts of fraud but small amounts of fraud also often occur, but consumers more often just leave it alone and don't report it because a small nominal does not make them experience big losses. Although there is no explicit regulation of online fraud in Law No. 11 of 2008 pertaining to Information and Electronic Transactions, the dissemination of false and misleading information that causes consumers to lose money through electronic transactions is covered by the ITE Law.

According to the provisions of the ITE Law, the focus is on the existence of misleading fake news which results in losses for consumers. It doesn't matter how much loss it causes. In

addition, provisions regarding fraud can also be found in Article 378 and Article 379 of the Criminal Code (KUHP). With the sound of the article is as follows:

Article 378 of the Criminal Code:

"Whoever with the intent to unlawfully benefit himself or others by using a false name or false prestige (*hoedaningheid*); by deception, or a series of lies, to induce another person to hand over something to him, or to give a debt or write off a debt, is threatened, for fraud, with a maximum imprisonment of four years."

Article 379 of the Criminal Code:

"The acts formulated in Article 378, if the goods handed over are not livestock and the price of the goods, the debt or credit is not more than twenty-five rupiahs, it is threatened as light fraud with a maximum imprisonment of three months or a maximum fine of two hundred and fifty rupiah"

If you look at the provisions in Article 379 of the Criminal Code, it is explained how much loss can be reported and distinguished whether the crime is fraud or minor fraud. Looking at the provisions of Article 379 of the Criminal Code, it is explained that what is meant by mild fraud is not the minimum price of goods Rp. 2,500,000.00, - but the price of the goods in question is not more than Rp. 2,500,000.00, -. So even though the amount of loss suffered is small, it is included in light fraud and the realm of crime.

In view of article 28 F of the 1945 Constitution of the Republic of Indonesia, forming the ITE Law means limiting the use of information technology. However, what needs to be emphasized is that the ITE Law was formed to regulate all electronic use freely but responsibly.

It should be completed as per Article 3 of the ITE Regulation since it is associated with the utilization of the web, which is the use of data innovation and electronic exchanges. As per Article 15 of the ITE Regulation, the entertainers or coordinators of the electronic framework have liabilities by and by, in particular:

1) The Electronic System must be operated safely and reliably by every Operator of the Electronic System, and they are accountable for its proper operation.
2) The operations of their electronic systems are the responsibility of electronic system operators.
3) If it is established that the Electronic System user acted with force majeure, error, or negligence, the provisions referred to in paragraph (2) do not apply.

It can be noted that the ITE Law itself has been able to protect consumers and ensnare perpetrators of light and heavy fraud because there are already binding articles and sanctions given for criminal acts. However, back to consumers who are sometimes hesitant or don't dare to report to the authorities because the cost of settling cases is not worth the price of the losses suffered and also takes a lot of time. In addition, consumers do not understand applicable laws and do not understand or do not know what they should do if they do not get their rights from business actors who commit fraud.

3.3 Efforts made by the Police in Revealing Criminal Acts of Online Fraud

In order to optimize the handling of fraud online (cyber fraud/internet fraud) which is growing day by day along with advances in technology, the National Police has taken several actions in the following areas: limited human resources are a problem that cannot be ignored, for this reason, it is necessary to increase human resource capabilities cyber investigative power as seen from:

First-hand understanding All members of Sub Directorate V Special Police Specialist should be given every opportunity to participate in information technology-related vocational

education. This is intended to provide the personnel of Sub Directorate V with qualified cybercrime disclosure knowledge so that they can further support the execution of their duties, particularly those pertaining to the disclosure of reported cybercrimes. At the very least, the individual will have a better understanding of the bureaucracy, procedures, techniques, tactics, provisions, and laws and regulations pertaining to the use of information technology in relation to their relationship with telecommunications service providers (providers) if Subdirector V personnel participate in vocational education in the field of information technology.

Both skills Along with the increasing knowledge of the personnel of *Subdit V Krimus*, it is hoped that the skills of investigators in disclosing information technology crime cases can also increase. Sub-Directorate V personnel are expected to be more skilled in operating high-tech equipment related to information and communication technology, including infrastructure facilities for processing Position Check data, Call Detail Record (CDR), and SMS (Short Message Service) such as Position Tracking Tools, CDR Analyst Notebooks/Laptops and *Cellebrite* Mobile Forensics, mobile phones/mobile phones equipped with *Netmonitor Celltrack* software, Analyst Notebooks, and Direction Finder. By having these various skills, the disclosure of cybercrimes through the use of information technology can be carried out effectively.

