

Korespondensi

International Journal of Cyber Criminology (IJCC)

Journal: International Journal of Cyber Criminology (IJCC)

Link: <https://cybercrimejournal.com/>

Scopus: <https://www.scopus.com/sourceid/21100218074>

Scimago: <https://www.scimagojr.com/journalsearch.php?q=21100218074&tip=sid&exact=no>

ISSN: 0974-2891

CiteScore: 2.1

SNIP: 1.168

H Index: 20

SJR: 0.230

Quartile: Q2

Scope: Social Sciences: Law

Author(s): Ahmad Syaafi, Mursidah, Aurora Fatimatuz Zahra, Fatham Mubina Iksir Gholi

Article Title: Employing Forensic Techniques in Proving and Prosecuting Cross-border
Cyber-financial Crimes

Corresponding author: Ahmad Syaafi

Volume: 17

Number: 1

Year: 2023

Submission: 23 August 2022

Peer Review Process 1: 27 September – 22 November 2022

Peer Review Process 2: 22 November 2022 – 10 February 2023

Acceptance: 23 Maret 2023

Published online: 1 April 2023

Link: <https://cybercrimejournal.com/menuscript/index.php/cybercrimejournal/article/view/139/>

Link PDF: <https://cybercrimejournal.com/menuscript/index.php/cybercrimejournal/article/view/139/51>

0. Journal Profile

IJCC is an

MULTIDISCIPLINARY FIELD THAT ENCOMPASSES

Researchers from various fields such as Criminology, Victimology, Sociology, Internet Science

MAKE SUBMISSION

Jan-June 2023 **NEW**

Vol 17 Issue 1

Articles

Identifying the Prevalence of Cybercrime in Indonesian Corporations: A Corporate Legislation Perspective

Djoni Sunardi Gojak

Evaluating Legal Frameworks for Cybercrime in Indonesian Public Administration: An Interdisciplinary Approach

Ikhwan Anwarly

Towards a Legal Framework for Civil Liability of Smart Robots in Jordanian Legislation

Dr. Hassan Sami Alabady

Cyber Security Challenges Faced by Employees in the Digital Workplace of Saudi Arabia's Digital Nature Organization

Dr. Vinata Venugopal Muthuswamy

Role of Cyber Security on Employees' Digital Workplace Performance: Exploring the Effects of Employees' Digital Awareness and Organizational Support

Associate Prof. Dr. Vinata Venugopal Muthuswamy, Professor Dr. N. Nithya

Employing Forensic Techniques in Proving and Prosecuting Cross-border Cyber-financial Crimes

Ahmad Syaifi, Mursidah, Aurora Fatimatuz Zahra, Fatham Mubina Risa Ghidi

Login

Register

2.3

2019 CiteScore

Q1 quartile

Powered by Scopus

International Journal of Cyber Criminology



This title
is indexed
in Scopus
Scopus

Improving research
results through
analytical power



ABOUT THE JOURNAL

What is Cyber Criminology? Who is the Founding Father? Who coined the term?

Cyber Criminology is a multidisciplinary field that encompasses researchers from various fields such as Criminology, Victimology, Sociology, Internet Science, and Computer Science. Jaishankar (2007) is the Founding Father of the academic discipline Cyber Criminology and he coined and defined Cyber Criminology as "the study of causation of crimes that occur in the cyberspace and its impact in the physical space". Jaishankar (2007) academically coined the term Cyber Criminology for two reasons. First, the body of knowledge that deals with cyber crimes should not be confused with investigation and be merged with cyber forensics; second, there should be an independent discipline to study and explore cyber crimes from a social science perspective. Since the launch of the International Journal of Cyber Criminology, the term Cyber Criminology has taken its academic roots in the online as well as offline academic circles.

Quick Links

- About the Journal
- Editorial Board
- Editorial Advisory Board
- Open Access
- Abstracting and Indexing
- Publication Ethics
- Commons License
- Submission
- Announcements
- Review Process
- Copyright

Scopus Preview

Author Search Sources

Source details

International Journal of Cyber Criminology

Scopus coverage years: from 2012 to 2021

Publisher: K. Jaishankar

ISSN: 0974-2891

Subject area: Social Sciences (Law)

Source type: Journal

Year	CiteScore
October 2021	2.2
SJR 2021	0.284
SNIP 2021	1.036

CiteScore CiteScore rank & trend Scopus content coverage



Source details

International Journal of Cyber Criminology

Scopus coverage years: from 2012 to 2022

Publisher: K. Jaishankar

ISSN: 0974-2891

Subject area: Social Sciences: Law

Source type: Journal

[View all documents >](#)

[Set document alert](#)

[Save to source list](#)

CiteScore 2022
2.1

SJR 2022
0.230

SNIP 2022
1.168

[CiteScore](#) [CiteScore rank & trend](#) [Scopus content coverage](#)

i Improved CiteScore methodology

CiteScore 2022 counts the citations received in 2019-2022 to articles, reviews, conference papers, book chapters and data papers published in 2019-2022, and divides this by the number of publications published in 2019-2022. [Learn more >](#)

CiteScore 2022 ⌵

$$2.1 = \frac{193 \text{ Citations 2019 - 2022}}{92 \text{ Documents 2019 - 2022}}$$

Calculated on 05 May, 2023

CiteScoreTracker 2023 ⓘ

$$2.1 = \frac{145 \text{ Citations to date}}{69 \text{ Documents to date}}$$

Last updated on 07 June, 2023 • Updated monthly

CiteScore rank 2022 ⓘ

Category	Rank	Percentile
Social Sciences		
Law	#196/885	77th

[View CiteScore methodology >](#) [CiteScore FAQ >](#) [Add CiteScore to your site](#)

About Scopus

[What is Scopus](#)

[Content coverage](#)

[Scopus blog](#)

[Scopus API](#)

[Privacy matters](#)

Language

[日本語版を表示する](#)

[查看简体中文版本](#)

[查看繁體中文版本](#)

[Просмотр версии на русском языке](#)

Customer Service

[Help](#)

[Tutorials](#)

[Contact us](#)

ELSEVIER

[Terms and conditions](#) ↗ [Privacy policy](#) ↗

Copyright © Elsevier B.V. ↗. All rights reserved. Scopus® is a registered trademark of Elsevier B.V.

We use cookies to help provide and enhance our service and tailor content. By continuing, you agree to the use of cookies ↗.



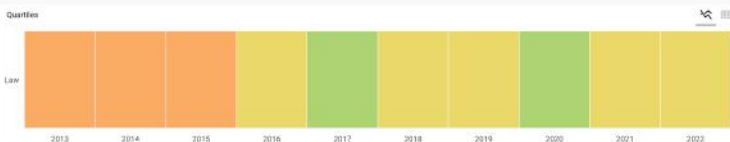
International Journal of Cyber Criminology

COUNTRY	SUBJECT AREA AND CATEGORY	PUBLISHER	H-INDEX
India	Social Sciences — Law		20
Universities and research institutions in India Media Ranking in India			
PUBLICATION TYPE	ISSN	COVERAGE	INFORMATION
Journals	09742891	2012-2021	Homepage How to publish in this journal cybercrimejournal@gmail.com

SCOPE

International Journal of Cyber Criminology (IJCC) is a peer reviewed online (open access) interdisciplinary journal published biannually and devoted to the study of cyber crime, cyber criminal behavior, cyber victims, cyber laws and cyber policy. IJCC is a unique Diamond open access, not for profit international journal, where the author(s) need not pay article processing charges / page charges and it is totally free for both the authors and the audience. IJCC will focus on all aspects of cyber/computer crime: Forms of Cyber Crime, Impact of cyber crimes in the real world, Policing Cyber space, International Perspectives of Cyber Crime, Developing cyber safety policy, Cyber Victims, Cyber Psychopathology, Geographical aspects of Cyber crime, Cyber offender behavior, cyber crime law, Cyber Pornography, Privacy & Anonymity on the Net, Internet Fraud and Identity Theft, Mobile Phone Safety, Human Factor of Cyber Crime and Cyber Security and Policy issues, Online Gambling, Copyright and Intellectual property Law. As the discipline of Cyber Criminology approaches the future, facing the dire need to document the literature in this rapidly changing area has become more important than ever before. The IJCC will be a nodal centre to develop and disseminate the knowledge of cyber crimes primarily from a social science perspective to the academic and lay world. The journal publishes theoretical, methodological, and applied papers, as well as book reviews. We do not publish highly technical cyber forensics / digital forensics papers and papers of descriptive / overview nature.

Join the conversation about this journal



FIND SIMILAR JOURNALS



International Journal of Cyber Criminology

Q2 Law

SJR 2021 0.23

powered by scimago.com

Show this widget in your own website

Just copy the code below and paste within your html code:

<https://www.scimago.com>

SCImago Graphica

Explore, visually communicate and make sense of data with our new data visualization tool.

Metrics based on Scopus® data as of April 2023

Developed by: SCImago
 Powered by: Scopus

Follow us on @ScimagoJR

Scimago Lab. Copyright 2007-2022. Data Source: Scopus®

EST MODUS IN REBUS

1992-2022

Cookie settings

Cookie policy

1. Submission



Ahmad Syaafi <asyaafi.fh.unlam@gmail.com>

[IJCC] Submission Acknowledgement

Editor IJCC <Editor@cybercrimejournal.com>

23 Agustus 2022 pukul 14.58

Kepada: Ahmad Syaafi <asyaafi.fh.unlam@gmail.com>

Dear Syaafi,

Thank you for submitting the manuscript, "Employing Forensic Techniques in Proving and Prosecuting Cross-border Cyber-financial Crimes" to International Journal of Cyber Criminology. With the online journal management system that we are using, you will be able to track its progress through the editorial process by logging in to the journal web site:

Submission URL:

<https://cybercrimejournal.com/menuscript/index.php/cybercrimejournal/authorDashboard/submission/136>

Username: asyaafi

If you have any questions, please contact me.

Thank you for considering this journal as a venue for your work.

Best regards,

International Journal of Cyber Criminology

<https://www.cybercrimejournal.com/>



Ahmad Syaufi <asyaufi.fh.unlam@gmail.com>

[IJCC] Decision - Send to review

Editor IJCC <Editor@cybercrimejournal.com>

27 September 2022 pukul 23.18

Kepada: Ahmad Syaufi <asyaufi.fh.unlam@gmail.com>

Dear Syaufi,

We have reached a decision regarding your submission to International Journal of Cyber Criminology, "Employing Forensic Techniques in Proving and Prosecuting Cross-border Cyber-financial Crimes".

Our decision is to: Send to review

Submission URL:

<https://cybercrimejournal.com/menuscrypt/index.php/cybercrimejournal/authorDashboard/submission/136>

Username: asyaufi

If you have any questions, please contact me.

Thank you for considering this journal as a venue for your work.

Best regards,

International Journal of Cyber Criminology

<https://www.cybercrimejournal.com/>

Employing Forensic Techniques in Proving and Prosecuting Cross-border Cyber-financial Crimes

Ahmad Syaufi

Faculty of Law, Universitas Lambung Mangkurat, Indonesia

Mursidah

SMAN 8 Banjarmasin, Indonesia

Aurora Fatimatuz Zahra

Faculty of Law, Universitas Muhammadiyah Yogyakarta, Indonesia

Fatham Mubina Iksir Gholi

Faculty of Law, Universitas Diponegoro, Indonesia

Abstract

Cyber-financial crimes across borders pose a big challenge to law enforcement, particularly in developing countries like Indonesia. They affect the economy, society and the financial sector, thus forensic techniques are essential in their investigation and prosecution. This study aims to explore the significance of forensic techniques in prosecuting cross-border cyber-financial crimes in Indonesia, discussing the legal basis for digital forensic investigations, the police's role, and the challenges they face. This study shows that forensic techniques are crucial for tackling cyber-financial crimes across borders in Indonesia. Law enforcement must have a legal grounding and expertise in digital forensic investigations, from collecting to presenting evidence in court. However, there are challenges such as insufficient resources, training, and cooperation between countries that law enforcers face. This study emphasizes the significance of using forensic techniques to address cross-border cyber-financial crimes in Indonesia.

Keywords: Forensic Techniques, Financial Crimes,

I. INTRODUCTION

In recent years, cyber-financial crimes across borders have become a significant challenge for law enforcement agencies worldwide, including in developing countries such as Indonesia (Mauladi, Laut Merta Jaya, & Esquivias, 2022; Mentari & Hudi, 2022). These crimes not only impact the financial sector but also have adverse effects on the economy and society as a whole. Forensic techniques have proven to be essential in the investigation and prosecution of these types of crimes.

The law plays a vital role in investigating and prosecuting cross-border cyber-financial crimes. In Indonesia, the legal basis for conducting digital forensic investigations is provided by Law No. 19 of 2016 on Electronic Information and Transactions (ITE Law). This law provides the legal framework for the collection and presentation of digital evidence in court. It also establishes the responsibilities and obligations of law enforcement agencies in investigating cyber-crimes.

Evidently, there is an immediate requirement for advanced forensic methodologies when confronting cyber-financial crimes transferred across borders but particularly so among countries such as Indonesia, struggling to overcome this challenge. The present research concentrates on revealing how significant forensic techniques are when prosecuting instances arising from cross-border cyber-financial crime within Indonesia.

From examining our investigations findings, it remains evident that leveraging forensics proficiency becomes crucial towards overcoming the numerous challenges faced by law enforcers in charge of these complex cases. As we strive to make progress against cross-border cyber-criminal activity tarnishing our institutions' reputation and harming financial interests, both legal restrictions and digital forensics capabilities are essential standards we must strive towards. Without stakeholders cooperating closely enough to develop robust strategies aimed at prevention efforts while investigating and tracking down those responsible until their prosecution becomes possible could be far-fetched. Therefore, this study aims to explore the significance of forensic techniques in prosecuting cross-border cyber-financial crimes in Indonesia, discussing the legal

basis for digital forensic investigations, the role of the police, and the challenges they face.

II. LITERATURE REVIEW

Forensic Techniques in Cybercrime Investigations

The investigation and prosecution of cybercrime have become increasingly complex due to the rise of technology and the use of the internet for criminal activities. Forensic techniques have been developed specifically for cybercrime investigations to collect and analyze digital evidence effectively. This literature review will examine relevant studies that provide an overview of the forensic techniques used in cybercrime investigations.

The collection of digital data is a crucial component of cybercrime investigations. A forensic investigation of electronic evidence requires the collection, preservation, analysis, and presentation of data. It is imperative that forensic investigators handle the data in a manner that does not unnecessarily alter or destroy evidence. Devices that generally store digital data, such as hard disk drives and flash drives, are classified as non-volatile memory and therefore are regularly selected as primary targets for data collection. A forensic investigation expert or appropriate agency should be used in all digital forensic investigations.

In the cybercrime investigation, various forensic techniques are employed to analyze the digital data collected. Data validation is a crucial forensic technique used to ensure the accuracy and completeness of digital evidence. The process of data validation entails confirming the precision and entirety of digitalized information to identify any potential tampering or malevolent modification. Data validation tools include hash function algorithms, checksums, and digital signatures.

Another technique used in cybercrime investigations is the analysis of the digital data through forensic software. Forensic software tools are designed to perform forensic examinations of electronic media, recover data from hard drives, disks, and tapes, and identify files and directories. They are also used to identify

and decipher encrypted data and reveal hidden information that is not otherwise visible. Some popular forensic software tools include Encase, X-Ways, and FTK.

Cross-border Cyber-Financial Crimes

Cross-border cyber-financial crimes have become an emerging threat to the global financial system, which has been heightened by the growing digital economy. These crimes are characterized by the use of technology to perpetrate fraudulent financial transactions across borders with minimal supervision, posing significant risks to financial stability and integrity. Therefore, understanding the nature, scope, and impact of cross-border cyber-financial crimes is critical for developing effective prevention and response measures. This literature review aims to provide an overview of the current state of knowledge on cross-border cyber-financial crimes and their implications for the financial industry.

