JPI Jurnal Pajak Indonesia
Indonesian Tax Review

Optimization of Tax Revenue Through Digital Forensic Activities for Tax Purposes

Panji Wisnu Nugroho[1]* · Nur Farida Liyana[1]

Accepted: 05/12/2024
Volume 8, Nomor 2, 2024

Abstract

This research aims to review the implementation of digital forensic activities and their impact on tax revenue at the Directorate General of Taxes (DGT), especially in South Jakarta I Regional Tax Office. This study details the research methods used, including literature review methods to understand the overview of digital forensic activity implementation, and field research methods through interviews with Digital Forensic Expert and academics experienced in tax law enforcement processes. The research results indicate that the implementation of digital forensic activities has been carried out in accordance with applicable Standard Operating Procedures. However, digital forensic activities have not yet had a significant impact on tax revenue. There are several obstacles faced in the digital forensic business process, such as the limited number of Digital Forensic Experts in DGT, uneven human resource capabilities, and limited availability of supporting devices. Therefore, this research is expected to serve as a guide for policymakers to optimize state revenue through increased effectiveness in law enforcement, especially those related to digital forensic activities.

Keywords Tax · Revenue · Digital Forensic · Tax Law · Electronic Evidence

1 INTRODUCTION

The targets and actualization of tax revenue in Indonesia have steadily increased over the years to support the country's economy through

✉ Corresponding Author
3032210011_panji@pknstan.ac.id

[1] Politeknik Keuangan Negara STAN, Tangerang Selatan, 15222, Indonesia

infrastructure development, societal welfare improvement, and other initiatives. However, the realization of tax revenue does not fully reflect its true potential. Based on the 2018 tax effort, it was found that actual tax revenue only achieved 43% to 69% of its full capacity (Harjowiryono, 2019), and the tax ratio in 2021 only reached 9.11% of GDP (Dihni, 2022). Furthermore, there is a positive correlation between Taxpayer compliance levels and tax revenue (Suryadi and Subardjo, 2019). Consequently, the government is required to increase the efforts to uncover potential tax revenues while enforcing stricter tax compliance laws.

Tax potential exploration is more efficient when accompanied by an effective and efficient tax administration system. The system should provide convenience for Taxpayers and reduce compliance costs. Furthermore, the tax administration system must adapt to technological advancements, as these developments significantly influence the business processes of Taxpayers. Therefore, all taxation stakeholders—including tax authorities and Taxpayers—must respond to these advancements (Asmarani, 2021). For instance, the digitization of tax data processing and document storage, such as tax returns and invoices, has shifted to paperless operations, reducing paper consumption and the need for physical storage (Astawan, 2022). This transformation impacts legal enforcement and tax supervision procedures, moving away from traditional methods reliant solely on physical documents (books, records, etc.). This technological evolution introduces new challenges in tax law enforcement and oversight.

One key aspect of tax law enforcement is through tax audits, whose primary purpose is to gather audit evidence for conclusions regarding compliance (Febrian, 2019). The advancement of technology facilitates the collection of digital audit evidence, which is easily replicated and altered compared to physical evidence (Rachmie, 2020). This underscores the unique characteristics of digital data compared to physical data.

While digital data usage in taxation improves efficiency, it also heightens risks of fraud in tax administration. Consequently, specific procedures are needed to ensure legal certainty in tax enforcement, particularly in audits, initial evidence examinations, and investigations. Such procedures fall under the domain of digital forensics. In accounting, forensic methods serve as investigative procedures to authenticate

accounting data and ensure its legal validity (Adekoya et al., 2020). Similarly, digital forensics involves handling electronic data to produce legally admissible information (DJP, 2022).

Digital forensic activities in taxation consists of two main tasks: electronic data processing and electronic data analysis (DJP, 2022). Data processing includes extracting and recovering electronic data, while electronic data analysis generates relevant information for tax law enforcement. Using specific hardware and software, digital forensics aids in detecting tax fraud practices, including evasion and avoidance. For example, digital forensics can uncover hidden asset accounts, trace Taxpayer money flows, and identify fraud patterns in tax reporting and payment. This ensures tax authorities maintain equity within Indonesia's tax system in both physical and digital realms.

The advantages of digital forensics lie in its ability to process large datasets quickly and accurately, which is difficult to achieve manually. For instance, email communications can serve as electronic evidence during legal investigations (Baroto & Prasetyo, 2020). Additionally, digital forensics has supported tax audit processes and secured tax revenues in Bali and Nusa Tenggara Regional Tax Offices (Shavitri & Darma, 2020). Thus, digital forensics enhances public confidence in the tax system, Taxpayer compliance, and long-term tax revenue.

