PERFORMANCE ANALYSIS OF INVESTIGATORS IN UNCOVERING CYBER FRAUD

(Case Study at the West Jakarta Metro Police)

Joshua Oktavianus Siagian[1*], Surya Nita[2], Aldika Martua Sitorus[3], Riska Sri Handayani[4]
[1,3] Police Academy of the Republic of Indonesia, Semarang, Indonesia
[2,4] Police Science Studies Program, School of Strategic and Global Studies, Universitas Indonesia
E-mail: [1)] joshuaoktavianus7@gmail.com

Abstract

The aim of this study is to evaluate the performance of investigators in handling cybercrime cases in the jurisdiction of West Jakarta Metro Police. The research method used is literature review and secondary data analysis from various reliable sources regarding the development of information technology and cybercrime in Indonesia. The research results show that Investigators in the Cybercrime Subunit of West Jakarta Metro Police have shown significant efforts in handling cybercrime cases, especially cyber fraud. They have utilized various investigation methods and techniques in accordance with the applicable laws in Indonesia, including the ITE Law and other related regulations. However, investigators face several challenges, including limited facilities and infrastructure such as inadequate computers and other devices. Budget constraints are also a major obstacle, especially in funding investigative operations outside Jakarta. In addition, poorly organized SOPs and lack of consistency in their implementation also hinder the effectiveness of investigations. This includes inconsistencies in delivering SP2HP in accordance with Perkap Number 14 of 2012. The implementation of information technology, such as Smart Policing and E-SP2HP programs, has helped improve personnel capacity and real-time reporting. However, further evaluation is needed to ensure the effectiveness and integration of this technology with the coordination of relevant institutions. Success in handling cybercrime also depends on cooperation among law enforcement agencies and increased training for cyber police officers. This includes establishing guidelines for handling cybercrime cases and adopting effective digital forensic methods.

Keywords: *Cybercrime, Cyber Fraud, Investigator Performance, Information Technology, Digital Forensics*

1. INTRODUCTION

Indonesia, as a developing nation, has long fallen behind on technological innovations due to inadequate development strategies, in particular due to an undervalued research agenda, leading to technology transfers from advanced industrial nations without sufficient technology mastery being transferred back; ultimately resulting in Indonesia lacking a firm technological basis against cybercrimes.

Digital technology's rapid progress has had a great effect on information access, social interaction and economic expansion - yet also presents potential dangers like fake information spreading or becoming too dependent upon technological platforms. Based on APJII survey data, internet usage among Indonesian citizens reached 215.63 million between 2022-2023; an increase of 2.67% since the previous period (210.03 million users). Indonesia currently boasts 78.19% internet users out of its total population of 275.77 Million individuals. Digital technology has dramatically heightened cybercrime threats, such as malware attacks, hacking and personal data theft, leading to identity theft,

job loss and disruption of critical infrastructure. Unfortunately, most members of society remain ignorant to these dangers while regulations continue to evolve in response to them (Hapsari & Pambayun, 2023).

Cybercrime, particularly actions carried out by black hat hackers or crackers, has been a major concern in recent years (Dioza, 2019). The police play a crucial role in maintaining security and public order, as well as protecting, nurturing, and serving the community in accordance with the Law Number 2 of 2002 regarding the State Police of the Republic of Indonesia. The delegation of authority between government agencies is regulated in this law, where governmental powers can be transferred from one government agency to another. Article 2 of the Law explains that the police function includes maintaining public security and order, law enforcement, protection, nurturing, and serving the community (Melisa & Anggraini, 2021).

The Digital Forensic Unit of the IT & Cyber Crime Subdirectorate of the Criminal Investigation Department of the Indonesian National Police plays a crucial role in collecting digital evidence to uncover criminal activities and identify perpetrators. This unit has been accredited as a testing laboratory according to ISO 17025:2005 standards by the National Accreditation Committee and is also a member of the Asia Pacific Accreditation Committee (APAC).