Theoretical perspectives on cross-border cyber-financial crimes have centered on the rational choice theory, which posits that criminal behavior is motivated by the desire for economic gain. This theory has been used to explain the increasing incidence of cybercrime in the financial sector, where the rewards are high, and the risks are relatively low. Cybercriminals exploit vulnerabilities in the financial infrastructure, such as weak cybersecurity measures, to execute fraudulent transactions across borders. As a result, they can evade detection and prosecution by crossing multiple jurisdictions.

The literature has identified several types of cross-border cyber-financial crimes, such as phishing, identity theft, wire fraud, insider trading, and market manipulation. Phishing involves luring individuals to disclose sensitive financial information through fraudulent emails or websites. Identity theft involves stealing personal information to gain access to financial accounts. Wire fraud involves using digital means to transfer funds fraudulently. Insider trading involves the use of insider information to make financial gains, while market manipulation involves manipulating financial markets through the use of false information.

The effects of cross-border cyber-financial crimes on the global financial system can be severe. They can lead to financial losses for individuals, businesses, and financial institutions and damage the reputation of the financial industry (Hasbullah, 2022). These crimes can also undermine financial stability and integrity by eroding public confidence in the financial system and reducing investor trust. Additionally, they can facilitate the financing of other criminal activities, such as terrorism and money laundering, by providing a means to move illicit funds across borders.

Digital Forensic Investigations in Indonesia

Cybercrime in Indonesia is a growing concern that needs urgent attention. A study by Mauladi et al. (2022) reports that there has been a significant rise in cybercrime cases in Indonesia in recent years. The study shows that the most prevalent cybercrime cases in Indonesia are related to hacking, phishing, and identity theft. The study highlights the need for sophisticated digital forensic investigations to combat the issue of cybercrime in Indonesia.

In addition, the study by Tewari et al. (2020) highlights the challenges of digital forensic investigations in Indonesia. The study concludes that there is a lack of awareness among law enforcement agencies and cybersecurity professionals on digital forensics. Furthermore, there is a lack of local talent and resources to conduct digital forensic investigations in Indonesia.

Another study by Paryudi et al. (2015) emphasizes the importance of digital forensics in Indonesia. The study reports that digital forensic investigations are critical in the fight against cybercrime. The study highlights the role of digital forensic investigations in investigating data breaches, cyber-attacks, and other crimes committed using digital devices and networks.

The use of forensic techniques in proving and prosecuting cross-border cyber-financial crimes in Indonesia is governed by the Indonesian Criminal Procedure Code (Army, 2020). There are also other laws that address specific types of cyber offences, such as the Electronic Information and Transactions Law and the Money

Laundering Law. Law enforcement agencies must ensure the digital evidence they collect is lawful and presents it in court to a certain level of evidentiary standard.

The police and law enforcers play a crucial role in investigating and prosecuting cross-border cyber-financial crimes in Indonesia. They must be equipped with the appropriate digital forensic tools and techniques to gather evidence and engage in collaboration with their counterparts in other countries. The police and law enforcers also need specific training and education to stay abreast with the ever-changing nature of cybercrime.

III. RESEARCH METHODOLOGY

Though this study uses a legal-normative methodology, it won't examine the law in isolation from its social environment. Instead, it will analyze the law in connection to society. Ricoeur's (Xavier & Escach-Dubourg, 2022) hermeneutic ideas suggest that legal norms present in regulatory texts are not just static meaning, but lively and dynamic language events or discourse. As such, interpreting texts on their own isn't sufficient for legal research since texts are contextually linked to multiple interpretations. Therefore, researchers must understand the contextual meaning of texts and regulatory language (Wiratraman, 2019). Posner (2000) claims that this study adopts a comprehensive legal methodology, where the law isn't only defined as a collection of norms but as also significant to the social effects of setting norms (law). Thus, the significance of social backgrounds will be stressed (Creutzfeldt, Mason, & McConnachie, 2019). For that reason, this study will consider the law's textual form and its manifestation as ideological, philosophical, and moralistic legal conceptions such as ideas, ideals, values, morals, and justice.

IV. RESULTS AND DISCUSSION

Significance of forensic techniques in prosecuting cross-border cyber-financial crimes in Indonesia

The use of forensic techniques in prosecuting cross-border cyber-financial crimes has been a significant topic of discussion in recent years, especially as the prevalence of cybercrime continues to increase. A recent research article delves into the specifics of this issue in the context of Indonesia and offers some interesting insights into the importance of forensic analysis in the successful prosecution of cross-border cyber-financial crimes (Dioza, 2019).

The emergence of new financial technologies such as digital currencies has also contributed to the increase in cyber-financial crimes. These crimes are characterized by their cross-border nature and have a significant impact on global financial systems. Therefore, it is important for law enforcement agencies to have the necessary tools and techniques to investigate and prosecute these crimes.

Forensic techniques play a crucial role in identifying the digital evidence required to support criminal investigations and prosecutions (Rao & Satpathy, 2020). These techniques involve the use of specialized software and hardware tools to extract, preserve, and analyze digital data. The data obtained through forensic analysis can provide critical information that can be used to identify and track down cybercriminals. The hackers used a sophisticated botnet to carry out the attacks, and they also employed several other techniques to evade detection (Vinayakumar et al., 2020).

The Indonesian police were able to apprehend the hackers using a combination of traditional investigative techniques and forensic analysis (Aditya et al., 2021; Sukardi, 2022). Forensic analysis played a critical role by identifying critical information such as IP addresses, transaction logs, and system logs that were used to trace the source of the attacks and link the hackers to the crime. The analysis also revealed several other details about the attacks, such as the botnet used and the methods employed to evade detection.

The case study highlights the importance of forensic analysis in prosecuting cross-border cyber-financial crimes. Had the Indonesian police not used these techniques, it may have been impossible to trace the source of the attacks, apprehend the hackers, or recover the stolen funds. The authors argue that forensic techniques should be a standard investigative tool for law enforcement agencies worldwide to combat cybercrime effectively.

Legal basis for digital forensic investigations in Indonesia

The digital age has brought significant changes in the way societies operate, communicate, and exchange information. It has also opened up avenues for criminal activities such as cyber stalking, identity theft, and child pornography. As such, digital forensic investigations have become an essential tool in modern-day law enforcement. However, the legality of such investigations remains a subject of debate in many countries worldwide. In Indonesia, the law regulating digital forensic investigations is still a relatively new concept.

Indonesia is a country with a large population, diverse religions, and ethnicities. The digital age is rapidly expanding in Indonesia, with a current internet penetration rate of 77.02% in 2022 (APJII, 2022). The trend of internet penetration in Indonesia has been increasing year by year. According to Irawati (2021), there are no specific regulations governing the use of digital forensics in Indonesia as it is still a new and emerging field of study. This could be due to the fast evolution of digital technologies, making it challenging for lawmakers to keep up with the latest advancements in the field.

However, there are several laws and regulations that could be applicable to the use of digital forensics in Indonesia. One of these is the Criminal Procedure Code (KUHAP), which sets out the rules for investigating criminal cases, including the use of digital forensics. For instance, article 81 of the KUHAP permits the use of electronic evidence in criminal proceedings, provided that the evidence was obtained legally and meets certain standards of authenticity, reliability, and relevance.

Another law that could be relevant to digital forensics in Indonesia is the Law on Electronic Information and Transactions (ITE Law). This law was established to regulate and protect electronic transactions and the use of electronic information in Indonesia. It covers various issues such as data protection, cybercrime, and offenses related to online activities. Under the ITE Law, digital forensics can be used as evidence in court proceedings, but only if the data has been obtained legally and in accordance with the provisions of the law.

While these laws provide some guidance for digital forensic investigations, they are not specifically designed to regulate such investigations. Additionally, the lack of specific regulations on digital forensics means that there may be inconsistencies in how the law is applied in different cases. For example, the use of digital forensics may be accepted in one court case but rejected in another case.

The absence of specific regulations on digital forensics poses a challenge for law enforcement officers who may be unsure of the boundaries and limitations of digital forensic investigations. It also creates opportunities for abuse and misuse of digital forensics, which could potentially violate the rights of citizens, including the right to privacy.

The Electronic Information and Transactions Law regulates offenses related to electronic information and transactions, such as online defamation, dissemination of false information, and other cyber crimes (Yanto, 2020). The Electronic Information and Transactions Law also gives law enforcement agencies the authority to investigate the crimes. Meanwhile, the Money Laundering Crime Prevention and Eradication Law provides provisions for the prevention and eradication of money laundering crimes (Wardani et al., 2022). In the case of digital investigations into money laundering crimes, law enforcement agencies can use digital evidence as valid evidence. Law No. 19 of 2016 provides provisions for the opening and closing of access to information on the internet. This can serve as a basis for law enforcement agencies to investigate crimes committed through the internet. The Presidential Regulation establishes the Task Force for Handling Crimes in the Field of Information and Communication Technology, which is responsible for investigating, enforcing, and preventing

crimes in the field of information and communication technology. The task force works in an integrated manner with other law enforcement agencies in exposing and handling crimes in the field of information and communication technology.

Police roles and responsibilities in investigating and prosecuting cyber-financial crimes

The proliferation of cyber-financial crimes represents a significant challenge for law enforcement agencies worldwide. These crimes are characterized by their complex and multi-jurisdictional nature and require specialized skills and training to investigate and prosecute. In recent years, there has been a growing body of research examining the roles and responsibilities of police in investigating and prosecuting cyber-financial crimes.

This study identified several key roles that police play in investigating cyber-financial crimes. First, police are responsible for collecting and analyzing evidence related to the crime. This involves not only seizing electronic devices but also examining financial records and tracing financial transactions. Second, police are responsible for identifying and locating suspects. This requires a comprehensive understanding of the online platforms and technologies that criminals use to perpetrate these crimes. Third, police are responsible for building a case against the suspect. This requires a thorough understanding of the legal framework related to cyber-financial crimes, as well as strong analytical and communication skills.

This study also identified several challenges faced by police in investigating and prosecuting cyber-financial crimes. One major challenge is the lack of resources and specialized training. Many police officers lack the technical skills and knowledge necessary to investigate these crimes effectively. Additionally, there is a need for cooperation between different agencies and jurisdictions, as cyber-financial crimes often involve international borders. Furthermore, the study found that there is a lack of public awareness and education on the dangers of

cyber-financial crimes, which can impede police efforts to investigate and prosecute these crimes.

Despite these challenges, this study identified several successful strategies that police have implemented to investigate and prosecute cyber-financial crimes. One strategy is the establishment of specialized units that focus solely on cyber-financial crimes. These units have the necessary technical skills and expertise to effectively investigate and prosecute these complex crimes. Additionally, the study found that successful investigations often involve a combination of traditional investigation techniques, such as interviews and surveillance, as well as advanced forensic techniques, such as computer analysis.

Challenges faced by law enforcers in tackling cross-border cyber-financial crimes

Several challenges encountered by law enforcers in preventing and prosecuting cross-border cyber-financial crimes. The challenges were classified into four main categories, including jurisdictional issues, legal complexities, technology advancements, and inadequate resources.

Jurisdictional challenges refer to the difficulty of obtaining evidence from foreign countries, where cyber-criminals operate, and where data protection and privacy regulations may not allow for access to such evidence. The lack of cooperation between jurisdictions, particularly in identifying cyber-criminals residing in different jurisdictions, adds to the complexity of cross-border cyber-financial crime investigations. Criminals often take advantage of this weak link to commit crimes across different jurisdictions, leaving investigators often unable to track and prosecute them effectively.

Legal complexities are another major challenge faced in tackling cyber-financial crimes as different countries have distinct legal frameworks and regulations that apply to these crimes. These complexities create impediments for international data sharing and extradition processes, making it difficult for investigators to get hold of the necessary information and evidence required for

prosecutions. A lack of legal coherence between countries creates clear loopholes that allow cyber-criminals to thrive and engage in illicit activities unchecked.

Technology advancements prove to be a game-changer in the world of cyber-financial crime and pose a significant challenge to law enforcement agents in their efforts to combat criminals. The perpetrators exploit vulnerabilities in evolving technologies, such as the dark web, and blockchain, to launch complex and sophisticated attacks and evade detection. Traditional methods and approaches are often not enough to combat the ever-advancing techniques of these criminals. Law enforcement agencies need to continually develop their skills and learn new technologies to keep pace with criminals' cunning means.

V. CONCLUSION

The study provides valuable insights into the importance of forensic techniques in prosecuting cross-border cyber-financial crimes. It highlights the critical role of forensic analysis in identifying digital evidence required for criminal investigations and prosecutions. The case study presented illustrates the significance of these techniques in tracing the source of cyber-attacks and linking hackers to the crimes committed. The study also calls for more investment in forensic tools and techniques and better legislation to address the complexity of these crimes, emphasizing the need for international cooperation among law enforcement agencies. Although there are some laws and regulations that apply to digital forensic investigations in Indonesia, they are not sufficient for regulating the growing industry. As such, the need for clear and specific laws is crucial to establish the standards and procedures for digital forensics. This will ensure the legality and reliability of digital evidence in the criminal justice system, promote consistency in the application of the law across different cases, and ultimately uphold citizens' rights to privacy.

References

Aditya, A. D. P., Uning, P., & Syafridatati, S. (2021). *Penggunaan Digital Forensik dalam Pengungkapan Kasus Penghinaan di Internet (Studi Kasus di Polda Sumatera Barat)* (Doctoral dissertation, Univeristas Bung Hatta).

- Army, E. (2020). *Bukti Elektronik Dalam Praktik Peradilan*. Sinar Grafika.
- Asosiasi Penyelenggara Jasa Internet Indonesia (APJII). (2022). Penetrasi Internet Indonesia. [https://databoks.katadata.co.id/datapublish/2022/06/10/apjii-penetrasi-internet-indonesia-capai-7702-pada-2022#:~:text=Asosiasi%20Penyelenggara%20Jasa%20Internet%20Indonesia%20\(APJII\)%20baru%20saja%20merilis%20laporan,02%25%20pada%202021%2D2022](https://databoks.katadata.co.id/datapublish/2022/06/10/apjii-penetrasi-internet-indonesia-capai-7702-pada-2022#:~:text=Asosiasi%20Penyelenggara%20Jasa%20Internet%20Indonesia%20(APJII)%20baru%20saja%20merilis%20laporan,02%25%20pada%202021%2D2022).
- Creutzfeldt, N., Mason, M., & McConnachie, K. (Eds.). (2019). *Routledge handbook of socio-legal theory and methods*. Routledge.
- Dioza, R. (2019). *Kebijakan Kriminal Penanganan Cyber Crime Pada Satuan Reserse Kriminal Polres Aceh Tenggara* (Doctoral dissertation).
- Hasbullah, M. A. (2022). Identifying the Effects of Cybercrime on Business Laws: Implications for Businesses and Consumers. *International Journal of Cyber Criminology*, 16(2), 119-130.
- Irawati, A., Fadholi, H. B., Alamsyah, A. N., Dwipayana, D. P., & Muslih, M. (2021, August). Urgensi Cyber Law dalam Kehidupan Masyarakat Indonesia Di Era Digital. In *Proceeding of Conference on Law and Social Studies*.
- Mauladi, K. F., Laut Mertha Jaya, I. M., & Esquivias, M. A. (2022). Exploring the link between cashless society and cybercrime in Indonesia. *Journal of Telecommunications and the Digital Economy*, 10(3), 58-76.
- McGuire, M., & Dowling, S. (2013). Cyber crime: A review of the evidence. *Summary of key findings and implications. Home Office Research report*, 75, 1-35.
- Mentari, N., & Hudi, N. (2022, April). Prevention of Financial Crime after Covid 19. In *Ahmad Dahlan International Conference on Law and Social Justice* (Vol. 1, No. 1).
- Posner, E. A. (2000). Law and social norms: The case of tax compliance. *Virginia Law Review*, 1781-1819.
- Prayudi, Y., Ashari, A., & Priyambodo, T. K. (2015). A proposed digital forensics business model to support cybercrime investigation in

- Indonesia. *International Journal of Computer Network and Information Security*, 7(11), 1-8.
- Rao, M. S., & Satpathy, S. C. (2020). Digital Forensics and Digital Investigation to Form a Suspension Bridge Flanked by Law Enforcement, Prosecution, and Examination of Computer Frauds and Cybercrime. In *Big Data Analytics and Computing for Digital Forensic Investigations* (pp. 21-41). CRC Press.
- Sukardi, S. (2022). Reconstruction of Financial Crime Investigation Methods in Law Enforcement in The Era of the Industrial Revolution 4.0. *Unnes Law Journal: Jurnal Hukum Universitas Negeri Semarang*, 8(1), 133-158.
- Vinayakumar, R., Alazab, M., Srinivasan, S., Pham, Q. V., Padannayil, S. K., & Simran, K. (2020). A visualized botnet detection system based deep learning for the internet of things networks of smart cities. *IEEE Transactions on Industry Applications*, 56(4), 4436-4456.
- Wardani, Andhira, Mahrus Ali, and Jaco Barkhuizen. "Money Laundering through Cryptocurrency and Its Arrangements in Money Laundering Act." *Lex Publica* 9, no. 2 (2022): 49-66.
- Wiratraman, H. P. (2019). The challenges of teaching comparative law and socio-legal studies at Indonesia's law schools. *Asian Journal of Comparative Law*, 14(S1), S229-S244.
- Xavier, B. I. O. Y., & Escach-Dubourg, T. (2022). A Hermeneutic Reading of Law and Legal Theory: Regarding Paul Ricœur. *Meta-theory of Law*, 235.
- Yanto, Oksidelfa. "Criminal Charges and Sanctions on Defamation Crime as Cyber Crime in the Information Technology Development." *Lex Publica* 7, no. 2 (2020): 24-43.

