The Efforts to Improve the Investigators' Performance in the Disclosure of Cyber Fraud Criminals by Subnit I Cyber-Crime Criminal Reserse of West Jakarta Metro Police Resort

Joshua Oktavianus Siagian

Akademi Kepolisian Republik Indonesia, Semarang, Indonesia
joshuaoktavianus7@gmail.com

Abstract

This study analyzes the investigators' performance in Subnit I Cyber Crime Criminal Reserse of West Jakarta Metro Police in the disclosure of cyber fraud crimes. During 2018 and 2020, the cyber fraud cases have been increased significantly. Consequentially, the optimal investigators' performance in disclosing the crime is required in order to continue their duty as the protector of the community. The qualitative approach was used with the type of field study research. To analyze the performance of investigators, the performance theory, the law enforcement theory, the resource theory, and information technology theory, were used, along with some relevant Perkapolri and prevailing laws regulations. The results of the study show that the investigators' performance at the investigation and inquiry stage to uncover the cyber fraud crimes has not been optimal. West Jakarta Metro Police has been working to improve the investigators' performance by implementing PPDLT, specific allocation, and smart policing, but the efforts have not been sufficient. Several factors that hinder the optimal efforts to improve the investigators' performance are limited personnel, request to increase the budget that has not been approved, no specific methods have been implemented to resolve the stack of cases, and the unavailability of technical SOP. Thus, it is necessary to transform the training and education methods for the investigators to tackle cyber fraud, to reform and trim bureaucratic procedures, and to strengthen the synergy with various parties that can help the investigations and both internally and externally.

I. Introduction

In article 13 of Law No. 2 of 2002 it contains the main tasks of the Indonesian National Police, namelymaintaining public order and security, enforcing the law, and providing protection, protection and service to the community. With this main task, the National Police, as a law enforcement apparatus, must prioritize security and order in society and its environment. However, with the development of the times, the duties of members of the Indonesian National Police have become increasingly difficult and complex, one of which is the result of technological developments such as the development of the internet.

According to research conducted by social media management platform HootSuite and marketing agency We Are Social conducting research entitled "Global Digital Reports 2020", the results of this research show that internet users in Indonesia alone have reached 175.4 million people out of a total of 272.1 million. Indonesian residents (We Are Socially Inc., 2020). 93% of internet users between the ages of 16 – 64 years buy and use online or

online products/services(We Are Socially Inc., 2020).This triggers an example of a new crime that often occurs in modern times, namely online fraud or better known as cyber fraud (Chazawi, 2011).

Even more so with the Covid-19 pandemicat the end of 2019 to date (January 2021) which has led to an increase in cyber fraud cases. The latest data (27 March 2021) shows cases of Covid-19 sufferers in Indonesia reaching 1,492,002 cases with 40,364 deaths and 1,327,121 patients recovering and will continue to increase until an unknown time (Worldometer, 28 March 2021, URL). This fact has resulted in changes in people's activities including the shift from offline shopping (outside the network) to online (in the network/online). In 2020, the Ministry of Communication and Informatics received 192,000 reports regarding cases of cyber fraud, one of which is the result of people tending to buy goods through electronic media and sometimes do not check in advance the legitimacy of the websites they visit (JPNN, 2020, URL).

In addition, based on data obtained from the Cyber Crime Subunit I, the Criminal Investigation Unit of the West Jakarta Metro Police, there has been an increase in cyber fraud crimes. The total number of fraudulent crimes through online media such as websites, blogs and other social media or what is called cyber fraud has increased from year to year. Can be seen in Table 1.

Table1. Table of Cyber Fraud at Polres Metro Jakarta Barat

NO	YEAR	*TOTAL CRIME*	*CRIME CLEARANCE*	PERCENTAGE
1	2018	105	50	47.6%
2	2019	82	35	42.6%
3	2020	132	53	40.15%

Source: West Jakarta Metro Police Criminal Investigation Unit, 2020

The facts show that criminal cases have increased*cyber fraud*at Polres Metro Jakarta Barat was not accompanied by an increase in criminal clearance which later became an interest in submitting research with the title "Efforts to ImproveInvestigation Performance in the Disclosure of Cyber Fraud Crimes by Subunit I Cyber Crime Criminal Investigation Unit of the West Jakarta Metro Police". Because the prohibitions and threats of sanctions are clearly regulated in the ITE Law and Article 378 of the Criminal Code, this research will focus on examining the performance of investigators who will provide solutions to overcome and increase criminal clearance of cyber fraud at the West Jakarta Metro Police.