The three attitudes of Sub-Director V investigators can understand and display *Polri's* professional ethics which is a unitary philosophical ethical basis with rules of conduct and speech regarding things that are required, prohibited, or appropriate for members of the Police to do, both in providing services to the community and in establishing cooperative relations with all elements of society, including telecommunications service provider companies (providers) to obtain data for checking the position of cellphone numbers, Call Detail Record (CDR) and Short Message Service (SMS). Where investigators in establishing cooperative relations should be able to display commendable attitudes and behavior by always respecting human dignity through respect based on the same position/degree, so that synergy will be maintained because each party respects one another.

Collaborating in conducting investigations and investigations in uncovering cybercrime cases because of its borderless nature and does not recognize regional boundaries, cooperation, and coordination with relevant agencies and law enforcement agencies and other countries is very important to do. There is a need for cooperation to facilitate disclosure. In addition, First, building cooperation with telecommunications providers in the jurisdiction to facilitate requests for data regarding the position of cell phones, CDR data, and SMS data. Second, building cooperation with banks in investigating who owns the account, the address of the account owner, and the account transaction itself. Third, building cooperation with the Financial Transaction Reports and Analysis Center (PPATK) to find out the financial transactions of criminals so that they can be blocked. Fourth, build cooperation with internet service providers to be able to find out internet traffic that is used by computer facilities so they can know the computer's IP address.

Fifth, build cooperation/coordination with the prosecutor's office in equating perceptions about the application of the elements of the article in ensnaring the perpetrators of the crime so that the investigation process carried out by the Special Crimes Investigation Unit of the DIY Regional Police can quickly process the filing and fast P.21 because there is no back and forth of case files; Sixth, building cooperation/coordinating/equalizing perceptions with the court is expected by investigators of the Sub-Directorate V of the Criminal Investigation Police in requesting a search permit, the determination of confiscation can be carried out quickly so that the investigation process for the search and confiscation can also be carried out quickly and electronic evidence can be quickly confiscated for the investigation process.

The police carry out law enforcement. After receiving a report, the process of investigation begins. An examination is a progression of steps taken to find an occasion that is associated with being a wrongdoing and decide if it very well may be researched utilizing this regulation's strategy.

Obviously the police are a piece of the law enforcement framework as a component, subsystem, and part. They are alluded to as "Examiners and Specialists" in the ongoing regulation, which incorporates both the Criminal Method Code (KUHAP) and the Guideline of the Indonesian Public Police Number 6 of 2019.

The right to file a written or oral report or complaint with investigators and/or investigators applies to anyone who is a victim, witness, or experiences a crime-related event. Any individual who knows about an intrigue to perpetrate a wrongdoing against life or property, public wellbeing, or public harmony and security is committed to inform specialists immediately.. Each government worker throughout completing his obligations who is familiar with the event of an occasion comprising a lawbreaker act is obliged to report this to the specialist or examiners right away.

At the point when an occasion with a sensible doubt of being a crook act happens, examiners who know about it and get reports or objections about it should promptly lead the essential examination. The specialist should quickly make the important moves inside the structure of the examination assuming that they are discovered in the act without hanging tight for the examiner's organization. The law requires the examiner to present an authority report in regards to this activity to the specialist.

The examination of instances of online misrepresentation varies from ordinary lawbreaker cases in such manner. Since they commonly utilize web-based entertainment and made up accounts, the culprits of these online-based misrepresentation wrongdoings complete their violations whenever, anyplace, and at a vague time without the information on some other people. The purchase and sale of online tickets, motorized vehicles, clothing, electronics, and other items are common examples of online-based fraud. Since exchanges are led on the web, arrangements came to among venders and purchasers are likewise founded on trust. Typically, prior to making an exchange, the vender and the purchaser convey by means of couriers, direct messages, etc. After an understanding is arrived at between the dealer and the purchaser, installment is normally made by moving a specific measure of cash to the merchant's record. The step taken by the Police is to follow the records utilized by the culprits of wrongdoings, where the last whereabouts or position of the culprits of these violations are.