According to data released by the e-MP Robinopsnal of the Indonesian National Police, cybercrime has seen a significant increase in 2022 compared to the previous year. The number of cybercrime cases has even increased by 14 times. From January 1 to December 22, 2022, the police have handled 8,831 cybercrime cases. All units within the Indonesian National Police and regional police departments are actively involved in addressing these cases. The Jakarta Metropolitan Police Department has been the most active in handling cybercrime cases, with a total of 3,709 cases. In contrast, during the same period in 2021, only 612 cybercrime cases were addressed nationwide, with the involvement of just 26 units.

Cybercrime is a different type of crime compared to conventional street crimes. It emerged alongside the information technology revolution. As stated by Nitibaskara (2006), "Social interactions that minimize physical presence are another characteristic of the information technology revolution. Social deviance adapts to new forms and characters in crime."

The regulation of cybercrime in Indonesia is governed by Law Number 11 of 2008 concerning Electronic Information and Transactions (ITE Law), which was later amended by Law Number 19 of 2016. This ITE Law serves as an important legal basis in addressing various forms of cybercrime, including defamation, dissemination of false information, and hacking. The changes in Law Number 19 of 2016 further strengthen certain articles and provide more clarity regarding the definition and types of criminal acts that can be sanctioned. With this regulation in place, it is hoped to provide stronger legal protection for the public and encourage the more secure and responsible use of information technology.

The SEC (Securities and Exchange Commission) guidelines on cybersecurity disclosure obligations underscore the increasing concerns about the impact of cyber incidents on financial performance, with a significant rise in companies referencing cybersecurity risks in their post-guidance disclosures (Cereola & Dynowska, 2019). The emergence of cyber fraud as a significant threat, exploiting the internet for personal gain and manipulation, further emphasizes the need for enhanced investigative techniques and

countermeasures to disrupt underground fraud (Howard, 2009). Evaluating the performance of investigators in obtaining information, gathering evidence, utilizing investigative techniques, understanding the law, and ensuring personal safety is crucial in effectively combating cyber fraud (Brown & Veneziano, 1992).

Given the background information provided, the objective of this research is to evaluate the performance of investigators in dealing with cybercrime cases in the jurisdiction of West Jakarta Metro Police.

2. RESEARCH METHODS

This study utilized a qualitative research methodology with a field study research design, emphasizing observation and in-depth examination of events at one location - specifically within West Jakarta Metro Police's jurisdiction. Data were collected through primary, secondary, and tertiary sources derived through interviews techniques, observation methods, document studies, document analyses, document triangulation techniques as well as triangulating various sources and collection techniques to ensure data validity. Data analysis involves various stages, such as data reduction, presentation, interpretation and verification. Assessing the performance of investigators requires using several theories as an analytical framework, such as performance theory to measure work effectiveness; law enforcement theory to examine specific practices; resource theory to measure availability and utilization; and information technology theory which examines its effect on performance. Moreover, this analysis takes into account both Chief of Police Regulations as legal foundation as well as relevant legislation as part of this evaluation process (Soekanto, 2004).

3. RESULTS AND DISCUSSION

The investigation of cyber fraud crimes by the Cyber Crime Sat Resrim of the West Jakarta Metro Police is guided by various legal references. The process involves adherence to Law Number 8 of 1981 concerning the Criminal Code, the Chief Regulation of the Republic of Indonesia Criminal Investigation Body Number 3 of 2014 concerning the Standard Operational Procedures for Criminal Investigation Implementation (Perkaba No. 3 of 2014), Police Regulation Number 6 of 2019 concerning Criminal Investigation (Polres No. 6 of 2019), and Law of the Republic of Indonesia Number 19 of 2016 concerning the Amendment of Law Number 11 of 2008 concerning Electronic Information and Transactions (ITE Law) (Dewi & Fahrial, 2021; Rahutomo, 2019). This rule establishes a framework for investigators to effectively address cyber fraud cases, ensuring that the investigation process is in line with legal requirements and standards outlined in Indonesian law (Dekawati & Marbun, 2022).

Based on an interview with the Criminal Investigation Unit of the West Jakarta Metro Police, we discuss the types of cybercrimes they deal with,

> "*The most commonly reported type of crime is cyber fraud, which includes scams through websites, blogs, forums, and social media. Additionally, they also handle cases such as cyber pornography, cyber terrorism, data theft and forgery, hacking, and illegal access. During the period from 2018 to 2020, data from the West Jakarta Metro Police recorded an increase in the number of cyber fraud cases from 105*

cases in 2018 to 132 cases in 2020, with a total of 319 cases over the three-year period."