This research based upon Shavitri and Darma's (2020) study, which demonstrated the impact of digital forensic and audit policy implementation on tax revenue success. However, this research distinguishes itself by focusing on the business processes of digital forensics and specifically examining the South Jakarta I Regional Tax Office. It seeks to review the implementation of digital forensic activities in taxation, assess their impact on the Core Tax Administration System (CTAS), and analyze their influence on tax revenue while identifying challenges faced by Digital Forensic Experts. From a theoretical perspective, this research serves as a reference for developing digital forensic activities in tax administration. Practically, it provides guidelines for policymakers to enhance law enforcement effectiveness through digital forensic activities in taxation.

2 LITERATURE REVIEW

Theory of Evidence

The evidentiary process is an important phase in the court system, namely to ensure that the trial facts in a case are obtained in a correct and fair manner and procedure. The evidentiary system adopted in Indonesia is based on the theory of evidence based on negative law (negative wettelijk) (Ante, 2013). The negative evidentiary theory explains that the guilt or innocence of a defendant is determined by the judge's belief based on the method and existence of valid evidence according to the law (Anam, 2022). This is reflected in Article 183 of the Indonesian Criminal Code (Kitab Undang-Undang Hukum Perdata/KUHAP), namely to obtain a conviction that a crime has occurred, there must be at least two valid pieces of evidence and the judge must obtain a conviction that a crime has occurred. This theory is a combination of two previously existing evidentiary theories, namely the positive evidentiary system according to law (positief wettelijk) and the conviction in time system.

Theory of State Revenue

State revenue is one of the important factors for the government to run the government. Smith (1776) explained that in collecting state revenue, the government must pay attention to four main principles, namely the principles of equity, certainty, convenience, and economy (Setiawan, 2019). In essence, the theory of state revenue can explain the reasons why citizens are willing to pay levies to the government and accept supervision from the government.

The achievement of state revenue targets depends on law enforcement and government supervision so that the obligation to pay official levies in the form of taxes can be fulfilled by citizens. The risk of tax evasion by citizens can occur if they believe that only some people pay taxes and other citizens can freely carry out tax avoidance practices without being known by the tax authorities and not receiving appropriate punishment. Therefore, the government can use sanctions and punishments for people who are unwilling to pay taxes in order to increase state revenue and the level of community compliance in paying taxes can be better.

Electronic Data/Evidence

Electronic data is a collection of information stored in digital/electronic form. Electronic data emerged along with the development of the era,

namely data presented on paper (paper-based data) causing various problems and having a high error rate both during the data collection stage and the digitization process (Ley et al., 2019). Electronic data has the characteristics of being easy to access, store, and share quickly. Electronic data is also very easy to change from its original form. Even so, electronic data has several risks such as security threats from cyber-attacks and is prone to data leaks, so an adequate electronic data security and protection system is needed.

Legal evidence in the current information technology era has provided space for electronic data to become evidence to enforce the law in court. Quoted from Kartika (2019), Makarim (2004) explains that electronic evidence is evidence obtained from crimes that utilize technological devices to direct a crime in the form of electronic data either stored in the technological device itself or has been processed through a certain information technology equipment or some other form such as traces of an activity utilizing information technology.

Although electronic evidence has not been explicitly regulated in the Criminal Procedure Code, several laws and regulations in Indonesia have facilitated and regulated that electronic data can be used as valid evidence in court (Kartika, 2019). For example, in Law Number 11 of 2008 as amended by Law Number 19 of 2016 concerning Electronic Information and Transactions (UU ITE) in Article 5 it is explained that electronic data/documents are recognized as valid legal evidence. Thus, legal evidence in the form of electronic data in the form of emails, text messages, electronic documents, voice recordings, or videos that meet standards can be recognized in the investigation process or during the court process.

Digital Forensic Investigation

Digital forensics is a branch of forensic science that focuses on the collection, analysis and interpretation of digital evidence to find a bright spot regarding a crime that is generally related to technology, information and communication. Digital forensics was born from a series of digital revolution processes that forced the existing legal order to create a new legal process such as investigators who are experts in computer forensics, forensic methods, forensic equipment, and techniques that must be updated (Ami-Narh et al., 2008).

Digital forensics has several frameworks that can be applied according to

needs. However, in this study, the framework used is from the National Institute of Justice (NIJ), namely through the five main stages of digital forensics explained in the following figure.

Figure 1. Digital Forensic Framework based on NIJ

Source: Agarwal *et al.* (2011)

The Role of Electronic Data in Digital Forensic

Society's dependence on the use of technology has made electronic data an important element in the process of resolving various legal cases. For example, in cybercrime investigations, electronic data obtained from the perpetrator's computer system can serve as evidence of illegal activity. Crimes that occur in cyberspace can be proven using digital forensics methods by acquiring and analyzing data that has been permanently deleted using certain applications (Riskiyadi, 2020). Furthermore, electronic data can also be applied in various other criminal investigations, such as murder or theft, where digital communication can help reveal motives, alibis, or schemes for certain crimes. A number of methods can be applied in the application of forensic science to obtain electronic data. These methods include but are not limited to data recovery, network analysis, and malware analysis (Parasram, 2020). The data recovery process is to search for, identify, and repair data that has been deleted or damaged. Network analysis refers to the monitoring and evaluation of data flows in a network to detect suspicious activity. Meanwhile, malware analysis refers to the exploration and research of malicious software to determine its origins and the effects that arise from its activities.