II. Research Methods

The research approach used is a qualitative approach with a type of field study research. The location of the research was carried out in the jurisdiction of the West Jakarta Metro Police. The data sources used are primary, secondary, and tertiary sources with data collection techniques through interviews, observation, and document studies. Data validation used data triangulation and then the data was analyzed using data reduction, data presentation, drawing conclusions, and verification. Analysis of the investigator's performance used is performance theory, law enforcement theory, resource theory, information technology theory, as well as Perkapolri and relevant laws and regulations.

III. Results and Discussion

3.1 Performance of Investigators of Subunit I Cyber-crime Criminal Investigation Unit of the West Jakarta Metro Police

Investigators assigned to the West Jakarta Metro Police Criminal Investigation Unit I Cyber Crime Unit in conducting cyber fraud investigations use the references in Law no. 8 of 1981 concerning KUHAP, Criminal Code, Regulation of the Head of Criminal Investigation of the Indonesian National Police Number 3 of 2014 concerning Standard Operational Procedures for Carrying Out Criminal Investigations (Perkaba No. 3 of 2014), Regulation of the Head of the National Police of the Republic of Indonesia Number 6 of 2019 concerning Investigation Criminal Acts (Perkapolri No. 6 of 2019) and Law of the Republic of Indonesia Number 19 of 2016 concerning Amendments to Law Number 11 of 2008 concerning Information and Electronic Transactions (ITE Law).

With so many laws being the reference for investigators as well as other related laws, the references and laws should be more comprehensive. Thus, criminal acts of cyber crime should be easier to uncover by investigators as indicated by the parallel crime clearance rates with total crime. However, the reality has not worked out that way.

By using the performance theory put forward by Agus Dharma (2003: 355), researchers analyzed why the performance of Cyber Crime Subunit I investigators in disclosing Cyber Fraud crimes was not optimal. This can be seen from the following indicators: (1) quantity; (2) quality; (3) timeliness; (4) cooperation; and (5) responsibility.

There are various types of cyber crimes in Subunit I Cyber Crime Polres Metro Jakarta Barat, such as cyber fraud which includes fraud through web blog forums and social media, cyber porn, cyber terror, cyber thief and forgery, hacking, cracking and illegal access, ATM skimming, defamation and others. Below is data on the number of crimes that have entered the West Jakarta Metro Police.

Table 2. Number of Types of Crime in Cyber-crime Subunit I Year 2018 to 2020

NO	CRIME TYPE	YEAR		
		2018	2019	2020
1	*Cyber fraud* (Online fraud via the web, blogs, forums and other social media)	105	82	132
2	*Cyber Porn, Exploitation child and woman*	1	2	4
3	*Cyber*Terror, threats and hostility	6	3	3
4	*Cyber*Thief and Forgery	14	8	12
5	*Hacking, Cracking, Illegal Access*	9	15	9
6	ATM skimming	5	13	22
7	Defamation and Insults online	20	30	18
8	*Cyber*Attack, Government Espionage	-	-	-

Source: West Jakarta Metro Police Criminal Investigation Unit Urmin

From the table above it can be concluded that the type of cyber fraud crime is the type of crime that is most frequently entered each year, namely in the 2018 period there were 105 cases increasing to 132 cases in December 2020. The total number of cyber fraud crimes when added up from 2018 to 2020 is as many as 319 cases.

3.2 Investigation Performance of Subunit I Cyber Crime Criminal Unit West Jakarta Metro Police

The investigation stage by the Cyber Crime Subunit I of the West Jakarta Metro Police Criminal Investigation Unit has an important role. At this stage the investigator seeks information from the public. However, at this stage, reports often fail because (i) the data is from fake and one-time use actors (fake IP addresses, cellphone numbers have been changed, accounts used to commit fraud are no longer active), (ii) the slow provision of data from banks because they have a tendency to be reluctant to provide data from customers and (iii) actors come from outside the region while the budget that must be provided is limited.In investigating Cyber Fraud cases, there are 3 methods of investigation that are usually used by personnel, namely, tracking cellphone numbers, tracking account numbers and tracking via social media as the researcher summarizes in the following table:

Table 3. Methods of Completion of Cyber Fraud Crimes from 2018 to 2020

No	Methods of Completion of Cyber Fraud Crimes	Amount
1	Tracking No Hp	102
2	Account No Tracking	95
3	Tracking via Social Media	85
4	Not yet Revealed	181

