

Original Article

Use Of Digital Forensic Technology To Reveal The Identity Of Social Engineering Crimes

Bara Pratama Mahaputra^{1✉}, Chairul Muriman², Surya Nita³

^{1,2,3}School of Strategic and Global Studies, University of Indonesia

Correspondence Author: bara.pratama@ui.ac.id✉

Abstract:

The threat of social engineering attacks is highly evident in Indonesia. This is reflected in the IDADX report, which shows a significant increase in phishing attack complaints in Indonesia during the first quarter of 2023, with 26,675 reports, up from 6,106 reports in the fourth quarter of 2022. The highest number of attacks occurred in February with 15,050 cases. This also resulted in Indonesia being the 8th country with the highest number of data breach cases globally, with 820,000 cases in the second quarter of 2022, according to Surfshark. The purpose of this research is to analyze the utilization of digital forensic technology in collecting digital evidence to reveal the identities of social engineering crime perpetrators. The writing of this article uses a qualitative analysis method supported by digital forensic theory. The results of the discussion indicate that forensics focuses on the identification, collection, analysis, and preservation of digital evidence that can be used in legal proceedings. Digital forensics leverages computer technology and digital devices to uncover and secure information relevant to a crime. In social engineering crimes, which involve psychological manipulation to obtain information or certain access from victims, digital forensics plays a crucial role in identifying, collecting, analyzing, and preserving digital evidence that can reveal the identities of the perpetrators and their methods. Digital forensic technology is used to analyze emails, text messages, activity logs, and other digital traces left by the perpetrators.

Keywords: Utilization, Revelation, Identity, Digital Forensics, Social Engineering.



<https://jurnal.usk.ac.id/riwayat>

Introduction

Social engineering is a technique of social manipulation and psychological tricks to make targets help perpetrators in carrying out their attacks ([Jan-Willem H. Bull'ee et al., 2015](#)). This type of crime relies on manipulation techniques to take advantage of

human error, so that the victim's personal data can be accessed easily ([Nathanael Reuben et al., 2024](#)). [Cullen and Aritage \(2016\)](#) also revealed that this crime is carried out by tricking users into taking actions that are detrimental to their own security, by exploiting the victim's weaknesses, and is often considered the weakest point in the information system.

Although nothing new, technology has made social engineering attacks more effective due to the large number of data leaks or sensitive information that can be exploited by perpetrators ([Cullen and Aritage, 2016](#)). This type of attack is described as the art of manipulation, using deception or persuasion to obtain information that could have a negative impact ([Jan-Willem Bull'ee et al., 2016](#)). Meanwhile, [Kevin et al., \(2022\)](#) explained that this crime uses techniques and social mechanisms or human interactions carried out through persuasion, influence and other interactions to control the victim's actions, both consciously and unconsciously. Social engineering can be divided into two categories in the real world: human-based and technology-based. In human-based attacks, no technology is used and all operations are carried out through psychological manipulation or covert information gathering ([Shazny and Amrut, 2023](#)). [Jan-Willem H. Bull'ee et al., \(2015\)](#) also explained that this attack is often carried out by calling the target and asking for their password. Popular social engineering attacks include phishing, vishing, and smishing, as well as other modern types such as water holing, baiting, tailgating, which have their roots in phishing, vishing, and smishing ([Shazny and Amrut, 2023](#)).

This type of social engineering crime has a significant impact on individuals, organizations, and society at large. Individuals are vulnerable to attacks such as phishing which can result in theft of personal and financial information. Organizations, especially financial institutions, are often targets due to the risk of loss of confidential information and large financial losses. The impact is not only on the direct victims, but also on the organization's reputation and public trust. Economically, social engineering attacks can cause economic decline in society due to financial losses experienced by companies and individuals ([Muhammad et al., 2023](#)). According to [Oluwatosin et al., \(2023\)](#), social engineering attacks have far-reaching impacts, including financial losses, data breaches, reputation damage, psychological effects, and threats to national security. Individuals and organizations can suffer major financial losses from identity theft, false billing, and fraud such as Business Email Compromise (BEC). Attackers can misuse the sensitive information obtained, causing privacy risks, legal consequences, and financial penalties. An organization's reputation can be damaged, resulting in a decline in customers, market share, and brand value that is difficult to recover from. Individual victims can experience emotional stress, loss of trust, and long-term psychological impacts. Social engineering attacks can also threaten critical infrastructure and disrupt national security.