Digital Forensics for Tax Purposes

Adekoya et al. (2020) recommend the use of forensic methods in accounting and taxation more widely in various tax offices in Nigeria because it has been proven to be able to increase transparency and accountability of tax compliance and revenue by minimizing the level of tax evasion and tax crimes. This is expected to strengthen tax law enforcement and provide maximum deterrent effects to perpetrators of

tax evasion and tax crimes. The use of forensic methods in accounting and taxation has also been shown to have a significant impact on tax law enforcement in Jordan. Al-Sharairi (2017) provides several recommendations, one of which is that there is a significant influence in reducing tax evasion cases carried out by a number of industrial companies in Jordan. The forensic method is considered to have provided a bright spot for the tax authorities in Jordan because it is able to identify various ways that several industrial companies use to get around paying taxes that are due.

3 METHOD, DATA, AND ANALYSIS

The research was conducted by collecting various data as a basis for further processing through certain research techniques. This study uses primary data in the form of data and documents regarding tax law enforcement carried out through digital forensics activities. The data is used to determine how the implementation of the digital forensics business process is carried out. The next primary data is the results of interviews with Digital Forensics Personnel in the form of past experiences when conducting digital forensics activities for tax purposes. In addition, other primary data collected are the results of interviews with academics who are experienced in the field of General Provisions and Tax Procedures (Undang-Undang Ketentuan Umum dan Tata Cara Perpajakan/KUP), especially related to tax law enforcement procedures at the Directorate General of Taxes. Then, the secondary data used in this study are in the form of scientific journals from within the country and international journals related to digital forensics as well as a collection of news regarding the development of the application of CTAS in the business process of law enforcement through digital forensics activities.

This study uses qualitative techniques carried out using library research methods and field research methods. This research method uses library sources in the form of books, journals, articles, and other documents. In addition, the author also uses references in the form of laws and regulations in this study. Both sources are used to obtain an overview of the implementation of digital forensic activities both in general and specifically at the Directorate General of Taxes.

The field research method was carried out by conducting direct interactive interviews with informants relevant to the topic of this research, namely Digital Forensic Personnel who are directly tasked with

carrying out digital forensic activities for tax purposes. This was chosen to obtain qualitative data in the form of an overview of the implementation of digital forensics, its impact on tax revenues, and the obstacles faced by Digital Forensic Personnel in carrying out their duties. The interview method was chosen because it is the most appropriate method to obtain an overview of digital forensic activities directly from task implementers in the field. Several questions asked to Forensic Personnel broadly cover technical, legal, and practical aspects related to the implementation of digital forensics in supporting the effectiveness of the tax system.

The second informant is an academic who is an expert in the field of General Provisions and Tax Procedures (KUP). This interview aims to obtain qualitative data in the form of information regarding digital forensics and the relationship between the tax law enforcement business process and its impact on tax revenues in a work unit. In addition, the interview was also conducted to obtain other qualitative data regarding the impact of the implementation of the CTAS on the law enforcement business process at the DGT, especially on the implementation procedure for digital forensic activities. The questions asked were the legal aspects of the implementation of digital forensic activities and the impact of CTAS on changes in digital forensic business processes.

4 RESULT AND DISCUSSION

Process of Implementing Digital Forensic Activities for Tax Purposes

Digital Forensic procedures for tax purpose are regulated in Chapter IV and Chapter V of SE-36/PJ/2017. This regulation is based on three main international standards, namely ISO 27001, ISO 27002, and ISO 27005. ISO 27001 regulates information security management in an organization or institution. This standard provides a framework that allows organizations to identify, evaluate, and mitigate risks related to information security. Organizations are required to implement a number of policies and procedures to maintain the confidentiality, integrity, and availability of sensitive information. ISO 27001 also requires continuous monitoring and evaluation of information security controls. ISO 27002, on the other hand, provides guidance on information security practices by covering 114 security controls divided into 14 main categories. This helps organizations identify, evaluate, and implement controls that are appropriate to their needs. Finally, ISO 27005 is a standard that provides

guidance on information security risk management through five main steps, which include policy setting, risk identification, risk analysis, risk evaluation, and monitoring and revision. This is important to ensure the security of the organization's information, comply with applicable laws, and manage risks effectively.

The issuance of digital forensic assignments is carried out based on requests from Law Enforcement Officers within the Directorate General of Taxes, in this case the South Jakarta I Regional Office of the Directorate General of Taxes before the implementation of digital forensic activities begins. The Law Enforcement Officers in question are Investigators, Initial Evidence Examiners, and Tax Inspectors. Thus, the criteria for Taxpayers selected to be the object of digital forensic activities are based on the assessment or professional considerations of Law Enforcement Officers. In addition, Taxpayers who are the objects of digital forensic activities are Taxpayers who generally use information technology devices in their daily activities so that the data, documents, and information obtained are mostly in the form of electronic data.