The interview revealed an increase in the number of cyber fraud cases from year to year, highlighting the expansion of the scope and intensity of criminal activities in the digital realm. This indicates that cybercrime is not only a local threat but also a global phenomenon that requires cooperation between law enforcement agencies and comprehensive efforts to strengthen cyber security in order to protect the public from the increasing risks of digital attacks.

The rise of cybercrime presents a major challenge on both local and global scales, highlighting the importance of cooperation between law enforcement agencies and robust cybersecurity measures to safeguard the public from escalating digital threats. The interconnected nature of the cyber realm enables cybercriminals to operate across borders, underscoring the necessity of international collaboration in addressing cyber threats (Sumadinata, 2023). The law enforcement authorities encounter various challenges in overseeing the virtual world, such as the difficulty of tracing anonymous violators and the technical complexity of digital crime investigations (Baraz & Montasari, 2023). To address this challenge, a framework such as the Cyber Resilience and Law Enforcement Collaboration (CyrLEC) framework has been proposed, emphasizing proactive prevention, early detection, rapid response, and close collaboration with law enforcement to effectively prosecute cyber criminals (Schiliro, 2023). By improving cybersecurity resilience and fostering efficient collaboration with law enforcement, organizations can enhance their ability to safeguard themselves and their communities from the expanding threats of cybercrime.

Interview with the Cyber Crime Subunit I of West Jakarta Metro Police, the investigation stage is considered crucial in handling cybercrime cases. According to the Cyber Crime Subunit I of West Jakarta Metro Police, "*... this stage is often faced with significant challenges. One of the main problems is the high number of reports that are canceled for various reasons. For example, the perpetrator's data is often fake and difficult to trace because of fake IP addresses, changed phone numbers, or inactive accounts. In addition, the slow provision of data from banking institutions is also a barrier, due to reluctance to provide information from customers related to transactions. Another challenge is that perpetrators often come from outside the area, while the budget available for handling such cases is limited*." In the analysis of Cyber Fraud cases, the Cyber Crime Subunit I of West Jakarta Metro Police uses several investigation methods that have proven to be effective. "*... usually tracking using phone numbers, bank account numbers, and through social media. Data collected from 2018 to 2020 shows that tracking phone numbers was done in 102 cases, tracking bank account numbers in 95 cases, and tracking through social media in 85 cases. However, there are also cases that have not been fully uncovered, reaching 181 cases during that period*." This provides an overview of the intensive efforts made by investigators in handling cybercrime in the West Jakarta Metro Police area.

Intensive efforts by investigators in tackling cybercrime involve recognizing the complex and sophisticated nature of cyber threats, demanding specialized responses. Investigators must possess core competencies such as decision-making, problem-solving, and embracing innovation to effectively track cybercriminals and bring them to justice. (Staniforth, 2014). With the increasing reliance on decentralized information technology,

tracking cybercriminals has become a challenge for law enforcement agencies due to the borderless and multi-jurisdictional nature of cybercrime (Kader & Minnaar, 2015). Specialized knowledge of the law and expertise in cyber investigations is essential due to the unique challenges and privacy laws associated with cybercrime (Curtis, 2011). As cybercrime evolves with various forms such as virus attacks, phishing, and identity theft, investigators face the task of keeping up with the changing modus operandi of cybercriminals in order to secure successful prosecutions (Kader & Minnaar, 2015).

The West Jakarta Metro Police Department has encountered difficulties in solving most of the 181 cases that occurred between 2018 and 2020. Nevertheless, the strategy of integrating mobile phone tracking, bank account numbers, and social media has demonstrated its effectiveness by increasing the number of successfully solved cases. The West Jakarta Metro Police Department emphasizes that mobile phone tracking has been the most successful method with a significant number of cases being uncovered. Meanwhile, the lack of success through social media is attributed to the cyber-fraud perpetrators' tendency to use fake identities or not leaving a trace that can be effectively traced after their crimes are committed.