The threat of social engineering attacks is also felt in Indonesia. This can be seen from the IDADX report which shows a significant increase in complaints about phishing attacks in Indonesia in the first quarter of 2023 with 26,675 reports, up from 6,106 reports in the fourth quarter of 2022. The most attacks occurred in February with 15,050 cases. The .id domain was the main target with 26,485 reports. This also caused Indonesia to become the 8th country with the highest number of data leak cases globally, with 820 thousand cases in the second quarter of 2022 according to Surfshark. Data leaks in Indonesia rose 143% from the first quarter of 2022 and since 2004, they have reached 120.9 million reports. In the second quarter of 2022, there was an increase of 450 accounts hacked per minute. The threat of social engineering also occurs in the jurisdiction of the

South Kalimantan Regional Police, with reports of 350 victims of fake ticket fraud as of September 2023 ([Frans Rumbon, 2023](#)). At the Banjar Police Station itself, similar cases were reported, including cases of online fraudulent investment fraud. The resolution of this case was directed to the South Kalimantan Regional Police because of its complexity, involving many victims from various regions and a wide network of perpetrators. Banjar Police has limited resources, expertise and facilities needed to handle this complex case, which requires access to digital forensic technology to collect and analyze complex and scattered electronic evidence for deeper investigations, better coordination and more effective use of resources to resolve cases fairly and transparently.

From the facts above, it can be understood that social engineering is a highly manipulative crime method, exploiting the victim's beliefs and psychological weaknesses to gain certain information or access. The main challenge in identifying social engineering perpetrators is that the nature of this crime does not leave physical traces, making it difficult to trace using traditional methods. Perpetrators often use false identities, software to hide their location, and other techniques that obscure their digital footprints, so investigations often stall due to a lack of physical evidence pointing directly to the perpetrator. At the Banjar Police, investigations into social engineering cases such as online fraudulent investment fraud often face obstacles in the application of digital forensic technology. Some technical and practical obstacles include infrastructure limitations such as sophisticated forensic hardware and software, as well as a lack of human resources skilled in digital forensics, considering that this technology requires special training and a deep understanding of digital data analysis. The high cost of acquiring and maintaining this technology is also a significant obstacle for the Banjar Police.

Obstacles in investigating social engineering cases are also exacerbated by the development of new and increasingly complex crime modes, where perpetrators are always looking for new opportunities to exploit victims. On the other hand, current digital forensic investigation methods have not been balanced with the creation of new standard operating procedures (SOP) to keep up with the speed of development of this type of crime mode, so investigators do not have adequate guidance to handle these cases effectively. The use of digital forensic technology also raises ethical issues that need to be considered, one of which is individual privacy. In attempting to collect digital evidence, there is a risk that irrelevant personal data will also be exposed, causing serious privacy violations, especially if the data collected involves sensitive information that is not directly related to the case under investigation. Investigators must exercise extreme caution in handling this personal data to ensure that individuals' rights remain protected.

In addition, there is the potential for misuse of technology by irresponsible parties for illegal purposes, such as spying on certain individuals or groups without a clear legal basis, which can give rise to serious problems related to abuse of power and human rights violations. The use of digital forensic technology also faces challenges from the lack of strict supervision and adequate regulation to accommodate growing needs in the future, especially with the enactment of the new Personal Data Protection Law which will be implemented in October 2024 ([Lubna et al., 2023](#)). Investigations using digital forensics must also face a growing phenomenon in Indonesian society today, where many people proudly share their personal information with the public. They often do not realize that posting their activities and identity can trigger problems if the information is misused by irresponsible parties (Lina, 2022). Although digital forensics involves the analysis of digital traces and has become an integral part of law enforcement in the digital era (Amsori

et al., 2024), this trend presents additional challenges. The large and scattered volume of data complicates the filtering and analysis process to find information relevant to the case, as well as ensuring its validity for use in court ([Telsy and Chelsia, 2020](#)).