Source: Urmin West Jakarta Metro Police Criminal Investigation Unit

Even though there are still many unresolved cases from 2018 to 2020, namely 181 cases, by combining the application of the three methods of investigation, the West Jakarta Metro Police are actually trying to increase the number of uncovered cases. As illustrated in Figure 1 below:
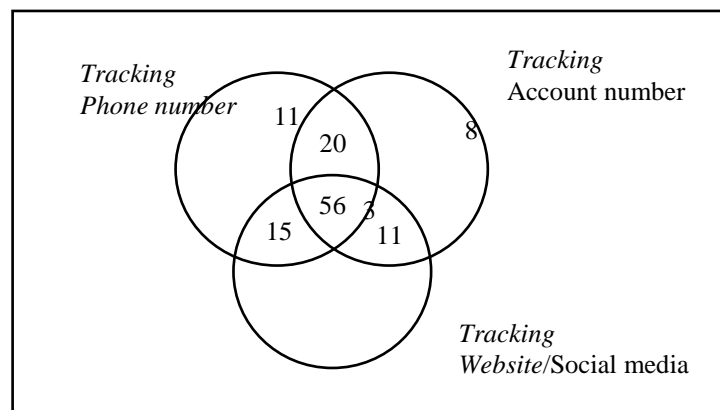

Figure 1. Venn diagram Method of Investigating Revealed Cases

From the picture above, it can be seen that the combination or combination of the three methods resulted in more cases being uncovered, namely 56 cases out of 124 criminal cases, compared to using only 1 or 2 methods. The diagram above also reflects that the most effective method is cell phone number tracking because it results in the most uncovered investigation cases, namely 102 criminal acts, followed by account number tracking with 95 criminal acts, and social media tracking with only 85 criminal acts. The small number of cases revealed through social media is because the perpetrators of cyber fraud generally do not have social media and/or use fake social media as an instrument for committing fraud and deactivate it immediately after the fraudulent action is completed, so there is no website data showing the perpetrator's profile.

3.3 The Investigative Performance of Subunit I Cyber-Crime Investigators at the West Jakarta Metro Police Criminal Investigation Unit

The following is a description of the investigative performance that investigators carried out in uncovering criminal acts of cyber fraud:

1. Insufficient Quantity and Quality of Personnel to Conduct Investigations

Table 4. Comparison of Ideal Conditions and Actual Conditions of West Jakarta Metro Police Criminal Investigation Unit Personnel

NO	Position	DSP	REAL	KET
1	Head of Criminal	1	1	-
2	Wakasatreskrim	1	1	-
3	Kaurbinopsal	1	1	-
4	Kaurmintu	1	1	-
5	Bamin	2	2	-
6	Banum	2	1	-1
7	Kaurident	1	1	-
8	Pair of ident	2	2	-
9	Identification	12	10	-2
10	Kanitdik	6	6	-
11	Head of Subunit I	12	12	-
12	Banit	144	96	-48
13	Banum	6	5	-1
	AMOUNT	**191**	**137**	**-54**

Description: DSP (Ideal Conditions), RIIL (Actual Conditions)

Referring to the List of Polri Personnel Composition (DSPP) in Perkap No. 23 of 2010 concerning Organizational Structure and Work Procedures, the West Jakarta Metro Police Criminal Investigation Unit ideally has 191 personnel. However, from table 4. currently there is still a shortage of personnel. The researcher has made a comparison between (i) ideal conditions and (ii) actual conditions.The most significant deficiency is in the number of Banit, with a total of 48 personnel to be filled. This non-ideal condition certainly has the potential to give rise to massive implications for the performance of investigators at the West Jakarta Metro Police Cyber-crime Subunit I because the allocation burden is too heavy on existing personnel.

Table 5. Personnel of Subunit I Cyber Crime Polres Metro Jakarta Barat

No.	EDUCATION	TOTAL PERSONNEL	INFORMATION
1.	**DIKBANG**		
	SELL	-	-
	PTIKSESPIM	1	
2.		-	
	TRAINING DIRECTOR	9	3 personnel have not carried out cyber-crime training
3.	**DIKUM**		
	S2	1	
	S1	5	5 not yet graduated
	NOT GRADUATE	5	

Source: West Jakarta Metro Police Criminal Investigation Unit

In Table 5, there are problems related to the not ideal education that members of the West Jakarta Metro Police Cyber Crime Subunit I should have. As Criminal Investigators, all members of the West Jakarta Metro Police Cyber Crime Subunit I should have completed their law degree studies. However, there were still 5 personnel from the West Jakarta Metro Police Cyber Crime Subunit I who had not finished their law degree studies. . In addition, there is not a single member of the Cyber Crime Sub-unit of the West Jakarta Metro Police who carries out education regarding ITE or Cyber Crime. Of course, this substantially affects the performance of investigators at the West Jakarta Metro Police Sub-unit in disclosing cyber fraud because the investigator's expertise is not yet specialized.