In line with this, (Gupta et al., 2022) stated that the lack of success in combating online fraud through social media can be attributed to the sophisticated tactics used by cybercriminals, such as the use of fake identities and the difficulty in tracking their activities. Cybercriminals exploit social media platforms for various fraudulent activities such as online scams, cyberbullying, and hacking, making it challenging to effectively identify and track them (Gupta et al., 2022). Furthermore, an increase in fraud on social media platforms has been noted, with criminals using unethical social engineering techniques to deceive users and steal data (Hussien & Mohialden, 2023). Efforts to detect and prevent identity fraud on social networks have been made through clustering and classification techniques, but the effectiveness of existing strategies remains uncertain (Borkar et al., 2022).

The Cyber Crime Unit of West Jakarta Metro Police highlights the importance of human factors in the performance of an institution, which is in line with the theory of resource factors. According to this theory, human factors are the main assets that play a key role in achieving organizational goals. However, as mentioned, the lack of quantity and inadequate skills of human resources can be a serious obstacle to the performance of the institution. The problems faced, such as difficulties in recruiting and retaining quality human resources, reflect the real impact of the imbalance between organizational needs and the availability of suitable workforce. This not only affects internal productivity but also reduces the institution's ability to provide adequate services to the public.

The Cybercrime Subunit I at the West Jakarta Metro Police Department has uncovered several major challenges. Firstly, the limitation of facilities and infrastructure is a critical issue. Despite having 36 computers for investigation, some of them are severely damaged, and only one laptop is available. This is clearly insufficient considering the complexity of cyber-based cases that require sophisticated technological devices. Moreover, the lack of printers and scanners can hinder the efficient process of evidence collection. Secondly, budget constraints are a serious problem. Data shows that there is no specific budget allocation for the Cybercrime Subunit I, which may result in a lack of funds for training, equipment, or technological infrastructure needed to effectively handle these cases. Furthermore, many cyber fraud cases occur outside Jakarta, but there is no budget allocation for investigations outside the area, making cross-border law

enforcement difficult. Thirdly, the lack of integrated and comprehensive Standard Operating Procedures (SOP) is also an issue. The existing SOPs are not fully organized or well-integrated, making it difficult to socialize and understand thoroughly by all investigators. A lack of deep understanding of SOPs can hinder the effectiveness of investigations, slow down the process, and increase the risk of procedural errors. Overall, these challenges indicate the need for significant improvements in terms of investment in facilities and infrastructure, better budget allocation, and enhancement in the development and implementation of comprehensive SOPs. It is crucial to enhance the capabilities of the Cybercrime Subunit I in handling cybercrime cases more effectively and efficiently in the future.

The investigation process in handling cyber fraud cases by the Cyber Crime Subnit I of West Jakarta Metro Police revealed several inconsistencies with existing regulations. Although National Police Regulation Number 14 of 2012 stipulates that SP2HP reports must be submitted every 15 days for complex cyber fraud cases, in reality, updates on the investigation are only provided once or delayed. Data from questionnaires show that 78% of complainants receive SP2HP reports more than 21 days after the scheduled deadline, highlighting the inconsistency with the proper procedures. These delays not only hinder transparency and public trust in the legal process but also do not align with the principle of timeliness in organizational performance theory. Furthermore, challenges in summoning witnesses and suspects also act as hindrances to the investigation. The majority of complainants, such as housewives and entrepreneurs, face difficulties in providing testimonies due to time constraints and other reasons like reluctance and logistical constraints. This indicates the need for a more effective time management strategy and a more sensitive approach to various professions and social conditions of complainants to ensure a more efficient and fair investigative process.

The West Jakarta Metro Police's initiatives in addressing challenges in investigations at Cyber Crime Subnit I highlight several aspects that require thorough evaluation. Initially, the lack of approved budget for investigations outside of DKI Jakarta, particularly beyond Java Island, poses a significant obstacle. This is concerning given the cybercrime's nature, which frequently involves locations beyond Jakarta. The limited budget for specialized equipment and operations may restrict investigators' performance in uncovering crimes.