The fact that people tend to share information openly also raises ethical issues in investigations. Investigators should be careful to ensure that they do not violate the privacy of individuals unrelated to the investigation even if the information is publicly available, by setting clear limits on how information from social media can be used in legal proceedings. In the investigation process using digital forensics, another challenge arises from the aspect of network-based evidence. These challenges can be seen from the stages of acquisition, content, storage, privacy, appropriation, and reception. Networks have many potential sources of evidence such as wireless access points and central log servers, making it difficult to find the right evidence. Even if the location of evidence is known, access is hindered by political, location, or technical issues. The problem of limited content is also an obstacle, because network devices often only store selected metadata and have limited storage capacity, so they do not record complete data that passes through the network. Non-persistent storage on network devices means data is easily lost if the device is reset. Another challenge stems from legal issues related to personal privacy in network-based acquisition techniques, depending on the applicable jurisdiction ([Imam and Ade, 2020](#)).

Looking at the various challenges in investigating social engineering crime cases, especially those involving digital forensic technology, it is clear that the current approach still has many shortcomings. Difficulty in identifying perpetrators, limited infrastructure, inadequate human resources, and high costs are some of the main obstacles. The rapid development of new types of crime requires the creation of more adaptive standard operating procedures (SOP). Ethical issues such as privacy violations and potential misuse of technology cannot be ignored either. The phenomenon of people tending to share personal information openly adds to the complexity of investigations. To overcome all this, in-depth and comprehensive research is needed to provide a detailed understanding of the various aspects of social engineering crimes and the challenges in investigating them. A comprehensive approach is needed to combine various disciplines such as information technology, law, psychology and ethics, so as to create holistic and sustainable solutions. Real case studies need to be conducted to analyze the various methods used by social engineering perpetrators and how they succeed in deceiving victims. By understanding the modus operandi of perpetrators, investigators can develop more effective strategies to identify and apprehend them through the various digital forensic technologies available, assess their effectiveness, and identify gaps or limitations that need to be addressed. In accordance with the explanation above, the title chosen in this research to answer this need is "The Use Of Digital Forensic Technology To Reveal The Identity Of Social Engineering Crimes". This research aims to analyze how digital forensic technology is used in collecting digital evidence to reveal the identity of social engineering crime perpetrators.

Digital forensic theory is the use of analytical and investigative techniques to identify, collect, examine and store evidence or information contained in computers or digital storage media. The aim is to present valid evidence in criminal cases ([Saputra et al., 2017](#)). This definition describes the application of information science and technology in the process of legal evidence, especially to uncover crimes involving computer devices, with the aim of obtaining digital evidence that can be used to ensnare criminals ([Kiswanto, 2014](#)). This mechanism can be applied to the Chain of Custody, namely the process of recording the chronological sequence of security, storage, supervision and movement of

evidence, both physical and electronic ([Charles and Pollock, 2015](#)). Chain of Custody documents provide details regarding the history of handling of evidence, ensuring its accuracy and integrity during the court process. The basic principle of Chain of Custody is to ensure that evidence is truly related to a crime, not fake evidence placed to ensnare someone. Authorities are required to maintain access, documentation and submission of evidence to responsible officials. The Chain of Custody document, even though the format is not standard, must include: 1) Details of the evidence collected; 2) Identity of all parties responsible for the evidence; 3) Duration of storage of evidence; 4) Any transfer of evidence (including signatures of the parties involved). From this explanation, it can be seen that digital forensics is used to collect, analyze and interpret electronic data, involving forensic principles that apply to digital evidence to find relevant information regarding the identity of the perpetrator of the crime.

Methods

This study is qualitative in nature. [Creswell \(2019\)](#) states that it entails crucial actions such developing protocols and questions, gathering information from participants, doing inductive analysis of the data to move from particular to broad themes, and deriving conclusions from the data. Put differently, qualitative research methodologies seek to provide a deeper understanding of a phenomenon by gathering extensive data. The author intends to utilize a qualitative descriptive methodology. In order to comprehend the features, context, and significance of a phenomenon—such as behavior, attitudes, or experiences—this method places a strong emphasis on providing a detailed description of the phenomenon without depending on data or statistics ([Moelong, 2008](#)). This indicates that in order to comprehend the subject matter being written about more thoroughly, information is gathered by direct engagement, observation, or text evaluation and then narratively evaluated. The focus of this research is the use of digital forensic technology in collecting digital evidence to reveal the identity of social engineering crime perpetrators using digital forensic theory.

Results

Digital forensics is a branch of forensic science that focuses on the identification, collection, analysis and storage of digital evidence that can be used in legal proceedings. This field utilizes computer technology and digital devices to reveal and secure information relevant to a crime. Digital forensics is the process of applying legitimate investigative and analytical techniques to identify, collect, examine, and preserve digital evidence. The main goal is to present evidence that is admissible in court in a criminal or civil case. This digital evidence can be data contained on a computer, mobile device, network, or other storage media.