This is not in accordance with the theory of resource factors, where one of them is the Man factor (human), asassets that play a role and are very important asfactorthe main mover in the implementation of all activities or agency activities. Of course, the insufficient number of resources and the inadequate expertise of resources will affect the overall performance of an agency.

2. Investigators have not mastered how to utilize special investigative tools

The researcher distributed questionnaires that asked respondents, namely investigators at Cyber Crime Subunit I of the West Jakarta Metro Police regarding the investigator's mastery of special investigation tools such as ANB, direction finder, and interpretation of the results of call data records from the Bareskrim Monitoring Center. From there it is known that only about 30% of investigators understand how to use the data. The results of the questionnaire are presented in the form of a diagram in Figure 2 below.

***Figure 2.** Diagram of Mastery of Investigation Tools by Investigators*
Source: Author Documentation

3. Limited facilities and infrastructure in cyber-crime subunit I

Table 6. Inventory data for the West Jakarta Metro Police Criminal Investigation Unit

NO	MATLOG TYPE	Amount	Good	Lightly damaged	Heavily damaged	Information
1	Computer	36	34	-	2	2 Piknas inventory
2	Printers	23	23	-	-	-
3	Faxmile	1	1	-	-	-
4	Telephone	1	1	-	-	-
5	Police Line	1	1	-	-	-
6	Test kits	1	1		-	-
7	Laptops	1	1	-	-	-
8	Wifi	10	10	-	-	-

Source: West Jakarta Metro Police Criminal Investigation Unit

Computers and laptops are certainly important elements in facilitating investigations related to cyber-based cases. However, of the 36 computers available to members, 2 of them were seriously damaged. While only 1 laptop is available. This is even with the condition, it is not known what the ideal amount should be allocated specifically for the Cyber Crime Sub-unit and separately from other Sub-units. Meanwhile, there are 23 printers in total, so there is no printer for each computer. Researchers also did not find whether there was a scanner facility, because it was not listed in the inventory. Even though a scanner is very likely needed to enter data. Not to mention, there is no standardization for adequate types of computers and laptops with the latest technology that is capable.

This is inconsistent with the resource factor theory, where one of them is the Machine factor, iea tool/facility utilized to obtain greater convenience as well as a tool

used for work efficiency and maximizing the activities carried out and material factors (material), namely infrastructure used during an activity with the aim of expediting and maximizing activities made in accordance with organizational management.

4. Budget limitations in subunit I cyber-crime

From a total of 319 cases of cyber fraud, the location of the perpetrators of cyber fraud in the West Jakarta Police area totaled 110 cases. Meanwhile, the location of the perpetrators who were outside the city of Jakarta was 209 cases. This can be seen in table 7 below.

Table 7. Locations of Cyber Fraud Actors from 2018 to 2020

NO	crime scene	AMOUNT
1	JAKARTA CITY	110
2	OUTSIDE THE CITY OF JAKARTA	209

Source: Urmin West Jakarta Metro Police Criminal Investigation Unit

Based on the table above, the West Jakarta Metro Police Criminal Investigation Unit Budget for the 2020 FY, it can be analyzed the fact that (i) there is no specific and detailed allocation of funds for Subunit I Cyber-crime and (ii) there is no allocation of funds for investigations and investigations outside DKI Jakarta. This is of course a conventional obstacle that can be destructive to law enforcement by investigators. Especially considering that actually cyber-crime should be included in the budget with a difficult case index because the level of settlement of cases requires special expertise and the space where incidents can cross borders.

5. The unavailability of Standard Operating Procedures (SOP) for Internal and External Investigations and Investigations

The existing SOPs and other internal policies related to cyber-crime investigations are also not integrated and organized. So that it is difficult to socialize it to investigators as a whole, as a result not all investigators know, actually read, and understand the applicable SOPs. Even on the substance of the SOP, many are not comprehensive and there are still many things that can be criticized.