4. Conclusion

The spread of information and communication technology has resulted in a world without borders, prompting significant social shifts. However, the creation of Information and Communication Technology produces positive benefits, but it turns out to be used for negative things. The rise of modern crimes is one of the negative effects of technological advancements. The quantity and complexity of crime, as well as variations in its methods, continue to grow alongside human civilization. The National Police have not done an adequate job of optimizing their use of social media to handle fraud cases. This condition is brought about by deficient HR capacities, both regarding information, abilities, financial plan, offices, and targets. There is currently only one person who has attended information technology vocational education, which has implications for investigator skills in cybercrime disclosure techniques and tactics that are still lacking. The obstacle in handling fraud cases through social media is the budget owned by

Satreskrim. In dealing with online fraud, the Police Criminal Investigation Unit conducts investigations and investigations including uncovering cybercrimes, The Criminal Investigation Sub-Directorate does not yet have the infrastructure to process Position Check data, Call Detail Records (CDR), and SMS (Short Message Service), nor does it know how to carry out tasks because the bureaucratic process that Bareskrim Polri and related agencies/parties use to borrow infrastructure facilities to process Job Check data, CDR, and SMS takes a long time.

References

[1] S. Philippsohn, "Trends in cybercrime - an overview of current financial crimes on the Internet," *Comput. Secur.*, vol. 20, no. 1, pp. 53–69, 2001, doi: 10.1016/S0167-4048(01)01021-5.

[2] H. Ho, R. Ko, and L. Mazerolle, "Situational Crime Prevention (SCP) techniques to prevent and control cybercrimes: A focused systematic review," *Comput. Secur.*, vol. 115, p. 102611, 2022, doi: 10.1016/j.cose.2022.102611.

[3] A. S. Selvik, M. M. Edvardsen, O. Laedre, and J. Lohne, "Opportunity Space for Work-related Crime from Procurement to Production," *Procedia Comput. Sci.*, vol. 196, no. 2021, pp. 894–901, 2021, doi: 10.1016/j.procs.2021.12.090.

[4] E. E. Supriyanto, "Opportunites for Implementation of e-Rupiah Policy as Financial Transaction Innovation in The Pandemic Covid-19," in *Global Policy in Handling Covid-19 Pandemic*, 1st ed., A. Tunda and A. Upe, Eds. Kendari: Rumah Bunyi, 2021.

[5] E. R. Leukfeldt and T. J. Holt, "Cybercrime on the menu? Examining cafeteria-style offending among financially motivated cybercriminals," *Comput. Human Behav.*, vol. 126, no. August 2021, p. 106979, 2022, doi: 10.1016/j.chb.2021.106979.

[6] A. Simonofski, J. Fink, and C. Burnay, "Supporting policy-making with social media and e-participation platforms data: A policy analytics framework," *Gov. Inf. Q.*, vol. 38, no. 3, pp. 1–13, 2021, doi: 10.1016/j.giq.2021.101590.

[7] O. Ribaux and T. R. Souvignet, "'Hello are you available?' Dealing with online frauds and the role of forensic science," *Forensic Sci. Int. Digit. Investig.*, vol. 33, p. 300978, 2020, doi: 10.1016/j.fsidi.2020.300978.

[8] E. E. Supriyanto, H. Warsono, and A. R. Herawati, "Literature Study on the Use of Big Data and Artificial Intelligence in Policy Making in Indonesia," *Adm. J. Ilm. Adm. Publik dan Pembang.*, vol. 12, no. 2, pp. 139–153, 2021, doi: 10.23960/administratio.v12i2.235.

[9] F. M. Dobrick, J. Fischer, and L. M. Hagen, *Research ethics in the digital age: Ethics for the social sciences and humanities in times of mediatization and digitization*. 2017.

[10] J. Eloranta, E. Golson, A. Markevich, and N. Wolf, *Economic history of warfare and state formation*. 2016.

[11] Ahmad Zuhdi, "Perkembangan Metodologi Penelitian Hukum," *J. Huk. dan Perad.*, vol. 1, no. 2, pp. 189–206, 2012.

[12] O. Woolley, *Ecological governance: Reappraising law's role in protecting ecosystem functionality*. 2014.

[13] B. Coban, *Social Media and Social Movements*. London: Lexiton Books, 2016.

[14] N. Agarwal, N. Dokoohaki, and S. Tokdemir, *Emerging research challenges and opportunities in computational social network analysis and mining*. Cham Switzerland: Springer, 2019.

[15] N. Al Mutawa, J. Bryce, V. N. L. Franqueira, A. Marrington, and J. C. Read, "Behavioural Digital Forensics Model: Embedding Behavioural Evidence Analysis into the Investigation of Digital Crimes," *Digit. Investig.*, vol. 28, pp. 70–82, 2019, doi: 10.1016/j.diin.2018.12.003.

[16] V. N. L. Franqueira and G. Horsman, "Towards Sound Forensic Arguments: Structured Argumentation Applied to Digital Forensics Practice," *Forensic Sci. Int. Digit. Investig.*, vol. 32, p. 300923, 2020, doi: 10.1016/j.fsidi.2020.300923.