Social engineering is a technique used by attackers to manipulate individuals into disclosing confidential information or performing actions that benefit the attacker. This technique often exploits trust, fear, greed, or urgency to achieve its goals. Types of Social Engineering Crimes are: 1) Phishing, fraud via emails or messages that appear official, asking recipients to reveal personal information or click on malicious links; 2) Vishing (Voice Phishing), fraud via telephone calls impersonating authorities to trick victims into providing sensitive information; 3) Smishing (SMS Phishing), fraud via text messages that tries to trick victims into clicking on links or providing personal information; 4) Baiting, fraud that offers something attractive to lure victims into disclosing personal information

or inserting malware into their system; 5) Pretexting, the attacker creates a fake scenario (pretext) to get information from the victim, such as pretending to be a friend or co-worker; 6) Tailgating, an attacker takes advantage of someone to gain physical access to a safe place by following them closely.

The impact of social engineering crimes is that individuals can lose personal information, identity theft and financial losses. Organizations can suffer the loss of confidential data, significant financial loss, and reputational damage. Decreased trust in institutions, negative economic impacts, and threats to national security. Social engineering crimes utilize psychological manipulation to obtain certain information or access from victims. Digital forensics plays an important role in identifying, collecting, analyzing and storing digital evidence that can reveal the identity of perpetrators and the methods they use. This process involves various techniques and stages designed to maintain the integrity of evidence and ensure that the results of the investigation can be accounted for in court. Digital forensics also helps in developing more effective prevention strategies against future social engineering crimes. The use of digital forensic technology to reveal the identity of perpetrators of social engineering crimes is the use of digital forensic techniques and tools to identify individuals or groups who commit social engineering crimes. Social engineering is a method used by criminals to manipulate people into providing personal information or taking actions that benefit the perpetrator. Digital forensic technology can be used to analyze emails, text messages, activity logs and other digital traces left by perpetrators. Use network analysis tools to trace the source of communications or attacks. Uses collected data to build profiles of perpetrators based on their behavioral patterns and digital footprints. The benefits of digital forensics include speeding up the process of identifying perpetrators and collecting evidence, increasing accuracy and accuracy in revealing the perpetrator's identity, and helping to prevent future social engineering crimes by identifying the techniques and methods used by perpetrators.

Digital forensic technology plays an important role in collecting digital evidence to reveal the identity of perpetrators of social engineering crimes through several methods, including:

1. Digital Evidence Acquisition

Digital devices, digital forensic investigators can use a variety of methods to acquire digital evidence from digital devices such as computers, smartphones, and tablets, including:

- a) Forensic imaging, creating a complete copy of a hard drive or other storage device to ensure data integrity.
- b) Data extraction, retrieving certain data from the device, such as email files, text messages, and web browsing history.
- c) Memory retrieval, captures the current contents of the device's memory, which may contain important information about the perpetrator's activities.
- d) Networks, digital evidence can also be collected from networks, including:
- e) Network logs, collecting data about users' online activities, such as IP addresses accessed and websites visited.
- f) Network traffic analysis, monitoring network traffic to identify suspicious activity, such as unusual data transfers.

2. Digital Evidence Analysis

Once digital evidence is collected, digital forensic investigators will analyze it to look for information that can help identify the perpetrators of social engineering

crimes. This analysis may include:

- a) Keyword search, looking for keywords that are relevant to the crime, such as the victim's name, financial information, or keywords related to the social engineering technique used.
- b) Metadata analysis, analyzing digital file metadata, such as date and time of creation, to find out the origin of the file and who has accessed it.
- c) Event reconstruction, reconstructing the sequence of events that occurred during the crime to identify the perpetrators and determine how they committed the crime.

3. Digital Evidence Recovery

Sometimes, social engineering criminals try to delete digital evidence from their devices. However, digital forensics investigators can use special techniques to recover deleted data, such as:

- a) Deleted data recovery, using special software to recover files that have been deleted from a hard drive or other storage device.
- b) Steganographic forensic analysis, uncovering hidden messages that have been hidden in image or audio files.