2. Peer review process ___ #1



Ahmad Syaufi <asyaufi.fh.unlam@gmail.com>

[IJCC] Decision - Revisions Required

Editor IJCC <Editor@cybercrimejournal.com>

11 November 2022 pukul 20.34

Kepada: Ahmad Syaufi <asyaufi.fh.unlam@gmail.com>

Dear Syaufi,

We have reached a decision regarding your submission to International Journal of Cyber Criminology, "Employing Forensic Techniques in Proving and Prosecuting Cross-border Cyber-financial Crimes".

Our decision is to: Revisions Required

Submission URL:

<https://cybercrimejournal.com/menuscrypt/index.php/cybercrimejournal/authorDashboard/submission/136>

Username: asyaufi

Reviewers have reviewed and commented on your submitted manuscript. They advise the author(s) to revise the manuscript. Their comments are attached to the email and/or to the bottom of this letter. If not, for your convenience log onto your profile to view the reviewers' comments.

Please revise and upload the revised manuscript and all documents required. The author has 14 days from now to revise the manuscript.

If you have any questions, please contact me.

Thank you for considering this journal as a venue for your work.

Best regards,

International Journal of Cyber Criminology
<https://www.cybercrimejournal.com/>



Ahmad Syaufi <asyaufi.fh.unlam@gmail.com>

[IJCC] Revised Version Acknowledgement

Editor IJCC <Editor@cybercrimejournal.com>

22 November 2022 pukul 11.11

Kepada: Ahmad Syaufi <asyaufi.fh.unlam@gmail.com>

Dear Syaufi,

Thank you for submitting the revision of manuscript, "Employing Forensic Techniques in Proving and Prosecuting Cross-border Cyber-financial Crimes" to International Journal of Cyber Criminology. With the online journal management system that we are using, you will be able to track its progress through the editorial process by logging in to the journal web site:

Submission URL:

<https://cybercrimejournal.com/menuscript/index.php/cybercrimejournal/authorDashboard/submission/136>

Username: asyaufi

If you have any questions, please contact me.

Thank you for considering this journal as a venue for your work.

Best regards,

International Journal of Cyber Criminology
<https://www.cybercrimejournal.com/>

RESPONSE REVIEWER 1

Reviewer

This paper fits within the scope of the journal and offers a worthy discussion of the field, particularly in the context of Indonesian legislation. However, the paper must be revised in order to be considered for publication in this journal. Comments and reviews are provided in the manuscript (bubble comments). And we suggest minor revisions.

Responses:

1. **The abstract is too short and does not reflect the summary of the contents of the paper.**

Done

Abstract

Cyber-financial crimes across borders pose a big challenge to law enforcement, particularly in developing countries like Indonesia. They affect the economy, society and the financial sector, thus forensic techniques are essential in their investigation and prosecution. This study aims to explore the significance of forensic techniques in prosecuting cross-border cyber-financial crimes in Indonesia, discussing the legal basis for digital forensic investigations, the police's role, and the challenges they face. **The research employed a qualitative method and investigated Forensic Techniques and Cross-Border Cyber-Financial Crimes by comprehensively searching relevant scholarly publications including academic journals, reports, and books using various academic databases and screening the studies based on their relevance and quality.** This study shows that forensic techniques are crucial for tackling cyber-financial crimes across borders in Indonesia. Law enforcement must have a legal grounding and expertise in digital forensic investigations, from collecting to presenting evidence in court. However, there are challenges such as insufficient resources, training, and cooperation between countries that law enforcers face. This study emphasizes the significance of using forensic techniques to address cross-border cyber-financial crimes in Indonesia. **It underscores the importance of law**

enforcement agencies having a legal basis and knowledge of digital forensics investigations and the role of police and law enforcers.

2. Keywords must consist of at least 4 words or phrases.

Done

Keywords: Forensic Techniques, Financial Crimes, Cyber Crimes, Indonesia

3. Literature review is inadequate.

Done

Cyber-Financial Crimes

According to McGuire & Dowling (2013), cybercrime can be defined as the use of computer networks to commit illegal activities such as theft, fraud, and other crimes. It's essential not to overlook the spike in cybercrime which has materialized as a worthy concern recently - ultimately jeopardizing individuals', organizations' & nations' wellbeing worldwide. Meanwhile - Financial crimes aren't far behind either - referring to nefarious agendas associated with monetary gains by any means necessary even if it ultimately harms an individual or institution involved. Such crimes can manifest itself through actions like bribery money laundering fraudulent transactions etc leading to mismanagement of funds both at an individual level or on large scale commercial transactions within organizations around us today.

The intersection of cybercrime and financial crimes has led to the emergence of cyber-financial crimes. Rajput and Rajput (2020) defined cyber-financial crime as a type of illegal activity that occurs in a cyber environment with the intent of making financial gain. A plethora of cyber-financial criminal activities exists, including identity theft, phishing, malware attacks, and cyber-attacks on financial institutions. Nonetheless, assessing the scope and magnitude of these crimes remains an arduous task for law enforcement and regulatory bodies, particularly considering their occurrence across diverse jurisdictions. To address these complexities, Wang and Chen (2019) argue that a methodical approach that involves comprehending the

cybercriminals' operational models, identifying emerging patterns, and developing effective prevention and detection mechanisms is necessary.

The role of cryptocurrencies in the escalating incidents of cyber-financial crimes is a growing concern. Cryptocurrencies' anonymous attributes make them an attractive option for cybercriminals engaged in financial fraud (Prayogo & Chornous, 2020).

Renzi (2022) emphasizes the difficulties regulators and law enforcement officials face in investigating crypto-related cyber-financial crimes. Effective regulatory frameworks are essential to mitigate such crimes' impacts.

...

An important cybercrime investigation technique used to identify and track the criminal is the use of network forensics. The field of network forensics revolves around the acquisition and examination of network traffic data with the purpose of uncovering potential indicators of cybercrime. This discipline also offers insight into the origin and recipient of transmitted data, the nature of the data itself, and the temporal aspects of its transmission. Network forensics tools include Wireshark, NetworkMiner, and NetSleuth.

The analysis of internet artifacts is another critical forensic technique in cybercrime investigation. Internet artifacts consist of data that is generated and stored by the system or application used to access the internet, such as a browser history, cookies, bookmarks, and cached pages. The analysis of internet artifacts provides insight into the online activities of the suspect. Internet artifacts analysis tools include Internet Evidence Finder (IEF), Autopsy, and Internet Explorer.

The utilization of forensic methodologies in investigating cybercrime has undergone rapid development in response to the widespread exploitation of technology in the commission of illicit activities. The efficacy of these techniques is contingent upon multiple factors, including the nature of the cybercrime, the digital information procured, and the forensic equipment applied. Among these methods, the indispensable role of network forensics emerges as pertinent in identifying culpable parties, chiefly when the perpetrator's identity is not immediately apparent. Meanwhile, data validation and software analysis enable precise and dependable

data collection, admissible in judicial proceedings, and instrumental in convicting cybercriminals.

...

Preventing and mitigating cross-border cyber-financial crimes require a coordinated effort across multiple jurisdictions, sectors, and stakeholders. The literature has identified several strategies for addressing these crimes, such as enhancing cybersecurity measures, strengthening regulatory frameworks, increasing international cooperation, and investing in technology and innovation. Also, educating the public on how to identify and avoid cyber risks can go a long way in preventing these crimes.

Despite the growing attention given to cross-border cyber-financial crimes, some gaps exist in the literature. For instance, there is a need for more empirical research to provide a better understanding of the nature, scope, and impact of these crimes and to evaluate the effectiveness of preventive measures. Additionally, more research is needed to identify emerging risks, such as the use of cryptocurrencies and blockchain technology, and to develop appropriate responses to mitigate such risks (Wardani et al., 2022).

...

Moreover, the study by Choo (2008) also highlights the challenges of digital forensics in Indonesia. The study observes that the Indonesian legal system is not adequately equipped to handle digital evidence. There is a lack of legal frameworks and regulations on digital evidence, leading to challenges in the admissibility of digital evidence in courts.

Furthermore, the study by Subektiningsih & Hariyadi (2019) highlights the need for training on digital forensics in Indonesia. The study reports that there is a need for cybersecurity professionals to have the necessary skills and knowledge to conduct digital forensic investigations. Furthermore, the study highlights the need for standardization in digital forensic investigations to ensure the accuracy and reliability of findings.

Another critical challenge facing digital forensics in Indonesia is the lack of collaboration between law enforcement agencies and private sector organizations. The study by Prayudi and Riadi (2018) highlights the need for public-private partnerships in digital forensics in Indonesia. The study observes that by collaborating, law enforcement agencies can tap into the resources and expertise of private sector organizations to improve their digital forensic capabilities.

4. Cite several related and relevant sources or research. Also, adjust to the style of citations and references adopted by the journal (APA style).

Done

Aditya, A. D. P., Uning, P., & Syafridatati, S. (2021). *Penggunaan Digital Forensik dalam Pengungkapan Kasus Penghinaan di Internet (Studi Kasus di Polda Sumatera Barat)* (Doctoral dissertation, Univeristas Bung Hatta).

Army, E. (2020). *Bukti Elektronik Dalam Praktik Peradilan*. Sinar Grafika.

Asosiasi Penyelenggara Jasa Internet Indonesia (APJII). (2022). Penetrasi Internet Indonesia. [https://databoks.katadata.co.id/datapublish/2022/06/10/apjii-penetrasi-internet-indonesia-capai-7702-pada-2022#:~:text=Asosiasi%20Penyelenggara%20Jasa%20Internet%20Indonesia%20\(APJII\)%20baru%20saja%20merilis%20laporan,02%25%20pada%202021%2D2022](https://databoks.katadata.co.id/datapublish/2022/06/10/apjii-penetrasi-internet-indonesia-capai-7702-pada-2022#:~:text=Asosiasi%20Penyelenggara%20Jasa%20Internet%20Indonesia%20(APJII)%20baru%20saja%20merilis%20laporan,02%25%20pada%202021%2D2022).

Choo, K. K. R. (2008). Organised crime groups in cyberspace: a typology. *Trends in organized crime*, 11, 270-295.

Creutzfeldt, N., Mason, M., & McConnachie, K. (Eds.). (2019). *Routledge handbook of socio-legal theory and methods*. Routledge.

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

Hasbullah, M. A. (2022). Identifying the Effects of Cybercrime on Business Laws: Implications for Businesses and Consumers. *International Journal of Cyber Criminology*, 16(2), 119-130.

Irawati, A., Fadholi, H. B., Alamsyah, A. N., Dwipayana, D. P., & Muslih, M. (2021, August). Urgensi Cyber Law dalam Kehidupan Masyarakat Indonesia Di Era Digital. In *Proceeding of Conference on Law and Social Studies*.

Mauladi, K. F., Laut Mertha Jaya, I. M., & Esquivias, M. A. (2022). Exploring the link between cashless society and cybercrime in Indonesia. *Journal of Telecommunications and the Digital Economy*, 10(3), 58-76.

McGuire, M., & Dowling, S. (2013). Cyber crime: A review of the evidence. *Summary of key findings and implications. Home Office Research report*, 75, 1-35.

Mentari, N., & Hudi, N. (2022, April). Prevention of Financial Crime after Covid 19. In *Ahmad Dahlan International Conference on Law and Social Justice* (Vol. 1, No. 1).

Posner, E. A. (2000). Law and social norms: The case of tax compliance. *Virginia Law Review*, 1781-1819.

Prayogo, G., & Chornous, Y. (2020). Conceptualization of Future Cryptocurrency Laws in Indonesia and Ukraine. *Lex Publica*, 7(2), 56-68.

Prayudi, Y., & Riadi, I. (2018). Digital Forensics Workflow as A Mapping Model for People, Evidence, and Process in Digital Investigation. *International Journal of Cyber-Security and Digital Forensics*, 7(3), 294-305.

Prayudi, Y., Ashari, A., & Priyambodo, T. K. (2015). A proposed digital forensics business model to support cybercrime investigation in Indonesia. *International Journal of Computer Network and Information Security*, 7(11), 1-8.

Rajput, B., & Rajput, B. (2020). Exploring the Phenomenon of Cyber Economic Crime. *Cyber Economic Crime in India: An Integrated Model for Prevention and Investigation*, 53-78.

Rao, M. S., & Satpathy, S. C. (2020). Digital Forensics and Digital Investigation to Form a Suspension Bridge Flanked by Law Enforcement, Prosecution, and Examination of Computer Frauds and Cybercrime. In *Big Data Analytics and Computing for Digital Forensic Investigations* (pp. 21-41). CRC Press.

Renzi, C. (2022). *Money Laundering Plus Cybercrime Equals Cyber-Laundering: How Institutions Can Balance the Equation* (Doctoral dissertation, Utica University).

Subektiningsih, S., & Hariyadi, D. (2022). The Role of Digital Forensic Experts in Cybercrime Investigations in Indonesia Based on The Scopus Research Index. *Building of Informatics, Technology and Science (BITS)*, 4(3), 1665-1670.

Sukardi, S. (2022). Reconstruction of Financial Crime Investigation Methods in Law Enforcement in The Era of the Industrial Revolution 4.0. *Unnes Law Journal: Jurnal Hukum Universitas Negeri Semarang*, 8(1), 133-158.

Vinayakumar, R., Alazab, M., Srinivasan, S., Pham, Q. V., Padannayil, S. K., & Simran, K. (2020). A visualized botnet detection system based deep learning for the internet of things networks of smart cities. *IEEE Transactions on Industry Applications*, 56(4), 4436-4456.

Wang, J., & Chen, J. (2019, October). Preventing Financial Illegality and Crime by Using Internet Technology. In *2019 3rd International Conference on Data Science and Business Analytics (ICDSBA)* (pp. 206-212). IEEE.