There are several changes in business processes that occur in digital forensics activities due to the implementation of the CTAS which will start running in 2024. Data Trigger that has the potential for law enforcement (special criteria) must first go through an examination process and then can go to a advance law enforcement process such as digital forensic procedures, preliminary evidence examinations, and criminal investigations. Meanwhile, after the implementation of CTAS, DGT will have a procedure to assess whether information, data, reports, or complaints (IDLP) have the potential and follow-up based on the level of risk that is divided into low, medium, and high so that advance law enforcement actions can be taken. The reason is that criminal acts in taxation are applied as a last resort (ultimum remidium) and the tax authorities must prioritize the state revenue side. Thus, changes in the law enforcement business process in CTAS are implemented to increase the efficiency and validity of the data to be processed, as well as minimize the potential for abuse of power by the tax authorities.

The digital forensic process regulated in Director General of Taxes Circular Letter Number SE-36/PJ/2017 includes 5 main steps consisting of electronic data acquisition, electronic data processing and analysis, reporting of digital forensic activities, electronic data storage, and

evaluation of digital forensic activities. The Digital Forensic Implementation Unit of the South Jakarta I Regional Tax Office in implementing digital forensic procedures has implemented the five stages. The following is an explanation of the description of the implementation of digital forensic activities at the South Jakarta I Regional Tax Office.

Electronic Data Acquisition Procedures

Electronic data acquisition is the process of obtaining electronic data that can be achieved through access, download, duplication, and/or other methods so that Electronic Data can be used as valid evidence in front of the law. There are several hardware and software that can be utilized by Digital Forensics to support their activities. The hardware includes computers, laptops, printers, HDDs, Solid State Drives (SSDs), Flashdisks Drive, USB Write Blocker, Ninja Forensics Duplicator, Tableau Forensics Image, Oxygen Forensics Kits, Encase Portable Device, XRY Mobile Forensics Tools, etc. The software used in Digital Forensic acquisition are Imaging/Imager Apps, Digital Advance Responsive Toolkit (DART), USB Write Blockers Apps, Duplicator Apps, Autopsy, Encase Forensics, and other applications. In the process of acquiring Electronic Data, Digital Forensic Officer carry out the following steps: Law Enforcement Officers show assignment documents to the Taxpayer to be examined, obtain approval, and assistance from the Taxpayer, or other parties during data acquisition. Furthermore, Digital Forensic Officer collect information related to the information system used by the Taxpayer through interviews or other methods. Next step is to identify the device suspected of being the storage media for Electronic Data and record it in the digital device information sheet.

The next process involves collecting electronic data from electronic devices using imaging methods to duplicate Electronic Data. Digital Forensic Officer are also responsible for documenting the electronic data acquisition process in detail. The results of the electronic data acquisition are given an identity, and the electronic data collection report must be created. Digital Forensic Officer then receive the results of the electronic data acquisition from the party requesting support for digital forensic activities, using the Electronic Data Handover Report (Berita Acara Serah Terima/BAST).

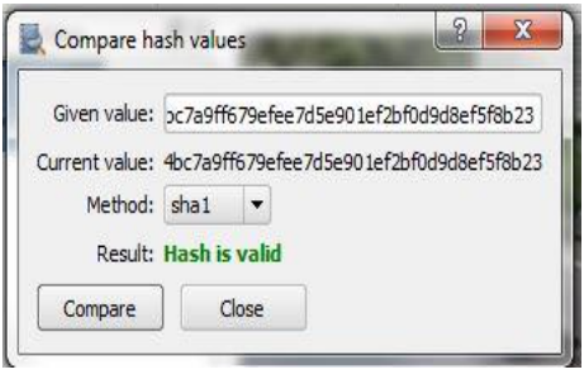
In addition, if law enforcement officers carry out these activities without the assistance of digital forensic personnel, law enforcement officers are

required to follow the procedures from the beginning but without creating BAST document. The digital forensics officer from DGT also can ask for help from external parties to the DGT who are considered more expert in carrying out digital forensics activities if it found that the process in the field encounters obstacles. Those external parties include the Ministry of Communication and Digital, Police Officer, and Prosecutor.

Electronic Data Processing and Analysis Procedures
Electronic data processing is the process of extracting and recovering electronic data from imaging into the original form of data. Electronic data analysis is the activity of interpreting recovered electronic data into an informative form of data. The process of processing and analyzing electronic data is carried out by the digital forensic officer appointed based on a decree issued by the Digital Forensic Unit (Unit Pelaksana Forensik Digital/UPFD), in this case the South Jakarta I Regional Tax Office. Electronic data processing and analysis involves several steps that crucial. First, a duplicate image file from electronic data is created as an initial step. Then, the hash value on the duplicated image file is verified with the hash value listed in the Minutes of Electronic Data Collection. Furthermore, the process is continued with the processing and analysis of the duplicated image file using digital forensic devices.