4. Digital Evidence Preservation

Digital evidence must be stored properly to ensure its integrity and to prevent damage or loss. Digital forensic investigators follow strict protocols for the preservation of digital evidence, including:

- a) Create a chain of custody, documenting who has access to digital evidence and when they access it.
- b) Store digital evidence in a safe place, store digital evidence in a safe and controlled place to prevent unauthorized access.
- c) Make copies of digital evidence, make copies of digital evidence for investigative purposes and in case the original evidence is damaged or lost

For example, in a phishing case, a perpetrator sends a fake email that appears to come from a bank to many victims. With this method, digital forensic technology helps to reveal the identity of the perpetrator of a social engineering crime in an efficient and legal manner, ensuring that the evidence collected can be used in court. Digital forensic technology in this case will be used to:

- a) Analyze emails, search email headers to find the originating IP address.
- b) IP Tracing, traces an IP address to a specific geographic location.
- c) Examining Device, if the perpetrator's device is accessible, creates an image of the device to analyze files and network activity.
- d) Connecting Dots, connecting data from email, activity logs, and metadata to identify perpetrators.

The example above shows that the use of digital forensic technology is very important in collecting digital evidence to reveal the identity of the perpetrator of a social engineering crime. By using digital forensic techniques, investigators can collect, analyze, and preserve digital evidence that can help them identify perpetrators and bring them to justice.

Conclusion

Digital forensics is a branch of forensic science that focuses on the identification,

collection, analysis and storage of digital evidence that can be used in legal proceedings. Digital forensics utilizes computer technology and digital devices to reveal and secure information relevant to a crime. In social engineering crimes, which involve psychological manipulation to obtain certain information or access from victims, digital forensics plays an important role in identifying, collecting, analyzing and storing digital evidence that can reveal the identity of the perpetrator and the methods they used. Digital forensic technology is used to analyze emails, text messages, activity logs, and other digital traces left by perpetrators. In this way, digital forensics helps speed up the process of identifying perpetrators, increasing accuracy in uncovering their identities, and developing more effective prevention strategies against future social engineering crimes.

Suggestion

To deal with and prevent social engineering crimes and utilize digital forensics effectively, several suggestions can be made: 1) Conduct regular training to increase awareness about social engineering techniques, such as phishing, vishing, and smishing. Simulate a social engineering attack to test employee readiness and response and increase awareness of the threat; 2) Use the latest security software, including advanced antivirus, firewall and threat detection solutions. Implement two-factor authentication for all critical system access to improve security; 3) Establish strict verification procedures before providing sensitive information or access to the system. Implement a strong password policy and require regular password changes; 4) Train security teams in digital forensics techniques to ensure they can properly identify and collect digital evidence. Invest in sophisticated digital forensics tools to analyze and recover data that has been deleted or hidden by the perpetrator; 5) Establish a trained incident response team to respond to social engineering attacks and carry out forensic investigations quickly. Prepare a recovery plan that includes steps to mitigate the impact of the attack and restore affected systems; 6) Establish cooperation with law enforcement and related institutions to share the latest information and techniques in overcoming social engineering crimes. Participate in cybersecurity forums and communities to share information about the latest threats and mitigation strategies; 7) Conduct regular security audits to evaluate the effectiveness of implemented security policies and technology. Always update security policies and the technology used to keep pace with the development of new threats.

References

- Agung Purnama Saputra, Husni Mubarak, Nur Widiyasono. (2017). Analisis Digital Forensik pada File Steganography (Studi Kasus: Peredaran Narkoba). *Jurnal Teknik Informatika dan Sistem Informasi*, Volume 3 Nomor1 April 2017.
- Amsori, dkk. (2024). Tantangan dan Peran Digital Forensik dalam Penegakan Hukum terhadap Kejahatan di Ranah Digital. *Journal Humaniora: Jurnal Hukum dan Ilmu Sosial*. Volume 02, No.01, Januari 2024, pp.14-19.
- Anonim. (2023). Serangan *Phishing* di Indonesia Terus Meningkat, Berikut Data Lengkap. Sumber: <https://bankjombang.co.id/serangan-phishing-di-indonesia-terus-meningkat-berikut-data-lengkap/>, diakses 25 Juni 2024, Pukul 12.08 WIB.
- Conteh N. Y. dan Schmick P.J. (2016). Cybersecurity: Risks, Vulnerabilities and Countermeasures to Prevent Social Engineering Attacks. *International Journal Of Advanced Computer Research*, 1(31–38).
- Creswell, J. W. (2019). *Research Design Pendekatan Metode Kualitatif, Kuantitatif, dan Metode Campuran*. Pustaka Pelajar.
- Diardo Luckandi. (2019). Analisis Transaksi Pembayaran Menggunakan Fintech pada