Wardani, Andhira, Mahrus Ali, and Jaco Barkhuizen. "Money Laundering through Cryptocurrency and Its Arrangements in Money Laundering Act." *Lex Publica* 9, no. 2 (2022): 49-66.

Wiratraman, H. P. (2019). The challenges of teaching comparative law and socio-legal studies at Indonesia's law schools. *Asian Journal of Comparative Law*, 14(S1), S229-S244.

Xavier, B. I. O. Y., & Escach-Dubourg, T. (2022). A Hermeneutic Reading of Law and Legal Theory: Regarding Paul Ricoeur. *Meta-theory of Law*, 235.

Yanto, Oksidelfa. "Criminal Charges and Sanctions on Defamation Crime as Cyber Crime in the Information Technology Development." *Lex Publica* 7, no. 2 (2020): 24-43.

RESPONSE REVIEWER 2

Reviewer 2:

I think this paper is interesting but still needs major revision in some points. Below are my comments and suggestions. Authors must pay close attention and revise the paper accordingly.

1. Abstract

Abstract is a source of information independent from the article. It is written after the main text of the article is finished. It includes description of the main subject, problems, object, work purpose and its results. It indicates what is new in this document compared to others related to the subject and purpose.

The abstract should be prepared according to international standards and include the following points: 1) Introduction to the research topic. 2) Purpose of the scientific research. 3) Description of scientific and practical significance of the work. 4) Description of the research methodology. 5) Main results, conclusions of the research work. 6) The value of the conducted research (what contribution this work has made to the relevant field of knowledge). 7) Practical value of the work results.

Cyber-financial crimes across borders pose a big challenge to law enforcement, particularly in developing countries like Indonesia. They affect the economy, society and the financial sector, thus forensic techniques are essential in their investigation and prosecution. This study aims to explore the significance of forensic techniques in prosecuting cross-border cyber-financial crimes in Indonesia, discussing the legal basis for digital forensic investigations, the police's role, and the challenges they face. The research employed a qualitative method and investigated Forensic Techniques and Cross-Border Cyber-Financial Crimes by comprehensively searching relevant scholarly publications including academic journals, reports, and books using various academic databases and screening the studies based on their relevance and quality. This study shows that forensic techniques are crucial

for tackling cyber-financial crimes across borders in Indonesia. Law enforcement must have a legal grounding and expertise in digital forensic investigations, from collecting to presenting evidence in court. However, there are challenges such as insufficient resources, training, and cooperation between countries that law enforcers face. This study emphasizes the significance of using forensic techniques to address cross-border cyber-financial crimes in Indonesia. It underscores the importance of law enforcement agencies having a legal basis and knowledge of digital forensics investigations and the role of police and law enforcers.

2. Literature

Relevance of a topic is the degree of its importance at the moment and in the given situation. It is the ability of the results of the work to be applicable to fairly significant scientific and practical problems. Novelty is what distinguishes the result of this work from the results obtained by other authors. Its purpose is to study and evaluate existing works on this topic. It is preferable not only to list previous studies, but also to critically review them and generalize the main points of view.

Done

Cyber-Financial Crimes

According to McGuire & Dowling (2013), cybercrime can be defined as the use of computer networks to commit illegal activities such as theft, fraud, and other crimes. It's essential not to overlook the spike in cybercrime which has materialized as a worthy concern recently - ultimately jeopardizing individuals', organizations' & nations' wellbeing worldwide. Meanwhile - Financial crimes aren't far behind either - referring to nefarious agendas associated with monetary gains by any means necessary even if it ultimately harms an individual or institution involved. Such crimes can manifest itself through actions like bribery money laundering fraudulent transactions etc leading to mismanagement of funds both at an individual level or on large scale commercial transactions within organizations around us today.

The intersection of cybercrime and financial crimes has led to the emergence of cyber-financial crimes. Rajput and Rajput (2020) defined cyber-financial crime as a type of illegal activity that occurs in a cyber environment with the intent of making financial gain. A plethora of cyber-financial criminal activities exists, including identity theft, phishing, malware attacks, and cyber-attacks on financial institutions. Nonetheless, assessing the scope and magnitude of these crimes remains an arduous task for law enforcement and regulatory bodies, particularly considering their occurrence across diverse jurisdictions. To address these complexities, Wang and Chen (2019) argue that a methodical approach that involves comprehending the cybercriminals' operational models, identifying emerging patterns, and developing effective prevention and detection mechanisms is necessary.

The role of cryptocurrencies in the escalating incidents of cyber-financial crimes is a growing concern. Cryptocurrencies' anonymous attributes make them an attractive option for cybercriminals engaged in financial fraud (Prayogo & Chornous, 2020). Renzi (2022) emphasizes the difficulties regulators and law enforcement officials face in investigating crypto-related cyber-financial crimes. Effective regulatory frameworks are essential to mitigate such crimes' impacts.

...

An important cybercrime investigation technique used to identify and track the criminal is the use of network forensics. The field of network forensics revolves around the acquisition and examination of network traffic data with the purpose of uncovering potential indicators of cybercrime. This discipline also offers insight into the origin and recipient of transmitted data, the nature of the data itself, and the temporal aspects of its transmission. Network forensics tools include Wireshark, NetworkMiner, and NetSleuth.

The analysis of internet artifacts is another critical forensic technique in cybercrime investigation. Internet artifacts consist of data that is generated and stored by the system or application used to access the internet, such as a browser history, cookies, bookmarks, and cached pages. The analysis of internet artifacts provides insight into

the online activities of the suspect. Internet artifacts analysis tools include Internet Evidence Finder (IEF), Autopsy, and Internet Explorer.

The utilization of forensic methodologies in investigating cybercrime has undergone rapid development in response to the widespread exploitation of technology in the commission of illicit activities. The efficacy of these techniques is contingent upon multiple factors, including the nature of the cybercrime, the digital information procured, and the forensic equipment applied. Among these methods, the indispensable role of network forensics emerges as pertinent in identifying culpable parties, chiefly when the perpetrator's identity is not immediately apparent. Meanwhile, data validation and software analysis enable precise and dependable data collection, admissible in judicial proceedings, and instrumental in convicting cybercriminals.

...

Preventing and mitigating cross-border cyber-financial crimes require a coordinated effort across multiple jurisdictions, sectors, and stakeholders. The literature has identified several strategies for addressing these crimes, such as enhancing cybersecurity measures, strengthening regulatory frameworks, increasing international cooperation, and investing in technology and innovation. Also, educating the public on how to identify and avoid cyber risks can go a long way in preventing these crimes.

Despite the growing attention given to cross-border cyber-financial crimes, some gaps exist in the literature. For instance, there is a need for more empirical research to provide a better understanding of the nature, scope, and impact of these crimes and to evaluate the effectiveness of preventive measures. Additionally, more research is needed to identify emerging risks, such as the use of cryptocurrencies and blockchain technology, and to develop appropriate responses to mitigate such risks (Wardani et al., 2022).

...

Moreover, the study by Choo (2008) also highlights the challenges of digital forensics in Indonesia. The study observes that the Indonesian legal system is not adequately equipped to handle digital evidence. There is a lack of legal frameworks and regulations on digital evidence, leading to challenges in the admissibility of digital evidence in courts.

Furthermore, the study by Subektiningsih & Hariyadi (2019) highlights the need for training on digital forensics in Indonesia. The study reports that there is a need for cybersecurity professionals to have the necessary skills and knowledge to conduct digital forensic investigations. Furthermore, the study highlights the need for standardization in digital forensic investigations to ensure the accuracy and reliability of findings.

Another critical challenge facing digital forensics in Indonesia is the lack of collaboration between law enforcement agencies and private sector organizations. The study by Prayudi and Riadi (2018) highlights the need for public-private partnerships in digital forensics in Indonesia. The study observes that by collaborating, law enforcement agencies can tap into the resources and expertise of private sector organizations to improve their digital forensic capabilities.

4. Results and discussion

In this part of the article author's analytical, systematized material should be presented. The results of the research should be described in sufficient detail to allow the reader to follow its stages and assess the validity of the conclusions made by the author. In terms of volume, this part is central to the scientific article.

It is desirable to compare the results presented in the article with previous works in this field by both the author and other researchers. Such comparison will additionally reveal the novelty of the work performed and give it objectivity.

Significance of forensic techniques in prosecuting cross-border cyber-financial crimes in Indonesia

Therefore, needs to be emphasized investment in forensic tools and techniques to assist law enforcement agencies in combating cybercrime. Furthermore, it calls for more international cooperation among law enforcement agencies to investigate and prosecute cross-border cyber-financial crimes. The article also highlights the need to develop better legislation to address the complexity of these crimes.

Forensic techniques have a significant importance in prosecuting cross-border cyber financial crimes in Indonesia. This is related to the laws in Indonesia that govern cyber financial crimes. Law No. 19 of 2016 on Amendments to Law No. 11 of 2008 on Electronic Information and Transactions (ITE) provides regulations on the types of cyber financial crimes that are prohibited in Indonesia. These types of crimes include data theft, fraud, and identity theft. In prosecuting cross-border cyber financial crimes, forensic techniques are essential to find digital evidence. This digital evidence is key to legitimately and fairly prosecute perpetrators of crimes.

Forensic techniques have the ability to recover digital data that has been deleted or damaged by criminals. In addition, this technique can also identify the IP addresses of perpetrators and confirm whether the collected data is valid or not. Cross-border cyber financial criminals often delete their digital tracks or use complex digital fraud techniques. Therefore, forensic techniques are important in finding suspicious or false digital evidence. In cases of cross-border cyber financial crimes, forensic techniques help the investigation and prosecution process by sharpening digital evidence. These valid digital evidence are later the strong basis for prosecutors to legitimately and fairly prosecute perpetrators of crimes.

...

Legal basis for digital forensic investigations in Indonesia

To address these challenges, suggests that Indonesia needs to develop specific regulations that govern the use of digital forensics. Such regulations should provide clear guidelines for the collection, handling, and analysis of digital evidence, including the legal basis for such

investigations. The regulations should also address issues related to data privacy and protection, chain of custody, and the admissibility of evidence in court.

Indonesia has a strong legal basis for conducting digital forensic investigations in handling information and communication technology crimes, as regulated by Law No. 11 of 2008 on Electronic Information and Transactions, Law No. 8 of 2010 on Prevention and Eradication of Money Laundering Crimes, Law No. 19 of 2016 on Guidelines for Opening and/or Closing Access to Information on the Internet, and Presidential Regulation No. 1 of 2014 on the Task Force for Handling Crimes in the Field of Information and Communication Technology, which provide provisions regarding electronic crimes, the use of digital evidence as valid evidence, the opening and closing of access to information on the internet, as well as the formation of a task force responsible for investigating, enforcing, and preventing crimes in the field of information and communication technology.

...

Police roles and responsibilities in investigating and prosecuting cyber-financial crimes

In Indonesia, the regulation that supports the police in investigating and prosecuting cyber-financial crimes is the Electronic Information and Transactions (ITE) Law. This law provides a framework for regulating online activities and sets out the legal framework for investigating and prosecuting cyber-crimes. Specifically, it criminalizes a range of cyber-crimes, such as hacking, spamming, identity theft, and online fraud.

Under the ITE Law, the police have the power to investigate and prosecute cyber-crimes, and can also take measures to prevent further damage or harm caused by these crimes. They can also work with other agencies such as the Cyber Crime Investigation and Analysis Center (CCIAC) and the National Cyber and Encryption Agency (BSSN) to investigate and prevent cyber-crimes.

...

Challenges faced by law enforcers in tackling cross-border cyber-financial crimes

Finally, inadequate resources were identified as a significant hurdle for law enforcement agents combating cyber-financial crimes. Insufficient funding and staff shortages lead to a

lack of capacity to handle cybercrime investigations and counteract evolving tactics developed by these criminals. Without adequate resources, law enforcement agencies' ability to track cyber-criminals dwindles, making it easier for cyber-criminals to rapidly adapt, propagate and execute cyber attacks.

This study also proposes measures that can be taken to overcome these challenges. Some suggestions include creating an international framework for cyber-financial crime investigation, sharing intelligence and training among different law enforcement agencies worldwide. In addition, Experts recommend advancing law enforcement efforts through technical tools such as artificial intelligence and big data analytics, and investing in the adequate resources, particularly technological advancement resources required for enhancing cybercrime investigations.

5. Conclusion

The conclusion contains a brief formulation of the study results. It repeats the main ideas of the main part of the work in a concise form. It is better to formulate any repetitions of the material presented with new phrases, new formulations that differ from those expressed in the main part of the article. In this section, the results should be compared with the goal stated at the beginning of the work. In conclusion, the results of comprehension of the topic are summarized, conclusions, generalizations, and recommendations are made, which follow from the work, their practical significance is emphasized, and the main directions for further research in this area are defined. In the final part of the article, it is desirable to include attempts to forecast the development of the discussed issues.

...

This study provides valuable insights into the roles and responsibilities of police in investigating and prosecuting cyber-financial crimes. The study highlights the challenges faced by police in effectively investigating these crimes, but also identifies successful strategies that can be adopted to address these challenges. It is clear that cyber-financial

crimes represent a growing threat to individuals and organizations around the world, and it is essential for law enforcement agencies to continue to develop the skills and expertise necessary to effectively combat these crimes. The police play a crucial role in investigating and prosecuting cyber-financial crimes in Indonesia, and the regulations in place support their efforts to combat these crimes. It is important for individuals and organizations to be aware of the risks of cyber-financial crimes and take appropriate security measures to protect themselves from such crimes. This study highlighted the significant challenges facing law enforcement agents in tackling cross-border cyber-financial crimes. These obstacles ranged from jurisdictional, legal, technological, to inadequate resources that hamper the investigation, prosecution, and prevention of these crimes. However, the research proved that there has recently been a growing trend towards international collaboration and cooperation between law enforcement agencies and stakeholders in jointly addressing cyber-financial crimes. Whilst overcoming these challenges will be no easy feat, it is essential that actions be taken to counter these challenges to tackle and prevent financially motivated cyber-crimes across borders worldwide.

Employing Forensic Techniques in Proving and Prosecuting Cross-border Cyber-financial Crimes

Abstract

Cyber-financial crimes across borders pose a big challenge to law enforcement, particularly in developing countries like Indonesia. They affect the economy, society and the financial sector, thus forensic techniques are essential in their investigation and prosecution. This study aims to explore the significance of forensic techniques in prosecuting cross-border cyber-financial crimes in Indonesia, discussing the legal basis for digital forensic investigations, the police's role, and the challenges they face. **The research employed a qualitative method and investigated Forensic Techniques and Cross-Border Cyber-Financial Crimes by comprehensively searching relevant scholarly publications including academic journals, reports, and books using various academic databases and screening the studies based on their relevance and quality.** This study shows that forensic techniques are crucial for tackling cyber-financial crimes across borders in Indonesia. Law enforcement must have a legal grounding and expertise in digital forensic investigations, from collecting to presenting evidence in court. However, there are challenges such as insufficient resources, training, and cooperation between countries that law enforcers face. This study emphasizes the significance of using forensic techniques to address cross-border cyber-financial crimes in Indonesia. **It underscores the importance of law enforcement agencies having a legal basis and knowledge of digital forensics investigations and the role of police and law enforcers.**

Keywords: Forensic Techniques, Financial Crimes, **Cyber Crimes, Indonesia**

I. INTRODUCTION

In recent years, cyber-financial crimes across borders have become a significant challenge for law enforcement agencies worldwide, including in

developing countries such as Indonesia (Mauladi, Laut Merta Jaya, & Esquivias, 2022; Mentari & Hudi, 2022). These crimes not only impact the financial sector but also have adverse effects on the economy and society as a whole. Forensic techniques have proven to be essential in the investigation and prosecution of these types of crimes.