All stages and techniques used during the processing and analysis process, along with the results, are recorded in the duplicate image file. This information is recorded in the Digital Forensic Process Report (LPTFD). Finally, the results of digital forensic processing and analysis are submitted to the party requesting support for digital forensic activities using the Minutes of Handover (BAST) of Electronic Data Processing Results. This process is a series of important steps in ensuring the integrity and reliability of the electronic data obtained. Electronic data that has been given a hash value will have a series of certain codes that are unique and can be verified for their truth through certain applications so that the electronic data obtained from digital forensic activities can be guaranteed to be valid. The following is an example of the results of hash data verification which can be seen in Figure 2 as follows;

Figure 2. Example of Hash Value Verified values



Source: Kusuma and Prawiranegara (2019)

Digital Forensic Reporting

Reporting is the process of documenting and reporting the entire series of digital forensic activities in each assignment. In the context of reporting digital forensic activities, there are two types of reports, the first report is Task Implementation Report in the context of electronic data collection, is a document prepared by digital forensic personnel for each forensic assignment. This document covers important aspects, such as the basis for the assignment, the identity of the Taxpayer, the Taxpayers faced, a list of electronic data obtained, and activity records. This report must be submitted to the Head of the Digital Forensic Implementation Unit within a maximum of 5 (five) working days after the assignment is completed, using a specific format. Based on the results of interviews with informants, it is known that the procedure for reporting the results of digital forensic activities in the South Jakarta I Regional Tax Office has been implemented in accordance with the five-day working period.

In addition, there is a Digital Forensic Task Implementation Report (LPTFD), which is also prepared by digital forensic personnel for each digital forensic activity assignment. This document includes elements such as title, introduction, implementation of electronic data collection, implementation of electronic data processing and analysis, implementation of electronic data storage, and closing. The LPTFD concept must be notified to the Head of the Digital Forensic Implementation Unit, and this report must be submitted within a maximum period of 6 (six) months from the date the Digital Forensic

Task Force (STFD) was issued, using a specific format. If the Tax Auditor, Initial Evidence Examiner, or Investigator conducts digital forensic activities without the assistance of digital forensic personnel, the results of the implementation of digital forensic activities can be included in the report on the results of the examination activities, examination of initial evidence, or investigation of criminal acts in the taxation sector.

Electronic Data Storage

The process of storing electronic data by the Digital Forensic Implementation Unit is carried out with a step-by-step procedure. First, the Digital Forensic Personnel submit Electronic Data in the form of an original image file to an officer at the Digital Forensic Implementation Unit, namely an echelon III structural unit managed by the Examination, Collection, Intelligence, and Investigation (PPIP) Sector of the South Jakarta I Regional Office of the Directorate General of Taxes with an Electronic Data Storage Report. Then, the officer receives the original image file and creates documentation and archiving of the receipt and submission of Electronic Data. Then, the officer stores the original image file received in a special storage place. If necessary, Digital Forensic Personnel, Tax Inspectors, Initial Evidence Inspectors, and Investigators can borrow Electronic Data from officers at the UPFD. Borrowing and returning Electronic Data uses the Electronic Data Borrowing and Returning Form.

Evaluation of Digital Forensic Activities

Evaluation of digital forensic activities is carried out through the preparation of a Routine Digital Forensic Report followed by Monitoring and Evaluation of Digital Forensic Activities. The Routine Digital Forensic Report is a report prepared by the UPFD in the form of a recapitulation of Digital Forensic activities that have been carried out for one quarter. The Routine Digital Forensic Report is confidential. The report is submitted by the Head of the UPFD to the Director of Law Enforcement no later than the 10th (tenth) of the following month after the quarter ends. Monitoring and Evaluation of digital forensic activities is carried out centrally by the Directorate of Law Enforcement. The Directorate of Law Enforcement monitors and evaluates Digital Forensic activities, including to evaluate: a) appointment of Digital Forensic Personnel; b) implementation of Digital Forensic activities; c) administration of Digital Forensics; and d) development of Digital Forensics, which has been carried out at the UPFD. Monitoring and

evaluation of Digital Forensic activities are carried out by considering the Routine Digital Forensic Report or other matters. The results of the implementation of monitoring and evaluation of Digital Forensic activities are stated in a report that at least contains: a) research on the completeness of Digital Forensic administration; b) research on procedures for Digital Forensic activities; and c) conclusions, opinions, and suggestions from the Digital Forensic monitoring and evaluation team. The report on the implementation of monitoring and evaluation of Digital Forensic activities can be used as material for improving and increasing the quality of Digital Forensic activities in the future.