6. SP2HP acceptance late

Based on Article 1 point 17 Perkap No. 6 of 2019, SP2HP is a letter of notification to the complainant/complained about the results of the investigation progress. For cyber fraud cases, in Perkap No. 14 of 2012, previously it was stipulated that the length of the SP2HP process was every 15 days because cyber fraud is a difficult crime. However, in actual terms, the progress of the investigation results was only given once by the investigator, even though it should have been informed periodically or it was given, but it was too late.Based on Perkaba No. 3 of 2014, SOP SP2HP is that SP2HP is given to the complainant/complainant signed by the investigator's supervisor for difficult cases, given on the 15th day, 30th day, 45th day, 60th day, 75th day and 90th and for the stage of completion and submission of case files, SP2HP is given at the time of handing over the first stage of case files.

Researchers distributed questionnaires to the reporters. On the question whether the reporter received the SP2HP in a timely manner, 78% of respondents stated that they received the SP2HP in more than 21 days, as illustrated in Figure 3 below:
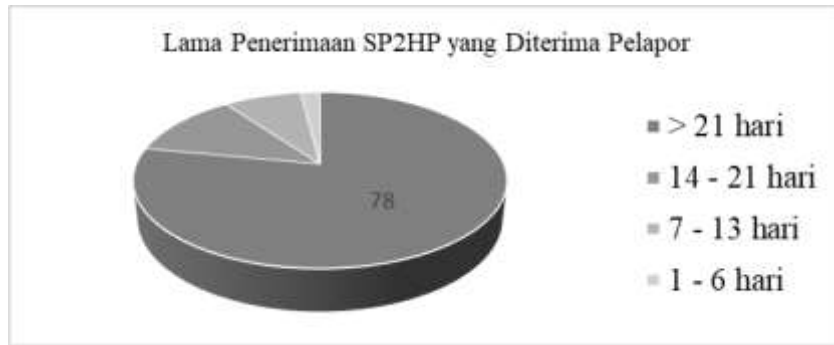
Figure 3. *Diagram of the Old SP2HP Receipt Received by the Reporter*
Source: Author Documentation, 2021

Delivery of SP2HP that was late and had not used a digital application but by mail resulted in the sending of SP2HP by Subunit I investigators*CyberCrime*late from the ideal timeframe, which is 15 days. The delay in sending SP2HP is not in accordance with Agus Dharma's theory of performance (2003:355). In measuring performance, one of the parameters is timeliness in completing work to achieve efficient and effective results.

7. Obstacles in summoning witnesses and suspects

Examination of witnesses for cyber fraud was not optimal because sometimes reporters did not have other witnesses to corroborate, and the majority of reporters did not want to give their cellphones to be examined because they were reluctant to the police, there was other information, they were worried the process would take a long time, and various other reasons. In addition, there were obstacles found in the examination of expert witnesses because they required a mature schedule. In general, it is difficult for expert witnesses to arrange the examination schedule, which causes delays in investigative activities.

Regarding the reasons for the reporter's reluctance to be examined, the researcher was able to obtain the following data Figure 4, the majority felt reluctant because they were afraid of investigators:
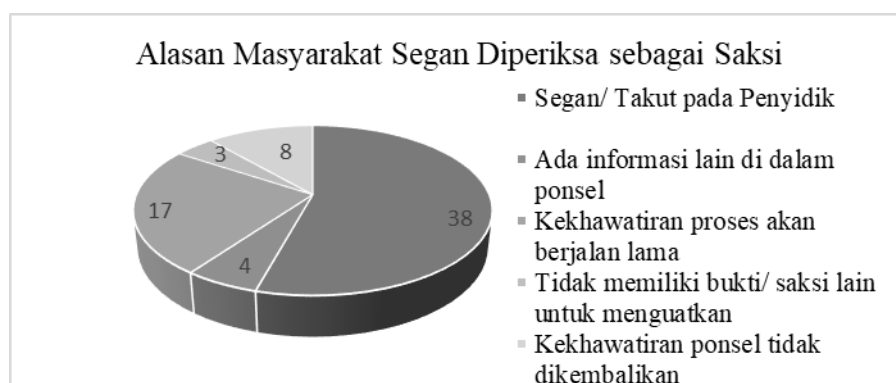
Figure 4. *Diagram of the reasons why people are reluctant to be examined as witnesses*
Source: Author Documentation, 2021

In addition, as presented in Table 8, the largest number of reporters or victims of cyber fraud in the jurisdiction of the West Jakarta Metro Police during the 2018 to 2020 period were mostly housewives with 112 reporters, followed by entrepreneurs with 85 reporters and private individuals with 81 reporter. It is also difficult for these three groups to be examined as witnesses because (i) housewives have to take care of their children, (ii)

entrepreneurs are often out of town for business, and (iii) private employees have difficulty obtaining office permits.