- UMKM di Indonesia: Pendekatan Adaptive Structuration Theory. *Jurnal Informatika dan Komputer (JIKO)* – Volume 4, Nomor 1, Februari 2019.
- Frans Rumbon. (2023). Penipu Kirim Surat Tilang Palsu, 350 Korban Kejahatan Siber Laporkan ke Polda Kalsel. Sumber: <https://banjarmasin.tribunnews.com/2023/09/05/penipu-kirim-surat-tilang-palsu-350-korban-kejahatan-siber-laporan-ke-polda-kalsel>, diakses 25 Juni 2024 Pukul 12.13 WIB.
- Imam Riadi dan Ade Kurniawan. (2020). *Forensik Jaringan dan Cloud*. Yogyakarta: Diandra Kreatif (Kelompok Penerbit Diandra).
- Jan-Willem H. Bull'ee, dkk. (2015). The persuasion and security awareness experiment: reducing the success of social engineering attacks. *J Exp Criminol*. Springer Science Business Media Dordrecht 2015.
- Jan-Willem H. Bull'ee, dkk. (2016). Telephone-based social engineering attacks: An experiment testing the success and time decay of an intervention. *Proceedings of the Singapore Cyber-Security Conference (SG-CRC) 2016*.
- Kevin Tjendrawinata, dkk. (2022). Social Engineering: Crisis in Humanity Pengertian, Mekanisme, Serta Studi Kasus Di Indonesia 2021. *Jurnal Teknik Informatika dan Sistem Informasi*, Vol. 9, No. 3, September 2022, Hal. 2085-2095.
- Kiswanto. (2014). Prosedur Penanganan Bukti Digital. Sumber: https://www.academia.edu/10690256/Prosedur_penanganan_bukti_digital, diakses 25 Juni 2024, Pukul 11.41 WIB.
- Lina Miftahul Jannah. (2022). Undang-Undang Perlindungan Data Pribadi dan Tantangan Implementasinya. Sumber: https://fia-ui-ac-id.translate.google/en/uu-perlindungan-data-pribadi-dan-tantangan-implementasinya/?_x_tr_sl=en&_x_tr_tl=id&_x_tr_hl=id&_x_tr_pto=wapp, diakses 18 Mei 2024, Pukul 13.28 WIB.
- Lubna Luxmi Dhirani, dkk. (2023). Dilemmas and Privacy Issues in Emerging Technologies: A Review. *Sensors* 2023, 23, 1151.
- M. Nur Faiz, R. Umar, and A. Yudhana. (2017). Implementasi Live Forensics untuk Perbandingan Browser pada Keamanan Email. *J. Inform. Sunan Kalijaga*, vol. 1, no. 3, pp. 108–114, 2017.
- Moelong, L. J. (2008). *Metodologi Penelitian Kualitatif*. PT. Remaja Rosdakarya.
- Muhamad Baihaqi Mohd Azhar, dkk. (2023). Social Engineering and Cyber Threats: Exploring Techniques, Impacts and Strategies. *International Journal of Accounting, Finance and Business (IJAFB)*, Volume: 8 Issues: 50 [September, 2023] pp. 13 – 25.
- Muhammad Hasan, dkk. (2022). *Metode Penelitian Kualitatif*. Makassar: Tahta Media Group.
- Nathanael Reuben, dkk. (2024). Raising Cyber Security Awareness to Reduce Social Engineering through Social Media in Indonesia. *Article*. Binus University.
- Oluwatosin Adeniji, dkk. (2023). Analysing Social Engineering Attacks and its Impact. *IEEE*.
- Shazny Ahmed Hussain Nismy dan Amrut Mahesh Kajave. (2023). How Cyber Criminal Use Social Engineering to Target Organizations. *IEEE*.
- T. Charles and M. Pollock. (2015). Digital forensic investigations at universities in South Africa. in *2015 Second International Conference on Information Security and Cyber Forensics (InfoSec)*, 2015, pp. 53–58.
- Telsy Aldemadra Nomorissa dan Chelsia Suryadithya. (2020). Forensic Data Analytics dalam Mendeteksi Fraud. *Prosiding ASIC 2020 Volume 1. No. 1, Tahun 2020*.