The Impact of Digital Tax Forensics Activities on Tax Revenue

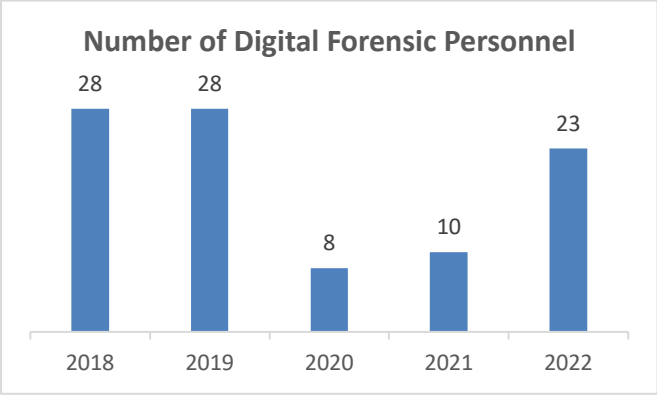
Digital forensics processes are generally utilized in tax law enforcement to collect electronic evidence that can be used in court. Tax law enforcement is important to carry out because it has a significant impact on a country's tax revenue, such as in Ghana, which is one of the countries with the lowest tax revenue rates compared to other middle-income countries. The IMF (2019) states that there are four solutions to increase tax revenue in Ghana, one of which is improving and increasing formal provisions of tax law.

Most Taxpayers have now adopted a computerized bookkeeping system so that the data, documents, and information they have are available in digital data. Therefore, it is important to ensure that digital forensic procedures are implemented correctly in current tax law enforcement. If the digital forensic process is not carried out in accordance with the procedure, there is a possibility that the digital data obtained does not have an adequate level of integrity and has the potential to be rejected in the trial process. In addition, the adoption of technology and digitalization of business processes by Taxpayers can further increase the efficiency and effectiveness of the implementation of Taxpayer supervision duties and functions through digital forensic activities for tax officers.

The information obtained states that digital forensic activities can help Law Enforcement Officers uncover tax avoidance practices carried out by Taxpayers. By using electronic data, documents, and information obtained from Taxpayers, Law Enforcement Officers can further understand the business processes, bookkeeping, and tax reporting by Taxpayers. This can help in detecting tax avoidance practices and finding appropriate evidence of such deviations by comprehensively studying the analysis and interpretation of the results of the electronic evidence that

has been obtained. For example, the digital forensic process can help identify assets hidden by Taxpayers to avoid paying taxes that should be paid. In the work area of the South Jakarta I Regional Tax Office, digital forensic activities have not had a significant impact on tax revenues. There are at least three reasons that explain this can happen. First, the Human Resources owned by the South Jakarta I Regional Tax Office are still limited because there are not many employees in the South Jakarta I Regional Tax Office who have the qualifications, competence, and experience to be able to become Digital Forensics Personnel. The development of number of the number of Digital Forensics Personnel are shown in the following graph.

Figure 3. Number of Digital Forensic Personnel at the South Jakarta I Regional Tax Office per year (2018-2022)



Source: Public Relation Division, South Jakarta I Regional Tax Office

The number of digital forensic personnel in the South Jakarta I Regional Tax Office has fluctuated from year to year with the lowest number reaching only 8 employees in 2020 and the largest number reaching 28 employees in 2018 and 2019. This shows that the number of forensic personnel has decreased in 2020 to 2021 by up to 70% due to the Covid-19 pandemic which has greatly affected the number of law enforcement activities supported by digital forensic activities. Even so, along with the situation that is starting to return to normal, it can be seen in the graph that the number of forensic personnel is starting to return to normal with an increase in the number of employees reaching 130% which is expected to maximize law enforcement activities in the South Jakarta I Regional

Tax Office so that the tax revenue target, especially in the material compliance supervision (PKM) sector, can be achieved. The next cause of tax revenue from digital forensic activities that is still not optimal is that the results of tax revenue from law enforcement activities, especially from the digital forensic sector, have not been specifically recorded/documented at the South Jakarta I Regional Tax Office, making it difficult to identify the exact amount of tax revenue from digital forensic activities. If the contribution of tax revenue from digital forensic activities can be better recorded and documented by the Digital Forensic Implementation Unit, it is expected to have an impact on the monitoring and evaluation process of digital forensic activities as well as better data accuracy and accountability. In addition, better recording and documentation of activities can also assist in the process of compiling the Digital Forensic Activity Results Report and optimizing the use of available resources.

The next reason related to the influence of digital forensic activities on tax revenue at the South Jakarta I Regional Tax Office is not yet optimal is that the Digital Forensic Implementation Unit has not been able to calculate the potential tax revenue by comparing law enforcement activities from the digital forensic process with law enforcement activities that are not/have not been supported by digital forensic activities. Therefore, the Digital Forensic Implementation Unit needs to make efforts such as obtaining adequate data and information to estimate the potential tax revenue that can be generated from digital forensic activities. For example, by calculating the potential amount of tax fines that have been successfully issued by Tax Assessment Letters or through the tax collection process thanks to the support of digital forensic activities.