Secondly, the implementation of Profession, Procedural, Discipline, Practice, and Piety (PPDLT) shows that despite the basic principles such as professionalism and discipline being applied, there are still weaknesses in the consistent implementation of SOP. This is reflected in the low percentage of members who answered that activity SOPs are always available or well-organized. The lack of consistency in implementing PPDLT can hinder efforts to improve the quality of investigation and overall unit performance Foeh & Papote (2021) demonstrates the positive impact of well-structured SOPs in reducing errors and operational incidents, emphasizing the importance of standard procedures in enhancing quality management.

Thirdly, through the adoption of the Smart Policing program, the West Jakarta Metro Police Department is striving to modernize their approach to cybercrime law enforcement. However, despite the increase in personnel capacity and the implementation of technologies such as E-SP2HP for real-time reporting, there is still a need for evaluation of the effectiveness of this newly developed SOP. The success of the program

will depend on how well it can integrate coordination with relevant institutions and ensure that all members are skilled in relevant soft and hard skills.

The implementation of cybercrime prevention policies, as seen in the Central Jakarta Metro Jaya Police, emphasizes the importance of communication, resources, and training for cyber police officers (Damayanti & Ismowati, 2021). Furthermore, the urgency of establishing guidelines for handling cybercrime cases within the Indonesian National Police Department highlights the need for digital forensic methods and effective evidence collection strategies (Anggraeny et al., 2022). By integrating predictive policing strategies, enhancing cybercrime prevention policies, and establishing digital forensic guidelines, the West Jakarta Metro Police take significant steps to modernize their approach in combating cybercrime.

Overall, west Jakarta Metro Police's response to cybercrime requires further strengthening budget support, improving implementation consistency of SOPs, and developing smart policing approaches with continuous evaluation in order to be efficient and effective against digital crime in their region. By doing so, this approach should increase efficiency and effectiveness against digital crimes that threaten its community.

4. CONCLUSION

Based on the findings, it can be concluded that West Jakarta Metro Police investigators in Subunit I Cybercrime demonstrate significant efforts when handling cyber fraud cases, using various investigative techniques in accordance with Indonesian laws such as ITE Law or other relevant regulations. Unfortunately, however, investigators face several barriers such as limited facilities/infrastructure such as inadequate computers/devices as well as budget limitations which restrict their investigations outside Jakarta.

Moreover, poorly organized SOPs and lack of consistency in their implementation also impede the effectiveness of investigations, including discrepancies in delivering SP2HP in accordance with National Police Chief Regulation Number 14 of 2012. The implementation of information technology, such as the Smart Policing program and E-SP2HP, has helped enhance personnel capacity and real-time reporting, but further evaluation is still needed to ensure the effectiveness and integration of this technology with the coordination of relevant agencies.

Success in combating cybercrime also depends on cooperation among law enforcement agencies and enhancing training for cyber police officers, including the establishment of guidelines for handling cybercrime cases and the adoption of effective digital forensic methods. Overall, this research indicates that despite significant efforts in combating cybercrime by investigators at West Jakarta Metro Police, there are still many aspects that need to be improved and enhanced to achieve higher effectiveness in investigating cyber cases in the future.

REFERENCES

Anggraeny, I., Monique, C., Wardoyo, Y. P., & Slamet, A. B. (2022). The Urgency of Establishing Guidelines for Handling Cybercrime Cases in the Indonesian National Police Department. *KnE Social Sciences*, 349–359.

Baraz, A., & Montasari, R. (2023). Law enforcement and the policing of cyberspace. In *Digital Transformation in Policing: The Promise, Perils and Solutions* (pp. 59–83). Springer.

Borkar, B. S., Patil, D. R., Markad, A. V, & Sharma, M. (2022). Real or fake identity deception of social media accounts using recurrent neural network. *2022 International Conference on Fourth Industrial Revolution Based Technology and Practices (ICFIRTP)*, 80–84.

Brown, M. F., & Veneziano, C. (1992). Evaluating investigator job performance: An analysis of practitioner opinions. *Justice Professional*, *7*(2), 93–104.

Cereola, S. J., & Dynowska, J. (2019). Investigating the Impact of Publicly Announced Information Security Breaches on Corporate Risk Factor Disclosure Tendencies. *Journal of Cybersecurity Education, Research and Practice*, *2019*(3).