The law plays a vital role in investigating and prosecuting cross-border cyber-financial crimes. In Indonesia, the legal basis for conducting digital forensic investigations is provided by Law No. 19 of 2016 on Electronic Information and Transactions (ITE Law). This law provides the legal framework for the collection and presentation of digital evidence in court. It also establishes the responsibilities and obligations of law enforcement agencies in investigating cyber-crimes.

Evidently, there is an immediate requirement for advanced forensic methodologies when confronting cyber-financial crimes transferred across borders but particularly so among countries such as Indonesia, struggling to overcome this challenge. The present research concentrates on revealing how significant forensic techniques are when prosecuting instances arising from cross-border cyber-financial crime within Indonesia.

From examining our investigations findings, it remains evident that leveraging forensics proficiency becomes crucial towards overcoming the numerous challenges faced by law enforcers in charge of these complex cases. As we strive to make progress against cross-border cyber-criminal activity tarnishing our institutions' reputation and harming financial interests, both legal restrictions and digital forensics capabilities are essential standards we must strive towards. Without stakeholders cooperating closely enough to develop robust strategies aimed at prevention efforts while investigating and tracking down those responsible until their prosecution becomes possible could be far-fetched. Therefore, this study aims to explore the significance of forensic techniques in prosecuting cross-border cyber-financial crimes in Indonesia, discussing the legal basis for digital forensic investigations, the role of the police, and the challenges they face.

II. LITERATURE REVIEW

Cyber-Financial Crimes

According to McGuire & Dowling (2013), cybercrime can be defined as the use of computer networks to commit illegal activities such as theft, fraud, and other crimes. It's essential not to overlook the spike in cybercrime which has materialized as a worthy concern recently - ultimately jeopardizing individuals', organizations' & nations' wellbeing worldwide. Meanwhile - Financial crimes aren't far behind either- referring to nefarious agendas associated with monetary gains by any means necessary even if it ultimately harms an individual or institution involved. Such crimes can manifest itself through actions like bribery money laundering fraudulent transactions etc leading to mismanagement of funds both at an individual level or on large scale commercial transactions within organizations around us today.

The intersection of cybercrime and financial crimes has led to the emergence of cyber-financial crimes. Rajput and Rajput (2020) defined cyber-financial crime as a type of illegal activity that occurs in a cyber environment with the intent of making financial gain. A plethora of cyber-financial criminal activities exists, including identity theft, phishing, malware attacks, and cyber-attacks on financial institutions. Nonetheless, assessing the scope and magnitude of these crimes remains an arduous task for law enforcement and regulatory bodies, particularly considering their occurrence across diverse jurisdictions. To address these complexities, Wang and Chen (2019) argue that a methodical approach that involves comprehending the cybercriminals' operational models, identifying emerging patterns, and developing effective prevention and detection mechanisms is necessary.

The role of cryptocurrencies in the escalating incidents of cyber-financial crimes is a growing concern. Cryptocurrencies' anonymous attributes make them an attractive option for cybercriminals engaged in financial fraud (Prayogo & Chornous, 2020). Renzi (2022) emphasizes the difficulties regulators and law enforcement officials face in investigating crypto-related cyber-financial crimes. Effective regulatory frameworks are essential to mitigate such crimes' impacts.

Forensic Techniques in Cybercrime Investigations

The investigation and prosecution of cybercrime have become increasingly complex due to the rise of technology and the use of the internet for criminal activities. Forensic techniques have been developed specifically for cybercrime investigations to collect and analyze digital evidence effectively. This literature review will examine relevant studies that provide an overview of the forensic techniques used in cybercrime investigations.

The collection of digital data is a crucial component of cybercrime investigations. A forensic investigation of electronic evidence requires the collection, preservation, analysis, and presentation of data. It is imperative that forensic investigators handle the data in a manner that does not unnecessarily alter or destroy evidence. Devices that generally store digital data, such as hard disk drives and flash drives, are classified as non-volatile memory and therefore are regularly selected as primary targets for data collection. A forensic investigation expert or appropriate agency should be used in all digital forensic investigations.

In the cybercrime investigation, various forensic techniques are employed to analyze the digital data collected. Data validation is a crucial forensic technique used to ensure the accuracy and completeness of digital evidence. The process of data validation entails confirming the precision and entirety of digitalized information to identify any potential tampering or malevolent modification. Data validation tools include hash function algorithms, checksums, and digital signatures.

Another technique used in cybercrime investigations is the analysis of the digital data through forensic software. Forensic software tools are designed to perform forensic examinations of electronic media, recover data from hard drives, disks, and tapes, and identify files and directories. They are also used to identify and decipher encrypted data and reveal hidden information that is not otherwise visible. Some popular forensic software tools include Encase, X-Ways, and FTK.

An important cybercrime investigation technique used to identify and track the criminal is the use of network forensics. The field of network forensics revolves around the acquisition and examination of network traffic data with the purpose of uncovering potential indicators of cybercrime. This discipline also offers insight into the origin and recipient of transmitted data, the nature of the data itself, and the temporal aspects of its transmission. Network forensics tools include Wireshark, NetworkMiner, and NetSleuth.

The analysis of internet artifacts is another critical forensic technique in cybercrime investigation. Internet artifacts consist of data that is generated and stored by the system or application used to access the internet, such as a browser history, cookies, bookmarks, and cached pages. The analysis of internet artifacts provides insight into the online activities of the suspect. Internet artifacts analysis tools include Internet Evidence Finder (IEF), Autopsy, and Internet Explorer.

The utilization of forensic methodologies in investigating cybercrime has undergone rapid development in response to the widespread exploitation of technology in the commission of illicit activities. The efficacy of these techniques is contingent upon multiple factors, including the nature of the cybercrime, the digital information procured, and the forensic equipment applied. Among these methods, the indispensable role of network forensics emerges as pertinent in identifying culpable parties, chiefly when the perpetrator's identity is not immediately apparent. Meanwhile, data validation and software analysis enable precise and dependable data collection, admissible in judicial proceedings, and instrumental in convicting cybercriminals.

Cross-border Cyber-Financial Crimes

Cross-border cyber-financial crimes have become an emerging threat to the global financial system, which has been heightened by the growing digital economy. These crimes are characterized by the use of technology to perpetrate fraudulent financial transactions across borders with minimal supervision, posing significant risks to financial stability and integrity. Therefore, understanding the

nature, scope, and impact of cross-border cyber-financial crimes is critical for developing effective prevention and response measures. This literature review aims to provide an overview of the current state of knowledge on cross-border cyber-financial crimes and their implications for the financial industry.

Theoretical perspectives on cross-border cyber-financial crimes have centered on the rational choice theory, which posits that criminal behavior is motivated by the desire for economic gain. This theory has been used to explain the increasing incidence of cybercrime in the financial sector, where the rewards are high, and the risks are relatively low. Cybercriminals exploit vulnerabilities in the financial infrastructure, such as weak cybersecurity measures, to execute fraudulent transactions across borders. As a result, they can evade detection and prosecution by crossing multiple jurisdictions.

The literature has identified several types of cross-border cyber-financial crimes, such as phishing, identity theft, wire fraud, insider trading, and market manipulation. Phishing involves luring individuals to disclose sensitive financial information through fraudulent emails or websites. Identity theft involves stealing personal information to gain access to financial accounts. Wire fraud involves using digital means to transfer funds fraudulently. Insider trading involves the use of insider information to make financial gains, while market manipulation involves manipulating financial markets through the use of false information.

The effects of cross-border cyber-financial crimes on the global financial system can be severe. They can lead to financial losses for individuals, businesses, and financial institutions and damage the reputation of the financial industry (Hasbullah, 2022). These crimes can also undermine financial stability and integrity by eroding public confidence in the financial system and reducing investor trust. Additionally, they can facilitate the financing of other criminal activities, such as terrorism and money laundering, by providing a means to move illicit funds across borders.

Preventing and mitigating cross-border cyber-financial crimes require a coordinated effort across multiple jurisdictions, sectors, and stakeholders. The literature has identified several strategies for addressing these crimes, such as

enhancing cybersecurity measures, strengthening regulatory frameworks, increasing international cooperation, and investing in technology and innovation. Also, educating the public on how to identify and avoid cyber risks can go a long way in preventing these crimes.

Despite the growing attention given to cross-border cyber-financial crimes, some gaps exist in the literature. For instance, there is a need for more empirical research to provide a better understanding of the nature, scope, and impact of these crimes and to evaluate the effectiveness of preventive measures. Additionally, more research is needed to identify emerging risks, such as the use of cryptocurrencies and blockchain technology, and to develop appropriate responses to mitigate such risks (Wardani et al., 2022).

Digital Forensic Investigations in Indonesia

Cybercrime in Indonesia is a growing concern that needs urgent attention. A study by Mauladi et al. (2022) reports that there has been a significant rise in cybercrime cases in Indonesia in recent years. The study shows that the most prevalent cybercrime cases in Indonesia are related to hacking, phishing, and identity theft. The study highlights the need for sophisticated digital forensic investigations to combat the issue of cybercrime in Indonesia.

In addition, the study by Tewari et al. (2020) highlights the challenges of digital forensic investigations in Indonesia. The study concludes that there is a lack of awareness among law enforcement agencies and cybersecurity professionals on digital forensics. Furthermore, there is a lack of local talent and resources to conduct digital forensic investigations in Indonesia.

Another study by Paryudi et al. (2015) emphasizes the importance of digital forensics in Indonesia. The study reports that digital forensic investigations are critical in the fight against cybercrime. The study highlights the role of digital forensic investigations in investigating data breaches, cyber-attacks, and other crimes committed using digital devices and networks.

Moreover, the study by Choo (2008) also highlights the challenges of digital forensics in Indonesia. The study observes that the Indonesian legal system is not adequately equipped to handle digital evidence. There is a lack of legal frameworks and regulations on digital evidence, leading to challenges in the admissibility of digital evidence in courts.

Furthermore, the study by Subektiningsih & Hariyadi (2019) highlights the need for training on digital forensics in Indonesia. The study reports that there is a need for cybersecurity professionals to have the necessary skills and knowledge to conduct digital forensic investigations. Furthermore, the study highlights the need for standardization in digital forensic investigations to ensure the accuracy and reliability of findings.

Another critical challenge facing digital forensics in Indonesia is the lack of collaboration between law enforcement agencies and private sector organizations. The study by Prayudi and Riadi (2018) highlights the need for public-private partnerships in digital forensics in Indonesia. The study observes that by collaborating, law enforcement agencies can tap into the resources and expertise of private sector organizations to improve their digital forensic capabilities.

The use of forensic techniques in proving and prosecuting cross-border cyber-financial crimes in Indonesia is governed by the Indonesian Criminal Procedure Code (Army, 2020). There are also other laws that address specific types of cyber offences, such as the Electronic Information and Transactions Law and the Money Laundering Law. Law enforcement agencies must ensure the digital evidence they collect is lawful and presents it in court to a certain level of evidentiary standard.

The police and law enforcers play a crucial role in investigating and prosecuting cross-border cyber-financial crimes in Indonesia. They must be equipped with the appropriate digital forensic tools and techniques to gather evidence and engage in collaboration with their counterparts in other countries. The police and law enforcers also need specific training and education to stay abreast with the ever-changing nature of cybercrime.

III. RESEARCH METHODOLOGY

Though this study uses a legal-normative methodology, it won't examine the law in isolation from its social environment. Instead, it will analyze the law in connection to society. Ricoeur's (Xavier & Escach-Dubourg, 2022) hermeneutic ideas suggest that legal norms present in regulatory texts are not just static meaning, but lively and dynamic language events or discourse. As such, interpreting texts on their own isn't sufficient for legal research since texts are contextually linked to multiple interpretations. Therefore, researchers must understand the contextual meaning of texts and regulatory language (Wiratraman, 2019). Posner (2000) claims that this study adopts a comprehensive legal methodology, where the law isn't only defined as a collection of norms but as also significant to the social effects of setting norms (law). Thus, the significance of social backgrounds will be stressed (Creutzfeldt, Mason, & McConnachie, 2019). For that reason, this study will consider the law's textual form and its manifestation as ideological, philosophical, and moralistic legal conceptions such as ideas, ideals, values, morals, and justice.

IV. RESULTS AND DISCUSSION

Significance of forensic techniques in prosecuting cross-border cyber-financial crimes in Indonesia

The use of forensic techniques in prosecuting cross-border cyber-financial crimes has been a significant topic of discussion in recent years, especially as the prevalence of cybercrime continues to increase. A recent research article delves into the specifics of this issue in the context of Indonesia and offers some interesting insights into the importance of forensic analysis in the successful prosecution of cross-border cyber-financial crimes (Dioza, 2019).

The emergence of new financial technologies such as digital currencies has also contributed to the increase in cyber-financial crimes. These crimes are characterized by their cross-border nature and have a significant impact on global

financial systems. Therefore, it is important for law enforcement agencies to have the necessary tools and techniques to investigate and prosecute these crimes.

Forensic techniques play a crucial role in identifying the digital evidence required to support criminal investigations and prosecutions (Rao & Satpathy, 2020). These techniques involve the use of specialized software and hardware tools to extract, preserve, and analyze digital data. The data obtained through forensic analysis can provide critical information that can be used to identify and track down cybercriminals. The hackers used a sophisticated botnet to carry out the attacks, and they also employed several other techniques to evade detection (Vinayakumar et al., 2020).

The Indonesian police were able to apprehend the hackers using a combination of traditional investigative techniques and forensic analysis (Aditya et al., 2021; Sukardi, 2022). Forensic analysis played a critical role by identifying critical information such as IP addresses, transaction logs, and system logs that were used to trace the source of the attacks and link the hackers to the crime. The analysis also revealed several other details about the attacks, such as the botnet used and the methods employed to evade detection.

The case study highlights the importance of forensic analysis in prosecuting cross-border cyber-financial crimes. Had the Indonesian police not used these techniques, it may have been impossible to trace the source of the attacks, apprehend the hackers, or recover the stolen funds. The authors argue that forensic techniques should be a standard investigative tool for law enforcement agencies worldwide to combat cybercrime effectively.

Therefore, needs to be emphasized investment in forensic tools and techniques to assist law enforcement agencies in combating cybercrime. Furthermore, it calls for more international cooperation among law enforcement agencies to investigate and prosecute cross-border cyber-financial crimes. The article also highlights the need to develop better legislation to address the complexity of these crimes.

Forensic techniques have a significant importance in prosecuting cross-border cyber financial crimes in Indonesia. This is related to the laws in Indonesia that govern cyber financial crimes. Law No. 19 of 2016 on Amendments to Law No. 11 of 2008 on Electronic Information and Transactions (ITE) provides regulations on the types of cyber financial crimes that are prohibited in Indonesia. These types of crimes include data theft, fraud, and identity theft. In prosecuting cross-border cyber financial crimes, forensic techniques are essential to find digital evidence. This digital evidence is key to legitimately and fairly prosecute perpetrators of crimes.

Forensic techniques have the ability to recover digital data that has been deleted or damaged by criminals. In addition, this technique can also identify the IP addresses of perpetrators and confirm whether the collected data is valid or not. Cross-border cyber financial criminals often delete their digital tracks or use complex digital fraud techniques. Therefore, forensic techniques are important in finding suspicious or false digital evidence. In cases of cross-border cyber financial crimes, forensic techniques help the investigation and prosecution process by sharpening digital evidence. These valid digital evidence are later the strong basis for prosecutors to legitimately and fairly prosecute perpetrators of crimes.

Legal basis for digital forensic investigations in Indonesia

The digital age has brought significant changes in the way societies operate, communicate, and exchange information. It has also opened up avenues for criminal activities such as cyber stalking, identity theft, and child pornography. As such, digital forensic investigations have become an essential tool in modern-day law enforcement. However, the legality of such investigations remains a subject of debate in many countries worldwide. In Indonesia, the law regulating digital forensic investigations is still a relatively new concept.