Law enforcement activities, either through digital forensic activities or through other activities, can still be an alternative step in increasing tax revenue, although it is not the main step based on the ultimum remidium principle. In the process of tax law enforcement, there are subjective and objective requirements that must be met so that the amount of tax to be paid by the Taxpayer can be determined by the tax officer. The digital forensic process can be used to collect data and information related to the subject or object of tax so that the process of determining the actual amount of tax to be paid can be done more efficiently and accurately.

5 CONCLUSION

Based on the discussion that has been conducted, it was concluded that the process of implementing digital forensic activities in the context of taxation includes the process of obtaining electronic data, processing and analyzing electronic data, reporting digital forensic activities, storing electronic data, and evaluating digital forensic activities. Digital forensics for tax purposes carried out by the South Jakarta I Regional Office of the Directorate General of Taxes has been carried out based on the Circular Letter of the Director General of Taxes number SE-36/PJ/2017 with reference to three established international standards, namely ISO 270001, ISO 27002, and ISO 27005. The impact of digital forensic activities for tax purposes is to collect evidence that will be used in court and help uncover tax avoidance practices so that tax revenues can be optimized for the state. Proper implementation of digital forensic procedures can increase the efficiency and effectiveness of supervision by tax authorities. However, in the South Jakarta I Regional Tax Office, the influence of digital forensics on tax revenue has not been significant due to several things such as limited human resources, lack of documentation of tax revenue results from digital forensic activities, and the tax authorities have not been able to calculate the potential tax revenue from these activities. Tax law enforcement, including digital forensics, is still within the scope of alternative methods in increasing tax revenue due to the application of the ultimum remidium principle.

The obstacles and barriers faced in the implementation of digital forensic activities in the South Jakarta I Regional Tax Office arise from both internal and external sides. Internal obstacles include limited human resources in terms of number and capabilities related to digital forensics, the abilities and skills of digital forensic personnel that are not evenly distributed, the availability of supporting devices in carrying out tasks that are limited, and the duties and functions of employee positions that have not focused on the main performance indicators (IKU) of digital forensics. Meanwhile, external obstacles faced in the implementation of digital forensic procedures in the South Jakarta I Regional Tax Office include Taxpayers who are less cooperative in implementing digital forensic activities, Taxpayers losing data or electronic devices they own, and financial and tax information devices or systems owned by Taxpayers are more advanced than the equipment owned by digital forensic

personnel.

The Directorate General of Taxes needs to increase the quantity and quality of Digital Forensic Human Resources so that the law enforcement business process through digital forensic activities can run in accordance with applicable SOPs. Increasing quantity can be done through internal recruitment. While improving quality can be done by providing technical training related to digital forensics to Digital Forensic Personnel. The results of this study are limited to the South Jakarta I Regional Office of the Directorate General of Taxes, so it is hoped that further research can be expanded to other regional offices in Indonesia.

REFERENCE

Adekoya, A. A., Oyebamiji, T. A., & Lawal, A. B. (2020). Forensic accounting, tax fraud and tax evasion in Nigeria–Review of literatures and matter for policy consideration. *International Journal of Emerging Trends in Social Sciences*, 9(1), 21-28.

Agarwal, A., Gupta, M., Gupta, S., & Gupta, S. C. (2011). Systematic digital forensic investigation model. *International Journal of Computer Science and Security (IJCSS)*, 5(1), 118-131.

Al-Sharairi, M. E. (2018). The role of forensic accounting in limiting tax evasion in the Jordanian public industrial shareholding companies through the perspective of Jordanian auditors. *International Journal of Economics and Finance*, 10(1), 233-243.

Ami-Narh et al. (2008). Digital forensics and the legal system: A dilemma of our times. *Australian Digital Forensics Conference*.

Anam, M. K. (2022). *Eksistensi Perundang-Undangan Terhadap Digital Forensik Dalam Sistem Pembuktian Pidana*. Universitas Islam Indonesia.

Ante, S. (2013). Pembuktian Dan Putusan Pengadilan Dalam Acara Pidana. *Lex Crimen*, 2(2).

Asmarani, N. G. C. (27 Agustus 2021). *Pengembangan Teknologi Bidang Perpajakan Sudah Jadi Keharusan*. DDTC. https://news.ddtc.co.id/pengembangan-teknologi-bidang-perpajakan-sudah-jadi-keharusan-32343.

Astawan, I. K. T. (2022). Implementasi E-Filling System sebagai Pusat Penyimpanan Data Perusahaan Medi Groups berbasis Cloud dengan menggunakan Aplikasi Google One. *Jurnal Manajemen Sistem Informasi (JMASIF)*, 1(2), 41-51.