Table 8. Types of Work for Cyber Fraud Victims, 2018 to 2020

NO	TYPE OF WORK	AMOUNT
1	PRIVATE	81
2	SELF-EMPLOYED	85
3	CIVIL SERVANT	17
4	HOUSEWIFE	112
5	TNI AD	14
6	RETIRED	10

Source: Urmin West Jakarta Metro Police Criminal Investigation Unit

In fact, the termination of investigations in Subunit I Cyber Crime has also followed Perkaba No. 3 of 2014 concerning SOP for Investigating Criminal Acts and Perkap No. 6 of 2019. However, it would be a shame if the problems that resulted in SP3 were due to a lack of evidence. This lack of evidence can be caused by skilled actors, but can also occur if investigators fail to uncover additional evidence due to a lack of facilities and infrastructure, delays in personnel handling cases due to lengthy bureaucracy which slows down the disclosure process and loss of evidence because the perpetrators have removed it. as a result of the investigator's lack of response.

The researcher summarizes the investigator's workload analysis as follows:

Figure 5. *Workload Analysis of Investigators of Subunit I Cyber-Crime Criminal Investigation Unit of the West Jakarta Metro Police*
Source: West Jakarta Metro Police Urmin and Author Documentation

Based on the 2020 Workload Analysis (ABK) data, the achievement of organizational effectiveness only reached a score of 0.71. If it is categorized according to the Regulation of the Head of the Indonesian National Police Number 15 of 2014 concerning Workload Analysis within the Republic of Indonesia National Police, this figure is included in category C (sufficient). This sub-optimal performance category resulted in the number of crime clearance not in line with the total crime in Cyber Crime Sub-unit I of West Jakarta Metro Police.

3.4 Efforts to Improve Investigator Performance in Disclosure of Cyber Fraud Crimes by Sub-unit I Cyber-crime Criminal Investigation Unit of the West Jakarta Metro Police

The West Jakarta Metro Police are trying to make various efforts at the investigation and investigation stage to deal with various challenges and obstacles that have the potential to reduce the performance of investigators in the West Jakarta Metro Police Cyber Crime Subunit I. The efforts that have been made are as follows:

a. Specific Allocation Program for Investigations outside the Area

Budget is a very important factor so that the activities carried out and wanted to be carried out by West Jakarta Metro Police investigators in carrying out their duties and responsibilities can run smoothly. The West Jakarta Metro Police Cyber Crime Sub-unit I has attempted to submit a budget plan for investigations outside the DKI Jakarta area, especially outside Java Island, but this budget request has not yet been approved by the leadership at Polda/Bareskrim. This is of course very difficult considering the characteristics of cybercrime that are mushrooming in society, the type of crime disclosure that requires the use of special and modern equipment, and the location of the perpetrators who are often outside DKI Jakarta. It takes high awareness of the urgency of increasing budget allocations, so that the Polres can independently provide sufficient facilities and infrastructure to support and increase the actual number of crime clearances.

b. Professional, Procedural, Discipline, Practice and Piety (PPDLT) Application

So far, the West Jakarta Metro Police have only made efforts as an application of the PPDLT principle, which is indeed a fundamental thing to be applied to all members of the Polres. The researcher then attempted to further examine the effectiveness of the implementation of the PPDLT that had been carried out. However, based on the results of the questionnaire, it was found that all PPDLT elements that were implemented had not been carried out optimally so that the impact on improving investigator performance was still minimal. Details can be seen in Figure 6 below:

Figure 6. *Implementation of PPDLT*
Source: Author documentation, 2021

c. *Smart Policing* in Cyber-Crime Investigations and Investigations

The smart policing method is a policing model that is expected to be able to overcome conventional problems, cyber or virtual problems in the digital era as well as forensic problems. This program is implemented to create a professional, intelligent, integrity, and modern figure that can be implemented at all levels from the National Police Headquarters to its regional units, including the West Jakarta Metro Police. In smart policing, capacity building is also carried out for Polri personnel, to sharpen their soft skills and hard skills. The implementation of this smart policing program is also an attempt to build an effective SOP. The following are parts of the implementation of smart policing carried out by the West Jakarta Metro Police for Cyber Crime Subunit I: (1) submission of a direction finder tool, (2) increased coordination with Bareskrim MCs, providers, and banks, (3) implementation of E -SP2HP for progress reports in real time, (4) increasing capacity building and professionalism, and (5) increasing coordination with witnesses and expert witnesses.