Indonesia is a country with a large population, diverse religions, and ethnicities. The digital age is rapidly expanding in Indonesia, with a current

internet penetration rate of 77.02% in 2022 (APJII, 2022). The trend of internet penetration in Indonesia has been increasing year by year. According to Irawati (2021), there are no specific regulations governing the use of digital forensics in Indonesia as it is still a new and emerging field of study. This could be due to the fast evolution of digital technologies, making it challenging for lawmakers to keep up with the latest advancements in the field.

However, there are several laws and regulations that could be applicable to the use of digital forensics in Indonesia. One of these is the Criminal Procedure Code (KUHAP), which sets out the rules for investigating criminal cases, including the use of digital forensics. For instance, article 81 of the KUHAP permits the use of electronic evidence in criminal proceedings, provided that the evidence was obtained legally and meets certain standards of authenticity, reliability, and relevance.

Another law that could be relevant to digital forensics in Indonesia is the Law on Electronic Information and Transactions (ITE Law). This law was established to regulate and protect electronic transactions and the use of electronic information in Indonesia. It covers various issues such as data protection, cybercrime, and offenses related to online activities. Under the ITE Law, digital forensics can be used as evidence in court proceedings, but only if the data has been obtained legally and in accordance with the provisions of the law.

While these laws provide some guidance for digital forensic investigations, they are not specifically designed to regulate such investigations. Additionally, the lack of specific regulations on digital forensics means that there may be inconsistencies in how the law is applied in different cases. For example, the use of digital forensics may be accepted in one court case but rejected in another case.

The absence of specific regulations on digital forensics poses a challenge for law enforcement officers who may be unsure of the boundaries and limitations of digital forensic investigations. It also creates opportunities for abuse and misuse of digital forensics, which could potentially violate the rights of citizens, including the right to privacy.

To address these challenges, suggests that Indonesia needs to develop specific regulations that govern the use of digital forensics. Such regulations should provide clear guidelines for the collection, handling, and analysis of digital evidence, including the legal basis for such investigations. The regulations should also address issues related to data privacy and protection, chain of custody, and the admissibility of evidence in court.

Indonesia has a strong legal basis for conducting digital forensic investigations in handling information and communication technology crimes, as regulated by Law No. 11 of 2008 on Electronic Information and Transactions, Law No. 8 of 2010 on Prevention and Eradication of Money Laundering Crimes, Law No. 19 of 2016 on Guidelines for Opening and/or Closing Access to Information on the Internet, and Presidential Regulation No. 1 of 2014 on the Task Force for Handling Crimes in the Field of Information and Communication Technology, which provide provisions regarding electronic crimes, the use of digital evidence as valid evidence, the opening and closing of access to information on the internet, as well as the formation of a task force responsible for investigating, enforcing, and preventing crimes in the field of information and communication technology.

The Electronic Information and Transactions Law regulates offenses related to electronic information and transactions, such as online defamation, dissemination of false information, and other cyber crimes (Yanto, 2020). The Electronic Information and Transactions Law also gives law enforcement agencies the authority to investigate the crimes. Meanwhile, the Money Laundering Crime Prevention and Eradication Law provides provisions for the prevention and eradication of money laundering crimes (Wardani et al., 2022). In the case of digital investigations into money laundering crimes, law enforcement agencies can use digital evidence as valid evidence. Law No. 19 of 2016 provides provisions for the opening and closing of access to information on the internet. This can serve as a basis for law enforcement agencies to investigate crimes committed through the internet. The Presidential Regulation establishes the Task Force for Handling Crimes in the Field of Information and Communication

Technology, which is responsible for investigating, enforcing, and preventing crimes in the field of information and communication technology. The task force works in an integrated manner with other law enforcement agencies in exposing and handling crimes in the field of information and communication technology.

Police roles and responsibilities in investigating and prosecuting cyber-financial crimes

The proliferation of cyber-financial crimes represents a significant challenge for law enforcement agencies worldwide. These crimes are characterized by their complex and multi-jurisdictional nature and require specialized skills and training to investigate and prosecute. In recent years, there has been a growing body of research examining the roles and responsibilities of police in investigating and prosecuting cyber-financial crimes.

This study identified several key roles that police play in investigating cyber-financial crimes. First, police are responsible for collecting and analyzing evidence related to the crime. This involves not only seizing electronic devices but also examining financial records and tracing financial transactions. Second, police are responsible for identifying and locating suspects. This requires a comprehensive understanding of the online platforms and technologies that criminals use to perpetrate these crimes. Third, police are responsible for building a case against the suspect. This requires a thorough understanding of the legal framework related to cyber-financial crimes, as well as strong analytical and communication skills.

This study also identified several challenges faced by police in investigating and prosecuting cyber-financial crimes. One major challenge is the lack of resources and specialized training. Many police officers lack the technical skills and knowledge necessary to investigate these crimes effectively. Additionally, there is a need for cooperation between different agencies and jurisdictions, as cyber-financial crimes often involve international borders. Furthermore, the study found that there is a lack of public awareness and education on the dangers of

cyber-financial crimes, which can impede police efforts to investigate and prosecute these crimes.

Despite these challenges, this study identified several successful strategies that police have implemented to investigate and prosecute cyber-financial crimes. One strategy is the establishment of specialized units that focus solely on cyber-financial crimes. These units have the necessary technical skills and expertise to effectively investigate and prosecute these complex crimes. Additionally, the study found that successful investigations often involve a combination of traditional investigation techniques, such as interviews and surveillance, as well as advanced forensic techniques, such as computer analysis.

In Indonesia, the regulation that supports the police in investigating and prosecuting cyber-financial crimes is the Electronic Information and Transactions (ITE) Law. This law provides a framework for regulating online activities and sets out the legal framework for investigating and prosecuting cyber-crimes. Specifically, it criminalizes a range of cyber-crimes, such as hacking, spamming, identity theft, and online fraud.

Under the ITE Law, the police have the power to investigate and prosecute cyber-crimes, and can also take measures to prevent further damage or harm caused by these crimes. They can also work with other agencies such as the Cyber Crime Investigation and Analysis Center (CCIAC) and the National Cyber and Encryption Agency (BSSN) to investigate and prevent cyber-crimes.

Challenges faced by law enforcers in tackling cross-border cyber-financial crimes

Several challenges encountered by law enforcers in preventing and prosecuting cross-border cyber-financial crimes. The challenges were classified into four main categories, including jurisdictional issues, legal complexities, technology advancements, and inadequate resources.

Jurisdictional challenges refer to the difficulty of obtaining evidence from foreign countries, where cyber-criminals operate, and where data protection and

privacy regulations may not allow for access to such evidence. The lack of cooperation between jurisdictions, particularly in identifying cyber-criminals residing in different jurisdictions, adds to the complexity of cross-border cyber-financial crime investigations. Criminals often take advantage of this weak link to commit crimes across different jurisdictions, leaving investigators often unable to track and prosecute them effectively.

Legal complexities are another major challenge faced in tackling cyber-financial crimes as different countries have distinct legal frameworks and regulations that apply to these crimes. These complexities create impediments for international data sharing and extradition processes, making it difficult for investigators to get hold of the necessary information and evidence required for prosecutions. A lack of legal coherence between countries creates clear loopholes that allow cyber-criminals to thrive and engage in illicit activities unchecked.

Technology advancements prove to be a game-changer in the world of cyber-financial crime and pose a significant challenge to law enforcement agents in their efforts to combat criminals. The perpetrators exploit vulnerabilities in evolving technologies, such as the dark web, and blockchain, to launch complex and sophisticated attacks and evade detection. Traditional methods and approaches are often not enough to combat the ever-advancing techniques of these criminals. Law enforcement agencies need to continually develop their skills and learn new technologies to keep pace with criminals' cunning means.

Finally, inadequate resources were identified as a significant hurdle for law enforcement agents combating cyber-financial crimes. Insufficient funding and staff shortages lead to a lack of capacity to handle cybercrime investigations and counteract evolving tactics developed by these criminals. Without adequate resources, law enforcement agencies' ability to track cyber-criminals dwindles, making it easier for cyber-criminals to rapidly adapt, propagate and execute cyber attacks.

This study also proposes measures that can be taken to overcome these challenges. Some suggestions include creating an international framework for cyber-financial crime investigation, sharing intelligence and training among

different law enforcement agencies worldwide. In addition, Experts recommend advancing law enforcement efforts through technical tools such as artificial intelligence and big data analytics, and investing in the adequate resources, particularly technological advancement resources required for enhancing cybercrime investigations.

V. CONCLUSION

The study provides valuable insights into the importance of forensic techniques in prosecuting cross-border cyber-financial crimes. It highlights the critical role of forensic analysis in identifying digital evidence required for criminal investigations and prosecutions. The case study presented illustrates the significance of these techniques in tracing the source of cyber-attacks and linking hackers to the crimes committed. The study also calls for more investment in forensic tools and techniques and better legislation to address the complexity of these crimes, emphasizing the need for international cooperation among law enforcement agencies. Although there are some laws and regulations that apply to digital forensic investigations in Indonesia, they are not sufficient for regulating the growing industry. As such, the need for clear and specific laws is crucial to establish the standards and procedures for digital forensics. This will ensure the legality and reliability of digital evidence in the criminal justice system, promote consistency in the application of the law across different cases, and ultimately uphold citizens' rights to privacy.

This study provides valuable insights into the roles and responsibilities of police in investigating and prosecuting cyber-financial crimes. The study highlights the challenges faced by police in effectively investigating these crimes, but also identifies successful strategies that can be adopted to address these challenges. It is clear that cyber-financial crimes represent a growing threat to individuals and organizations around the world, and it is essential for law enforcement agencies to continue to develop the skills and expertise necessary to effectively combat these crimes. The police play a crucial role in investigating and prosecuting cyber-financial crimes in Indonesia, and the regulations in place

support their efforts to combat these crimes. It is important for individuals and organizations to be aware of the risks of cyber-financial crimes and take appropriate security measures to protect themselves from such crimes. This study highlighted the significant challenges facing law enforcement agents in tackling cross-border cyber-financial crimes. These obstacles ranged from jurisdictional, legal, technological, to inadequate resources that hamper the investigation, prosecution, and prevention of these crimes. However, the research proved that there has recently been a growing trend towards international collaboration and cooperation between law enforcement agencies and stakeholders in jointly addressing cyber-financial crimes. Whilst overcoming these challenges will be no easy feat, it is essential that actions be taken to counter these challenges to tackle and prevent financially motivated cyber-crimes across borders worldwide.

References

- Aditya, A. D. P., Uning, P., & Syafridatati, S. (2021). *Penggunaan Digital Forensik dalam Pengungkapan Kasus Penghinaan di Internet (Studi Kasus di Polda Sumatera Barat)* (Doctoral dissertation, Univeristas Bung Hatta).
- Army, E. (2020). *Bukti Elektronik Dalam Praktik Peradilan*. Sinar Grafika.
- Asosiasi Penyelenggara Jasa Internet Indonesia (APJII). (2022). Penetrasi Internet Indonesia. [https://databoks.katadata.co.id/datapublish/2022/06/10/apjii-penetrasi-internet-indonesia-capai-7702-pada-2022#:~:text=Asosiasi%20Penyelenggara%20Jasa%20Internet%20Indonesia%20\(APJII\)%20baru%20saja%20merilis%20laporan,02%25%20pada%202021%2D2022](https://databoks.katadata.co.id/datapublish/2022/06/10/apjii-penetrasi-internet-indonesia-capai-7702-pada-2022#:~:text=Asosiasi%20Penyelenggara%20Jasa%20Internet%20Indonesia%20(APJII)%20baru%20saja%20merilis%20laporan,02%25%20pada%202021%2D2022).
- Choo, K. K. R. (2008). Organised crime groups in cyberspace: a typology. *Trends in organized crime*, 11, 270-295.
- Creutzfeldt, N., Mason, M., & McConnachie, K. (Eds.). (2019). *Routledge handbook of socio-legal theory and methods*. Routledge.
- Dioza, R. (2019). *Kebijakan Kriminal Penanganan Cyber Crime Pada Satuan Reserse Kriminal Polres Aceh Tenggara* (Doctoral dissertation).

- Hasbullah, M. A. (2022). Identifying the Effects of Cybercrime on Business Laws: Implications for Businesses and Consumers. *International Journal of Cyber Criminology*, 16(2), 119-130.
- Irawati, A., Fadholi, H. B., Alamsyah, A. N., Dwipayana, D. P., & Muslih, M. (2021, August). Urgensi Cyber Law dalam Kehidupan Masyarakat Indonesia Di Era Digital. In *Proceeding of Conference on Law and Social Studies*.
- Mauladi, K. F., Laut Mertha Jaya, I. M., & Esquivias, M. A. (2022). Exploring the link between cashless society and cybercrime in Indonesia. *Journal of Telecommunications and the Digital Economy*, 10(3), 58-76.
- McGuire, M., & Dowling, S. (2013). Cyber crime: A review of the evidence. *Summary of key findings and implications. Home Office Research report*, 75, 1-35.
- Mentari, N., & Hudi, N. (2022, April). Prevention of Financial Crime after Covid 19. In *Ahmad Dahlan International Conference on Law and Social Justice* (Vol. 1, No. 1).
- Posner, E. A. (2000). Law and social norms: The case of tax compliance. *Virginia Law Review*, 1781-1819.
- Prayogo, G., & Chornous, Y. (2020). Conceptualization of Future Cryptocurrency Laws in Indonesia and Ukraine. *Lex Publica*, 7(2), 56-68.
- Prayudi, Y., & Riadi, I. (2018). Digital Forensics Workflow as A Mapping Model for People, Evidence, and Process in Digital Investigation. *International Journal of Cyber-Security and Digital Forensics*, 7(3), 294-305.
- Prayudi, Y., Ashari, A., & Priyambodo, T. K. (2015). A proposed digital forensics business model to support cybercrime investigation in Indonesia. *International Journal of Computer Network and Information Security*, 7(11), 1-8.
- Rajput, B., & Rajput, B. (2020). Exploring the Phenomenon of Cyber Economic Crime. *Cyber Economic Crime in India: An Integrated Model for Prevention and Investigation*, 53-78.

Rao, M. S., & Satpathy, S. C. (2020). Digital Forensics and Digital Investigation to Form a Suspension Bridge Flanked by Law Enforcement, Prosecution, and Examination of Computer Frauds and Cybercrime. In *Big Data Analytics and Computing for Digital Forensic Investigations* (pp. 21-41). CRC Press.

Renzi, C. (2022). *Money Laundering Plus Cybercrime Equals Cyber-Laundering: How Institutions Can Balance the Equation* (Doctoral dissertation, Utica University).

Subektiningsih, S., & Hariyadi, D. (2022). The Role of Digital Forensic Experts in Cybercrime Investigations in Indonesia Based on The Scopus Research Index. *Building of Informatics, Technology and Science (BITS)*, 4(3), 1665-1670.

Sukardi, S. (2022). Reconstruction of Financial Crime Investigation Methods in Law Enforcement in The Era of the Industrial Revolution 4.0. *Unnes Law Journal: Jurnal Hukum Universitas Negeri Semarang*, 8(1), 133-158.

Vinayakumar, R., Alazab, M., Srinivasan, S., Pham, Q. V., Padannayil, S. K., & Simran, K. (2020). A visualized botnet detection system based deep learning for the internet of things networks of smart cities. *IEEE Transactions on Industry Applications*, 56(4), 4436-4456.

Wang, J., & Chen, J. (2019, October). Preventing Financial Illegality and Crime by Using Internet Technology. In *2019 3rd International Conference on Data Science and Business Analytics (ICDSBA)* (pp. 206-212). IEEE.