Dihni, V. A. (8 Mei 2022). Ini Tren Tax Ratio Indonesia dalam 5 Tahun Terakhir.Katadata.https://databoks.katadata.co.id/datapublish/2022/08/05/ini-tren-tax-ratio-indonesia-dalam-5-tahun-terakhir#:~:text=Menurut%20laporan%20Kementerian%20Keuangan%20(Kemenkeu,9%2C89%25%20terhadap%20PDB.

Direktorat Jenderal Pajak. (2022). Laporan Tahunan Kanwil DJP Jakarta Selatan I Tahun 2021. Direktorat Jenderal Pajak.

Direktorat Jenderal Pajak. (2022). Laporan Tahunan Direktorat Jenderal Pajak 2021. Direktorat Jenderal Pajak.

Faiz, M. N. et al. (2018). Studi Komparasi Investigasi Digital Forensik pada Tindak Kriminal. *Journal of Informatics Information System Software Engineering and Applications (INISTA)*, 1(1).

Febrian, F. (2019). Penerapan Data Extraction Analysis dalam Pemeriksaan Pajak dengan Power Query. *Seminar Nasional Aplikasi Teknologi Informasi (SNATI)*.

Harjowiryono, Marwanto. (2019). Analisis Faktor-Faktor yang Memengaruhi Kepatuhan Pajak Bendahara Pemerintah Dalam Penyetoran Pajak. *Indonesian Treasury Review*, 4(3), 195-217.

International Monetary Fund. (2019). *Technical Assistance Report-Ghana-Enhancing Domestic Revenue Mobilization-Improving Tax Compliance and Administration*. International Monetary Fund.

International Standard. (2013). *ISO/IEC 27002*. International Standard.

International Standard. (2013). *ISO/IEC 27005* Information technology – Security techniques – Information security risk management website https://ilmukomputer.org/wp-content/uploads/2013/04/Terjemahan-vasthu-ISO_IEC_27005-20081.pdf

Kartika, P. P. (2019). Data Elektronik Sebagai Alat Bukti Yang Sah Dalam Pembuktian Tindak Pidana Pencucian Uang. *Indonesian Journal of Criminal Law*, 1(1), 33-46.

Kementerian Keuangan. (2015). Peraturan Menteri Keuangan Republik Indonesia Nomor 184/PMK.03/2015 tentang Tata Cara Pemeriksaan. Jakarta: Sekretariat Negara.

Kementerian Keuangan. (23 Agustus 2022). *Bertemu Badan Anggaran DPR RI, Menkeu Sampaikan Laporan Realisasi Anggaran 2021*. Kementerian Keuangan Republik Indonesia website: https://www.kemenkeu.go.id/informasi-publik/publikasi/berita-utama/Bertemu-Badan-Anggaran-DPR-RI-Menkeu

Ley, B., Rijal, K.R., Marfurt, J. et al. (2019). Analysis of erroneous data

entries in paper based and electronic data collection. *BMC Res Notes*. 12, 537.

Parasram, S. V. (2020). *Digital Forensics with Kali Linux: Perform data acquisition, data recovery, network forensics, and malware analysis with Kali Linux 2019*. x. Packt Publishing Ltd.

Prawiranegara, I. N., & Kusuma, G. H. A. (2019). Analisa Digital Forensik Rekaman Video CCTV dengan Menggunakan Metadata dan Hash. *Prosiding SISFOTEK*, 3(1), 223 - 227.

Putra, A. F.. (2017). Pengaruh Etika, Sanksi Pajak, Modernisasi Sistem, dan Transparansi Pajak Terhadap Kepatuhan Pajak. *Jurnal Akuntansi Indonesia*, 6(1), 1-12.

Republik Indonesia. (2021). Undang-Undang Republik Indonesia Nomor 7 Tahun 2021 tentang Harmonisasi Peraturan Perpajakan

Riskiyadi, M. (2020). Investigasi Forensik Terhadap Bukti Digital Dalam Mengungkap Cybercrime. *Cyber Security dan Forensik Digital*, 3(2), 12-21.

Setiawan, T. P. (2019). *Kebijakan Bebas Visa Kunjungan (Bvk) Dalam Meningkatkan Sektor Ekonomi Pariwisata Di Indonesia*. Universitas Muhammadiyah Sumatera Utara.

Shavitri, L. P. D., & Darma, G. S. (2020). Pengaruh Implementasi Kebijakan Pemeriksaan dan Forensik Digital terhadap Kualitas Pemeriksaan dan Keberhasilan Penerimaan Pajak. *E-Jurnal Akuntansi*, 30(10), 2682-2697.

Situmorang, S. H., Muda, I., Doli, M., & Fadli, F. S. (2010). *Analisis data untuk riset manajemen dan bisnis*. USUpress.

Suryadi, T. L., & Subardjo, A. (2019). Pengaruh Kepatuhan Wajib Pajak, *Penagihan Pajak Dan Pemeriksaan Pajak Terhadap Penerimaan Pajak. Jurnal Ilmu dan Riset Akuntansi (JIRA)*, 8(4).