Curtis, G. (2011). *The law of cybercrimes and their investigations*. Taylor & Francis.

Damayanti, D., & Ismowati, M. (2021). The Implementation Of The Cybercrime Prevention Policy At The Metro Jaya Police Station In Central Jakarta. *Proceedings Of The 1st International Conference On Science And Technology In Administration And Management Information, Icstiami 2019, 17-18 July 2019, Jakarta, Indonesia*.

Dekawati, G., & Marbun, W. (2022). Pendekatan Teori Criminal Thinking Pada Kasus Pembunuhan Anak Oleh Anak. *Krisna Law : Jurnal Mahasiswa Fakultas Hukum Universitas Krisnadwipayana*, *4*(1), 59–67. https://doi.org/10.37893/krisnalaw.v4i1.15

Dewi, N. M. T., & Fahrial, R. L. (2021). Suatu Kajian Yuridis Terhadap Penggunaan Alat Bukti Elektronik dalam Kejahatan Cyber dalam Sistem Penegakan Hukum. *Jurnal Hukum Saraswati (JHS)*, *3*(2).

Dioza, R. (2019). *Kebijakan Kriminal Penanganan Cyber Crime Pada Satuan Reserse Kriminal Polres Aceh Tenggara*. Doctoral dissertation.

Foeh, J. E. H. J., & Papote, E. (2021). Analisis Faktor-Faktor Yang Mempengaruhi Kinerja Anggota Ditlantas Kepolisian Daerah NTT. *Ultima Management: Jurnal Ilmu Manajemen*, *13*(1), 148–163.

Gupta, A., Matta, P., & Pant, B. (2022). Identification of cybercriminals in social media using machine learning. *2022 International Conference on Smart Generation Computing, Communication and Networking (SMART GENCON)*, 1–6.

Hapsari, R. D., & Pambayun, K. G. (2023). Ancaman cybercrime di indonesia: Sebuah tinjauan pustaka sistematis. *Jurnal Konstituen*, *5*(1), 1–17.

Howard, R. (2009). *Cyber fraud: tactics, techniques and procedures*. Auerbach Publications.

Hussien, N. M., & Mohialden, Y. M. (2023). An overview of fraud applications and software on social media. *Handbook of Research on Advanced Practical Approaches to Deepfake Detection and Applications*, 1–11.

Kader, S., & Minnaar, A. (2015). Cybercrime investigations: Cyber-processes for detecting of cybercriminal activities, cyber-intelligence and evidence gathering. *Acta Criminologica: African Journal of Criminology & Victimology*, *2015*(sed-5), 67–81.

Melisa, M., & Anggraini, N. (2021). Peran Kepolisian Dalam Melakukan Pembinaan Keamanan Dan Ketertiban Masyarakat Desa Melalui Pendekatan Komprehensip (Penelitian Di Polsek Baturaja Barat). *Jurnal Pro Justitia (JPJ)*, *2*(1), 76–88.

Nitibaskara, R. (2006). *Tegakkan hukum gunakan hukum*. Penerbit Buku Kompas.

Rahutomo, T. A. (2019). Strategi Pemolisian Pencegahan Kejahatan Penipuan Melalui Media Elektronik di Polres Metro Jakarta Pusat. *Airlangga Development Journal*, *3*(2), 146–160.

Schiliro, F. (2023). Building a Resilient Cybersecurity Posture: A Framework for Leveraging Prevent, Detect and Respond Functions and Law Enforcement Collaboration. *ArXiv Preprint ArXiv:2303.10874*.

Soekanto, S. (2004). Faktor-faktor yang mempengaruhi penegakan hukum. *PT Raja Grafindo Persada, Jakarta*.

Staniforth, A. (2014). Police investigation processes: practical tools and techniques for tackling cyber crimes. In *Cyber Crime and Cyber Terrorism Investigator's Handbook* (pp. 31–42). Elsevier.

Sumadinata, W. S. (2023). Cybercrime And Global Security Threats: A Challenge In International Law. *Russian Law Journal*, *11*(3), 438–444.

Copyrights