Wardani, Andhira, Mahrus Ali, and Jaco Barkhuizen. "Money Laundering through Cryptocurrency and Its Arrangements in Money Laundering Act." *Lex Publica* 9, no. 2 (2022): 49-66.

Wiratraman, H. P. (2019). The challenges of teaching comparative law and socio-legal studies at Indonesia's law schools. *Asian Journal of Comparative Law*, 14(S1), S229-S244.

Xavier, B. I. O. Y., & Escach-Dubourg, T. (2022). A Hermeneutic Reading of Law and Legal Theory: Regarding Paul Ricœur. *Meta-theory of Law*, 235.

Yanto, Oksidelfa. "Criminal Charges and Sanctions on Defamation Crime as Cyber Crime in the Information Technology Development." *Lex Publica* 7, no. 2 (2020): 24-43.

2. Peer review process ____ #2



Ahmad Syaufi <asyaufi.fh.unlam@gmail.com>

[IJCC] Decision - Revisions Required

Editor IJCC <Editor@cybercrimejournal.com>

2 Februari 2023 pukul 21.28

Kepada: Ahmad Syaufi <asyaufi.fh.unlam@gmail.com>

Dear Syaufi,

We have reached a decision regarding your submission to International Journal of Cyber Criminology, "Employing Forensic Techniques in Proving and Prosecuting Cross-border Cyber-financial Crimes".

Our decision is to: Revisions Required

Submission URL:

<https://cybercrimejournal.com/menuscrypt/index.php/cybercrimejournal/authorDashboard/submission/136>

Username: asyaufi

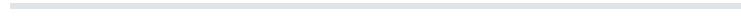
Reviewers have reviewed and commented on your submitted manuscript. They advise the author(s) to revise the manuscript. Their comments are attached to the email and/or to the bottom of this letter. If not, for your convenience log onto your profile to view the reviewers' comments.

Please revise and upload the revised manuscript and all documents required. The author has 14 days from now to revise the manuscript.

If you have any questions, please contact me.

Thank you for considering this journal as a venue for your work.

Best regards,



International Journal of Cyber Criminology
<https://www.cybercrimejournal.com/>



Ahmad Syaufi <asyaufi.fh.unlam@gmail.com>

[IJCC] Revised Version Acknowledgement

Editor IJCC <Editor@cybercrimejournal.com>

10 Februari 2023 pukul 14.11

Kepada: Ahmad Syaufi <asyaufi.fh.unlam@gmail.com>

Dear Syaufi,

Thank you for submitting the revision of manuscript, "Employing Forensic Techniques in Proving and Prosecuting Cross-border Cyber-financial Crimes" to International Journal of Cyber Criminology. With the online journal management system that we are using, you will be able to track its progress through the editorial process by logging in to the journal web site:

Submission URL:

<https://cybercrimejournal.com/menuscript/index.php/cybercrimejournal/authorDashboard/submission/136>

Username: asyaufi

If you have any questions, please contact me.

Thank you for considering this journal as a venue for your work.

Best regards,

International Journal of Cyber Criminology

<https://www.cybercrimejournal.com/>

Reviewer 2:

I think the paper is good. It only needs to be proofread by native speakers or certified experts.

Responses:

The paper has been proofread natively to increase readability. Please check the revised manuscript.

Employing Forensic Techniques in Proving and Prosecuting Cross-border Cyber-financial Crimes

Abstract

Cyber-financial crimes across borders pose a big challenge to law enforcement, particularly in developing countries like Indonesia. They affect the economy, society and the financial sector, thus forensic techniques are essential in their investigation and prosecution. This study aims to explore the significance of forensic techniques in prosecuting cross-border cyber-financial crimes in Indonesia, discussing the legal basis for digital forensic investigations, the police's role, and the challenges they face. The research employed a qualitative method and investigated Forensic Techniques and Cross-Border Cyber-Financial Crimes by comprehensively searching relevant scholarly publications including academic journals, reports, and books using various academic databases and screening the studies based on their relevance and quality. This study shows that forensic techniques are crucial for tackling cyber-financial crimes across borders in Indonesia. Law enforcement must have a legal grounding and expertise in digital forensic investigations, from collecting to presenting evidence in court. However, there are challenges such as insufficient resources, training, and cooperation between countries that law enforcers face. This study emphasizes the significance of using forensic techniques to address cross-border cyber-financial crimes in Indonesia. It underscores the importance of law enforcement agencies having a legal basis and knowledge of digital forensics investigations and the role of police and law enforcers.

Keywords: Forensic Techniques, Financial Crimes, Cyber Crimes, Indonesia

I. INTRODUCTION

In recent years, cyber-financial crimes across borders have become a significant challenge for law enforcement agencies worldwide, including in

developing countries such as Indonesia (Mauladi, Laut Merta Jaya, & Esquivias, 2022; Mentari & Hudi, 2022). These crimes not only impact the financial sector but also have adverse effects on the economy and society as a whole. Forensic techniques have proven to be essential in the investigation and prosecution of these types of crimes.

The law plays a vital role in investigating and prosecuting cross-border cyber-financial crimes. In Indonesia, the legal basis for conducting digital forensic investigations is provided by Law No. 19 of 2016 on Electronic Information and Transactions (ITE Law). This law provides the legal framework for the collection and presentation of digital evidence in court. It also establishes the responsibilities and obligations of law enforcement agencies in investigating cyber-crimes.

Evidently, there is an immediate requirement for advanced forensic methodologies when confronting cyber-financial crimes transferred across borders but particularly so among countries such as Indonesia, struggling to overcome this challenge. The present research concentrates on revealing how significant forensic techniques are when prosecuting instances arising from cross-border cyber-financial crime within Indonesia.

From examining our investigations findings, it remains evident that leveraging forensics proficiency becomes crucial towards overcoming the numerous challenges faced by law enforcers in charge of these complex cases. As we strive to make progress against cross-border cyber-criminal activity tarnishing our institutions' reputation and harming financial interests, both legal restrictions and digital forensics capabilities are essential standards we must strive towards. Without stakeholders cooperating closely enough to develop robust strategies aimed at prevention efforts while investigating and tracking down those responsible until their prosecution becomes possible could be far-fetched. Therefore, this study aims to explore the significance of forensic techniques in prosecuting cross-border cyber-financial crimes in Indonesia, discussing the legal basis for digital forensic investigations, the role of the police, and the challenges they face.

II. LITERATURE REVIEW

Cyber-Financial Crimes

According to McGuire & Dowling (2013), cybercrime can be defined as the use of computer networks to commit illegal activities such as theft, fraud, and other crimes. It's essential not to overlook the spike in cybercrime which has materialized as a worthy concern recently - ultimately jeopardizing individuals', organizations' & nations' wellbeing worldwide. Meanwhile - Financial crimes aren't far behind either- referring to nefarious agendas associated with monetary gains by any means necessary even if it ultimately harms an individual or institution involved. Such crimes can manifest itself through actions like bribery money laundering fraudulent transactions etc leading to mismanagement of funds both at an individual level or on large scale commercial transactions within organizations around us today.

The intersection of cybercrime and financial crimes has led to the emergence of cyber-financial crimes. Rajput and Rajput (2020) defined cyber-financial crime as a type of illegal activity that occurs in a cyber environment with the intent of making financial gain. A plethora of cyber-financial criminal activities exists, including identity theft, phishing, malware attacks, and cyber-attacks on financial institutions. Nonetheless, assessing the scope and magnitude of these crimes remains an arduous task for law enforcement and regulatory bodies, particularly considering their occurrence across diverse jurisdictions. To address these complexities, Wang and Chen (2019) argue that a methodical approach that involves comprehending the cybercriminals' operational models, identifying emerging patterns, and developing effective prevention and detection mechanisms is necessary.

The role of cryptocurrencies in the escalating incidents of cyber-financial crimes is a growing concern. Cryptocurrencies' anonymous attributes make them an attractive option for cybercriminals engaged in financial fraud (Prayogo & Chornous, 2020). Renzi (2022) emphasizes the difficulties regulators and law enforcement officials face in investigating crypto-related cyber-financial crimes. Effective regulatory frameworks are essential to mitigate such crimes' impacts.

Forensic Techniques in Cybercrime Investigations

The investigation and prosecution of cybercrime have become increasingly complex due to the rise of technology and the use of the internet for criminal activities. Forensic techniques have been developed specifically for cybercrime investigations to collect and analyze digital evidence effectively. This literature review will examine relevant studies that provide an overview of the forensic techniques used in cybercrime investigations.

The collection of digital data is a crucial component of cybercrime investigations. A forensic investigation of electronic evidence requires the collection, preservation, analysis, and presentation of data. It is imperative that forensic investigators handle the data in a manner that does not unnecessarily alter or destroy evidence. Devices that generally store digital data, such as hard disk drives and flash drives, are classified as non-volatile memory and therefore are regularly selected as primary targets for data collection. A forensic investigation expert or appropriate agency should be used in all digital forensic investigations.

In the cybercrime investigation, various forensic techniques are employed to analyze the digital data collected. Data validation is a crucial forensic technique used to ensure the accuracy and completeness of digital evidence. The process of data validation entails confirming the precision and entirety of digitalized information to identify any potential tampering or malevolent modification. Data validation tools include hash function algorithms, checksums, and digital signatures.

Another technique used in cybercrime investigations is the analysis of the digital data through forensic software. Forensic software tools are designed to perform forensic examinations of electronic media, recover data from hard drives, disks, and tapes, and identify files and directories. They are also used to identify and decipher encrypted data and reveal hidden information that is not otherwise visible. Some popular forensic software tools include Encase, X-Ways, and FTK.

An important cybercrime investigation technique used to identify and track the criminal is the use of network forensics. The field of network forensics revolves around the acquisition and examination of network traffic data with the purpose of uncovering potential indicators of cybercrime. This discipline also offers insight into the origin and recipient of transmitted data, the nature of the data itself, and the temporal aspects of its transmission. Network forensics tools include Wireshark, NetworkMiner, and NetSleuth.

The analysis of internet artifacts is another critical forensic technique in cybercrime investigation. Internet artifacts consist of data that is generated and stored by the system or application used to access the internet, such as a browser history, cookies, bookmarks, and cached pages. The analysis of internet artifacts provides insight into the online activities of the suspect. Internet artifacts analysis tools include Internet Evidence Finder (IEF), Autopsy, and Internet Explorer.

The utilization of forensic methodologies in investigating cybercrime has undergone rapid development in response to the widespread exploitation of technology in the commission of illicit activities. The efficacy of these techniques is contingent upon multiple factors, including the nature of the cybercrime, the digital information procured, and the forensic equipment applied. Among these methods, the indispensable role of network forensics emerges as pertinent in identifying culpable parties, chiefly when the perpetrator's identity is not immediately apparent. Meanwhile, data validation and software analysis enable precise and dependable data collection, admissible in judicial proceedings, and instrumental in convicting cybercriminals.

Cross-border Cyber-Financial Crimes

Cross-border cyber-financial crimes have become an emerging threat to the global financial system, which has been heightened by the growing digital economy. These crimes are characterized by the use of technology to perpetrate fraudulent financial transactions across borders with minimal supervision, posing significant risks to financial stability and integrity. Therefore, understanding the

nature, scope, and impact of cross-border cyber-financial crimes is critical for developing effective prevention and response measures. This literature review aims to provide an overview of the current state of knowledge on cross-border cyber-financial crimes and their implications for the financial industry.

Theoretical perspectives on cross-border cyber-financial crimes have centered on the rational choice theory, which posits that criminal behavior is motivated by the desire for economic gain. This theory has been used to explain the increasing incidence of cybercrime in the financial sector, where the rewards are high, and the risks are relatively low. Cybercriminals exploit vulnerabilities in the financial infrastructure, such as weak cybersecurity measures, to execute fraudulent transactions across borders. As a result, they can evade detection and prosecution by crossing multiple jurisdictions.

The literature has identified several types of cross-border cyber-financial crimes, such as phishing, identity theft, wire fraud, insider trading, and market manipulation. Phishing involves luring individuals to disclose sensitive financial information through fraudulent emails or websites. Identity theft involves stealing personal information to gain access to financial accounts. Wire fraud involves using digital means to transfer funds fraudulently. Insider trading involves the use of insider information to make financial gains, while market manipulation involves manipulating financial markets through the use of false information.

The effects of cross-border cyber-financial crimes on the global financial system can be severe. They can lead to financial losses for individuals, businesses, and financial institutions and damage the reputation of the financial industry (Hasbullah, 2022). These crimes can also undermine financial stability and integrity by eroding public confidence in the financial system and reducing investor trust. Additionally, they can facilitate the financing of other criminal activities, such as terrorism and money laundering, by providing a means to move illicit funds across borders.

Preventing and mitigating cross-border cyber-financial crimes require a coordinated effort across multiple jurisdictions, sectors, and stakeholders. The literature has identified several strategies for addressing these crimes, such as

enhancing cybersecurity measures, strengthening regulatory frameworks, increasing international cooperation, and investing in technology and innovation. Also, educating the public on how to identify and avoid cyber risks can go a long way in preventing these crimes.

Despite the growing attention given to cross-border cyber-financial crimes, some gaps exist in the literature. For instance, there is a need for more empirical research to provide a better understanding of the nature, scope, and impact of these crimes and to evaluate the effectiveness of preventive measures. Additionally, more research is needed to identify emerging risks, such as the use of cryptocurrencies and blockchain technology, and to develop appropriate responses to mitigate such risks (Wardani et al., 2022).

Digital Forensic Investigations in Indonesia

Cybercrime in Indonesia is a growing concern that needs urgent attention. A study by Mauladi et al. (2022) reports that there has been a significant rise in cybercrime cases in Indonesia in recent years. The study shows that the most prevalent cybercrime cases in Indonesia are related to hacking, phishing, and identity theft. The study highlights the need for sophisticated digital forensic investigations to combat the issue of cybercrime in Indonesia.

In addition, the study by Tewari et al. (2020) highlights the challenges of digital forensic investigations in Indonesia. The study concludes that there is a lack of awareness among law enforcement agencies and cybersecurity professionals on digital forensics. Furthermore, there is a lack of local talent and resources to conduct digital forensic investigations in Indonesia.

Another study by Paryudi et al. (2015) emphasizes the importance of digital forensics in Indonesia. The study reports that digital forensic investigations are critical in the fight against cybercrime. The study highlights the role of digital forensic investigations in investigating data breaches, cyber-attacks, and other crimes committed using digital devices and networks.

Moreover, the study by Choo (2008) also highlights the challenges of digital forensics in Indonesia. The study observes that the Indonesian legal system is not adequately equipped to handle digital evidence. There is a lack of legal frameworks and regulations on digital evidence, leading to challenges in the admissibility of digital evidence in courts.

Furthermore, the study by Subektiningsih & Hariyadi (2019) highlights the need for training on digital forensics in Indonesia. The study reports that there is a need for cybersecurity professionals to have the necessary skills and knowledge to conduct digital forensic investigations. Furthermore, the study highlights the need for standardization in digital forensic investigations to ensure the accuracy and reliability of findings.

Another critical challenge facing digital forensics in Indonesia is the lack of collaboration between law enforcement agencies and private sector organizations. The study by Prayudi and Riadi (2018) highlights the need for public-private partnerships in digital forensics in Indonesia. The study observes that by collaborating, law enforcement agencies can tap into the resources and expertise of private sector organizations to improve their digital forensic capabilities.

The use of forensic techniques in proving and prosecuting cross-border cyber-financial crimes in Indonesia is governed by the Indonesian Criminal Procedure Code (Army, 2020). There are also other laws that address specific types of cyber offences, such as the Electronic Information and Transactions Law and the Money Laundering Law. Law enforcement agencies must ensure the digital evidence they collect is lawful and presents it in court to a certain level of evidentiary standard.