3.5 Factors Influencing Efforts to Increase Investigator Performance in Disclosure of Cyber Fraud Crimes by the West Jakarta Police Criminal Investigation Unit

Efforts to improve the performance of investigators have been carried out by the West Jakarta Metro Police, but the total number of crimes is still not comparable to crime clearance, which shows that the completion of cyber fraud cases is still quite low at the investigation and investigation stage so that they cannot be followed up or delegated to the prosecutor's office. Researchers analyzed the factors that influence efforts to improve performance that are not yet optimal, including:

1. Human (Man)

Influencing human factors can be divided into internal factors and external factors. The internal factor in this case is the human resources within the West Jakarta Metro Police, namely: (1) the minimum number of qualified personnel who can transfer knowledge, (2) the minimum number of personnel who can replace other personnel when not on duty to attend special training cyber crime, (3) training programs or training as well as seminars and workshops and even e-learning conducted by the West Jakarta Metro Police have not been specially programmed and standardized.

Meanwhile, the external factors in question are factors from outside the organization or the West Jakarta Metro Police cyber crime unit but still within the Polres unit or from outside the Polres unit organization which hinder efforts to improve the performance of West Jakarta Metro Police investigators in disclosing cyber fraud crimes, namely (1) the lack of support from reporters or witnesses, (2) the lack of support from unscrupulous providers or banks in providing data and information support needed by investigators, (3) the lack of public knowledge about the investigative and investigative process which results in people being reluctant to be called as witnesses.

2. Money

Apart from not agreeing on an increase in the budget because there is no urgency that was conveyed properly by the West Jakarta Metro Police to describe the urgent situation in Subunit I Cyber Crime, the existing budget at the Polres Metro Jakarta Barat has not been managed properly and has not been allocated specifically for Subunit I Cyber Crime so that it is not optimal for investigative and investigative activities.

3. Materials

Material is the infrastructure used to support the ongoing activity. Following are the infrastructures that support the continuation of investigation activities of Subunit I Cyber-crime Polres Metro Jakarta Barat: (1) there is no module for dealing with cyber crime and cyber fraud at the Polres level, (2) there is no clear document regulating the reward and punishment system, (3) SOPs related to cyber-crime investigations are incomplete and sporadic so that investigators do not really understand and read the SOP provisions, (4) there is no MoU with external parties.

4. Machine

Machines, in this case related to tools or facilities to facilitate cyber fraud investigation activities: (1) Facilities that support investigations and investigations of cyber crimes are still lacking and conventional. Starting from computers and laptops that have not been standardized to accommodate the latest technology, (2)Essential facilities such as the Cyber Crime Investigation Satellite Office laboratory, Strategic Information Laboratory and Tactical Operation Center, digital/forensic laboratory, and monitoring center are only available at Polda level.

5. Methods

Factors that impede efforts to improve performance based on the method are (1) there is no method specifically applied to train the abilities of investigators and investigators in handling cyber crime, (2) it is difficult to get new investigators because investigator allocation procedures must be shared with other Polres areas, (3) there is no method that can be applied to complete the pile of work and cases handled by the limited number of investigators at the West Jakarta Metro Police. This causes there is no time for investigators to develop themselves through training or training.

IV. Conclusion

1. Investigators' performance has not been optimal both in terms of quality, quantity and timeliness of completing work, which can be seen from the investigation stage, sending sp2hp to the reporter, examining witnesses and the confiscation stage which has not been completed optimally. These stages are influenced by the quantity and quality of personnel in the utilization of investigative tools, investigative and investigative facilities and infrastructure, the budget for diligence in carrying out tasks, the level of public trust in the police and the implementation of procedures.
2. Efforts to increase the performance of investigators (specific allocation, PPDLT, and smart policing) have been carried out quite well but have not run optimally because there are still many inhibiting factors found during their implementation. The budget allocations for out-of-region areas have not been accounted for by the Polda, the investigation SOP has not been updated, the reward and punishment system has not been made in writing, the training has not presented IT experts and cyber-crime experts from outside the police agency, the special cyber-crime investigative tool has not been acc. Headquarters, MoU with banks and providers has not been made in writing, and human errors are still found in carrying out work.
3. Factors that influence efforts to increase investigator performance consist of 5 factors: (1) humans/man, the leadership plays a positive role in overseeing the course of efforts to increase performance and act professionally; and negatively there are still members who are less enthusiastic in the field of cyber-crime and are not transitioning (?) to

using digital-based applications; externally: witnesses, expert witnesses and bank providers and operators of the Bareskri Monitoring Center still find it difficult to cooperate with the police, (2) money/money where the special budget for subunit I cyber-crime has not been approved by the management, (3) material, namely SOP There are no cyber-crime investigations and MoUs with other agencies, and written evidence of a reward and punishment system has not been made clear.

References

Amstrong, Michael. (2010). Armstrong's handbook of Human Resorce Management Practice 11th edition. United Kingdom: Kogan Page Limited.

Badan Pembinaan Hukum Nasional. (2004). Laporan Tim Forum Dialog Hukum dan Non Hukum Kelompok Kerja Bidang Hukum dan Teknologi BPHN.

Chazawi, A. (2011). *Tindak Pidana Informasi dan Transaksi Elektronik*. Bayumedia Publishing.

Dharma, Agus. (2001). Manajemen Kinerja. Jakarta: Pustaka Pelajar

Dharma, Agus. (2006). Manajemen Prestasi Kerja. Rajawali Pers.

Gilbert, Noperto. (2016). Penyidikan Tindak Pidana Judi Online oleh Subdit II Cyber-crime DITRESKRIMSUS POLDA Sumatera Utara. Jakarta: Sekolah Tinggi Ilmu Kepolisian.

Indartono, Setyabudi. (2016). Pengantar Manajemen: *Character Inside*. Yogyakarta: Fakultas Ekonomi Universitas Negeri Yogyakarta.

JPNN. (2020). Wabah Virus Corona: Ada yang Tega Tipu Pembeli Masker hingga Rp 200 Juta. Diambil dari: https://www.jpnn.com/news/wabah-virus-corona-ada-yang-tega-tipu-pembeli-masker-hingga-rp-200-juta

Kepolisian Negara Republik Indonesia. (2012). Peraturan Kepala Kepolisian Negara Republik Indonesia No. 14 Tahun 2012 tentang Manajemen Tindak Pidana.

Kepolisian Negara Republik Indonesia. (2019). Peraturan Kepala Kepolisian Negara Republik Indonesia No. 6 Tahun 2019 tentang Penyidikan Tindak Pidana.

Makarim, Edmon. (2003). Kompilasi Hukum Telematika. Jakarta: Rajagrafindo Persada.

Mangkunegara, Anwar Prabu. (2009). Manajemen Sumber Daya Manusia Perusahaan. Bandung: Rosda.

Mangkunegara, Anwar Prabu. (2013). Evaluasi Kinerja SDM, Cetakan Keempat. Jakarta: Refika Aditama.

Republik Indonesia. (1981). Undang-undang No. 8 tahun 1981 tentang KUHP. Lembaran Negara RI Tahun 1981, No. Sekretariat Negara. Jakarta

Republik Indonesia. (1999). Undang-undang No. 8 tahun 1999 tentang Perlindungan Konsumen

Republik Indonesia. (2002). Undang-undang No. 2 tahun 2002 tentang Kepolisian Negara Republik Indonesia.

Republik Indonesia. (2016). Undang-undang No. 19 tahun 2006 tentang Informasi dan Transaksi Elektronik.

Robbin, Stephen P. dan Mary Coulter. (2012). *Management* 7th edition. New Jersey: Pearson education Inc.

Soekanto, Soerjono. (2013). Faktor-faktor Yang Mempengaruhi Penegakan Hukum. Jakarta: Raja Press.

Terry, George R. dan Leslie W. Rue. (2013). *Principles of Management.*

We Are Socially Inc. (2020, February). *Digital 2020 - We Are Social*. Dikutip Agustus 2020 dari We Are Social: https://wearesocial.com/digital-2020

We Are Socially Inc. (2020, January). *Digital 2020: Indonesia*. Dikutip Agustus 2020 dari Data Reportal: https://datareportal.com/reports/digital-2020-indonesia

Worldometer. (2020, August). *Total Coronavirus Cases in Indonesia*. Dikutip Agustus 2020 dari Worldometer: https://www.worldometers.info/coronavirus/country/indonesia/