The police and law enforcers play a crucial role in investigating and prosecuting cross-border cyber-financial crimes in Indonesia. They must be equipped with the appropriate digital forensic tools and techniques to gather evidence and engage in collaboration with their counterparts in other countries. The police and law enforcers also need specific training and education to stay abreast with the ever-changing nature of cybercrime.

III. RESEARCH METHODOLOGY

Though this study uses a legal-normative methodology, it won't examine the law in isolation from its social environment. Instead, it will analyze the law in connection to society. Ricoeur's (Xavier & Escach-Dubourg, 2022) hermeneutic ideas suggest that legal norms present in regulatory texts are not just static meaning, but lively and dynamic language events or discourse. As such, interpreting texts on their own isn't sufficient for legal research since texts are contextually linked to multiple interpretations. Therefore, researchers must understand the contextual meaning of texts and regulatory language (Wiratraman, 2019). Posner (2000) claims that this study adopts a comprehensive legal methodology, where the law isn't only defined as a collection of norms but as also significant to the social effects of setting norms (law). Thus, the significance of social backgrounds will be stressed (Creutzfeldt, Mason, & McConnachie, 2019). For that reason, this study will consider the law's textual form and its manifestation as ideological, philosophical, and moralistic legal conceptions such as ideas, ideals, values, morals, and justice.

IV. RESULTS AND DISCUSSION

Significance of forensic techniques in prosecuting cross-border cyber-financial crimes in Indonesia

The use of forensic techniques in prosecuting cross-border cyber-financial crimes has been a significant topic of discussion in recent years, especially as the prevalence of cybercrime continues to increase. A recent research article delves into the specifics of this issue in the context of Indonesia and offers some interesting insights into the importance of forensic analysis in the successful prosecution of cross-border cyber-financial crimes (Dioza, 2019).

The emergence of new financial technologies such as digital currencies has also contributed to the increase in cyber-financial crimes. These crimes are characterized by their cross-border nature and have a significant impact on global

financial systems. Therefore, it is important for law enforcement agencies to have the necessary tools and techniques to investigate and prosecute these crimes.

Forensic techniques play a crucial role in identifying the digital evidence required to support criminal investigations and prosecutions (Rao & Satpathy, 2020). These techniques involve the use of specialized software and hardware tools to extract, preserve, and analyze digital data. The data obtained through forensic analysis can provide critical information that can be used to identify and track down cybercriminals. The hackers used a sophisticated botnet to carry out the attacks, and they also employed several other techniques to evade detection (Vinayakumar et al., 2020).

The Indonesian police were able to apprehend the hackers using a combination of traditional investigative techniques and forensic analysis (Aditya et al., 2021; Sukardi, 2022). Forensic analysis played a critical role by identifying critical information such as IP addresses, transaction logs, and system logs that were used to trace the source of the attacks and link the hackers to the crime. The analysis also revealed several other details about the attacks, such as the botnet used and the methods employed to evade detection.

The case study highlights the importance of forensic analysis in prosecuting cross-border cyber-financial crimes. Had the Indonesian police not used these techniques, it may have been impossible to trace the source of the attacks, apprehend the hackers, or recover the stolen funds. The authors argue that forensic techniques should be a standard investigative tool for law enforcement agencies worldwide to combat cybercrime effectively.

Therefore, needs to be emphasized investment in forensic tools and techniques to assist law enforcement agencies in combating cybercrime. Furthermore, it calls for more international cooperation among law enforcement agencies to investigate and prosecute cross-border cyber-financial crimes. The article also highlights the need to develop better legislation to address the complexity of these crimes.

Forensic techniques have a significant importance in prosecuting cross-border cyber financial crimes in Indonesia. This is related to the laws in Indonesia that govern cyber financial crimes. Law No. 19 of 2016 on Amendments to Law No. 11 of 2008 on Electronic Information and Transactions (ITE) provides regulations on the types of cyber financial crimes that are prohibited in Indonesia. These types of crimes include data theft, fraud, and identity theft. In prosecuting cross-border cyber financial crimes, forensic techniques are essential to find digital evidence. This digital evidence is key to legitimately and fairly prosecute perpetrators of crimes.

Forensic techniques have the ability to recover digital data that has been deleted or damaged by criminals. In addition, this technique can also identify the IP addresses of perpetrators and confirm whether the collected data is valid or not. Cross-border cyber financial criminals often delete their digital tracks or use complex digital fraud techniques. Therefore, forensic techniques are important in finding suspicious or false digital evidence. In cases of cross-border cyber financial crimes, forensic techniques help the investigation and prosecution process by sharpening digital evidence. These valid digital evidence are later the strong basis for prosecutors to legitimately and fairly prosecute perpetrators of crimes.

Legal basis for digital forensic investigations in Indonesia

The digital age has brought significant changes in the way societies operate, communicate, and exchange information. It has also opened up avenues for criminal activities such as cyber stalking, identity theft, and child pornography. As such, digital forensic investigations have become an essential tool in modern-day law enforcement. However, the legality of such investigations remains a subject of debate in many countries worldwide. In Indonesia, the law regulating digital forensic investigations is still a relatively new concept.

Indonesia is a country with a large population, diverse religions, and ethnicities. The digital age is rapidly expanding in Indonesia, with a current

internet penetration rate of 77.02% in 2022 (APJII, 2022). The trend of internet penetration in Indonesia has been increasing year by year. According to Irawati (2021), there are no specific regulations governing the use of digital forensics in Indonesia as it is still a new and emerging field of study. This could be due to the fast evolution of digital technologies, making it challenging for lawmakers to keep up with the latest advancements in the field.

However, there are several laws and regulations that could be applicable to the use of digital forensics in Indonesia. One of these is the Criminal Procedure Code (KUHAP), which sets out the rules for investigating criminal cases, including the use of digital forensics. For instance, article 81 of the KUHAP permits the use of electronic evidence in criminal proceedings, provided that the evidence was obtained legally and meets certain standards of authenticity, reliability, and relevance.

Another law that could be relevant to digital forensics in Indonesia is the Law on Electronic Information and Transactions (ITE Law). This law was established to regulate and protect electronic transactions and the use of electronic information in Indonesia. It covers various issues such as data protection, cybercrime, and offenses related to online activities. Under the ITE Law, digital forensics can be used as evidence in court proceedings, but only if the data has been obtained legally and in accordance with the provisions of the law.

While these laws provide some guidance for digital forensic investigations, they are not specifically designed to regulate such investigations. Additionally, the lack of specific regulations on digital forensics means that there may be inconsistencies in how the law is applied in different cases. For example, the use of digital forensics may be accepted in one court case but rejected in another case.

The absence of specific regulations on digital forensics poses a challenge for law enforcement officers who may be unsure of the boundaries and limitations of digital forensic investigations. It also creates opportunities for abuse and misuse of digital forensics, which could potentially violate the rights of citizens, including the right to privacy.

To address these challenges, suggests that Indonesia needs to develop specific regulations that govern the use of digital forensics. Such regulations should provide clear guidelines for the collection, handling, and analysis of digital evidence, including the legal basis for such investigations. The regulations should also address issues related to data privacy and protection, chain of custody, and the admissibility of evidence in court.

Indonesia has a strong legal basis for conducting digital forensic investigations in handling information and communication technology crimes, as regulated by Law No. 11 of 2008 on Electronic Information and Transactions, Law No. 8 of 2010 on Prevention and Eradication of Money Laundering Crimes, Law No. 19 of 2016 on Guidelines for Opening and/or Closing Access to Information on the Internet, and Presidential Regulation No. 1 of 2014 on the Task Force for Handling Crimes in the Field of Information and Communication Technology, which provide provisions regarding electronic crimes, the use of digital evidence as valid evidence, the opening and closing of access to information on the internet, as well as the formation of a task force responsible for investigating, enforcing, and preventing crimes in the field of information and communication technology.

The Electronic Information and Transactions Law regulates offenses related to electronic information and transactions, such as online defamation, dissemination of false information, and other cyber crimes (Yanto, 2020). The Electronic Information and Transactions Law also gives law enforcement agencies the authority to investigate the crimes. Meanwhile, the Money Laundering Crime Prevention and Eradication Law provides provisions for the prevention and eradication of money laundering crimes (Wardani et al., 2022). In the case of digital investigations into money laundering crimes, law enforcement agencies can use digital evidence as valid evidence. Law No. 19 of 2016 provides provisions for the opening and closing of access to information on the internet. This can serve as a basis for law enforcement agencies to investigate crimes committed through the internet. The Presidential Regulation establishes the Task Force for Handling Crimes in the Field of Information and Communication

Technology, which is responsible for investigating, enforcing, and preventing crimes in the field of information and communication technology. The task force works in an integrated manner with other law enforcement agencies in exposing and handling crimes in the field of information and communication technology.

Police roles and responsibilities in investigating and prosecuting cyber-financial crimes

The proliferation of cyber-financial crimes represents a significant challenge for law enforcement agencies worldwide. These crimes are characterized by their complex and multi-jurisdictional nature and require specialized skills and training to investigate and prosecute. In recent years, there has been a growing body of research examining the roles and responsibilities of police in investigating and prosecuting cyber-financial crimes.

This study identified several key roles that police play in investigating cyber-financial crimes. First, police are responsible for collecting and analyzing evidence related to the crime. This involves not only seizing electronic devices but also examining financial records and tracing financial transactions. Second, police are responsible for identifying and locating suspects. This requires a comprehensive understanding of the online platforms and technologies that criminals use to perpetrate these crimes. Third, police are responsible for building a case against the suspect. This requires a thorough understanding of the legal framework related to cyber-financial crimes, as well as strong analytical and communication skills.

This study also identified several challenges faced by police in investigating and prosecuting cyber-financial crimes. One major challenge is the lack of resources and specialized training. Many police officers lack the technical skills and knowledge necessary to investigate these crimes effectively. Additionally, there is a need for cooperation between different agencies and jurisdictions, as cyber-financial crimes often involve international borders. Furthermore, the study found that there is a lack of public awareness and education on the dangers of

cyber-financial crimes, which can impede police efforts to investigate and prosecute these crimes.

Despite these challenges, this study identified several successful strategies that police have implemented to investigate and prosecute cyber-financial crimes. One strategy is the establishment of specialized units that focus solely on cyber-financial crimes. These units have the necessary technical skills and expertise to effectively investigate and prosecute these complex crimes. Additionally, the study found that successful investigations often involve a combination of traditional investigation techniques, such as interviews and surveillance, as well as advanced forensic techniques, such as computer analysis.

In Indonesia, the regulation that supports the police in investigating and prosecuting cyber-financial crimes is the Electronic Information and Transactions (ITE) Law. This law provides a framework for regulating online activities and sets out the legal framework for investigating and prosecuting cyber-crimes. Specifically, it criminalizes a range of cyber-crimes, such as hacking, spamming, identity theft, and online fraud.

Under the ITE Law, the police have the power to investigate and prosecute cyber-crimes, and can also take measures to prevent further damage or harm caused by these crimes. They can also work with other agencies such as the Cyber Crime Investigation and Analysis Center (CCCIAC) and the National Cyber and Encryption Agency (BSSN) to investigate and prevent cyber-crimes.

Challenges faced by law enforcers in tackling cross-border cyber-financial crimes

Several challenges encountered by law enforcers in preventing and prosecuting cross-border cyber-financial crimes. The challenges were classified into four main categories, including jurisdictional issues, legal complexities, technology advancements, and inadequate resources.

Jurisdictional challenges refer to the difficulty of obtaining evidence from foreign countries, where cyber-criminals operate, and where data protection and

privacy regulations may not allow for access to such evidence. The lack of cooperation between jurisdictions, particularly in identifying cyber-criminals residing in different jurisdictions, adds to the complexity of cross-border cyber-financial crime investigations. Criminals often take advantage of this weak link to commit crimes across different jurisdictions, leaving investigators often unable to track and prosecute them effectively.

Legal complexities are another major challenge faced in tackling cyber-financial crimes as different countries have distinct legal frameworks and regulations that apply to these crimes. These complexities create impediments for international data sharing and extradition processes, making it difficult for investigators to get hold of the necessary information and evidence required for prosecutions. A lack of legal coherence between countries creates clear loopholes that allow cyber-criminals to thrive and engage in illicit activities unchecked.

Technology advancements prove to be a game-changer in the world of cyber-financial crime and pose a significant challenge to law enforcement agents in their efforts to combat criminals. The perpetrators exploit vulnerabilities in evolving technologies, such as the dark web, and blockchain, to launch complex and sophisticated attacks and evade detection. Traditional methods and approaches are often not enough to combat the ever-advancing techniques of these criminals. Law enforcement agencies need to continually develop their skills and learn new technologies to keep pace with criminals' cunning means.

Finally, inadequate resources were identified as a significant hurdle for law enforcement agents combating cyber-financial crimes. Insufficient funding and staff shortages lead to a lack of capacity to handle cybercrime investigations and counteract evolving tactics developed by these criminals. Without adequate resources, law enforcement agencies' ability to track cyber-criminals dwindles, making it easier for cyber-criminals to rapidly adapt, propagate and execute cyber attacks.

This study also proposes measures that can be taken to overcome these challenges. Some suggestions include creating an international framework for cyber-financial crime investigation, sharing intelligence and training among

different law enforcement agencies worldwide. In addition, Experts recommend advancing law enforcement efforts through technical tools such as artificial intelligence and big data analytics, and investing in the adequate resources, particularly technological advancement resources required for enhancing cybercrime investigations.

V. CONCLUSION

The study provides valuable insights into the importance of forensic techniques in prosecuting cross-border cyber-financial crimes. It highlights the critical role of forensic analysis in identifying digital evidence required for criminal investigations and prosecutions. The case study presented illustrates the significance of these techniques in tracing the source of cyber-attacks and linking hackers to the crimes committed. The study also calls for more investment in forensic tools and techniques and better legislation to address the complexity of these crimes, emphasizing the need for international cooperation among law enforcement agencies. Although there are some laws and regulations that apply to digital forensic investigations in Indonesia, they are not sufficient for regulating the growing industry. As such, the need for clear and specific laws is crucial to establish the standards and procedures for digital forensics. This will ensure the legality and reliability of digital evidence in the criminal justice system, promote consistency in the application of the law across different cases, and ultimately uphold citizens' rights to privacy.

This study provides valuable insights into the roles and responsibilities of police in investigating and prosecuting cyber-financial crimes. The study highlights the challenges faced by police in effectively investigating these crimes, but also identifies successful strategies that can be adopted to address these challenges. It is clear that cyber-financial crimes represent a growing threat to individuals and organizations around the world, and it is essential for law enforcement agencies to continue to develop the skills and expertise necessary to effectively combat these crimes. The police play a crucial role in investigating and prosecuting cyber-financial crimes in Indonesia, and the regulations in place

support their efforts to combat these crimes. It is important for individuals and organizations to be aware of the risks of cyber-financial crimes and take appropriate security measures to protect themselves from such crimes. This study highlighted the significant challenges facing law enforcement agents in tackling cross-border cyber-financial crimes. These obstacles ranged from jurisdictional, legal, technological, to inadequate resources that hamper the investigation, prosecution, and prevention of these crimes. However, the research proved that there has recently been a growing trend towards international collaboration and cooperation between law enforcement agencies and stakeholders in jointly addressing cyber-financial crimes. Whilst overcoming these challenges will be no easy feat, it is essential that actions be taken to counter these challenges to tackle and prevent financially motivated cyber-crimes across borders worldwide.

References

- Aditya, A. D. P., Uning, P., & Syafridatati, S. (2021). *Penggunaan Digital Forensik dalam Pengungkapan Kasus Penghinaan di Internet (Studi Kasus di Polda Sumatera Barat)* (Doctoral dissertation, Univeristas Bung Hatta).
- Army, E. (2020). *Bukti Elektronik Dalam Praktik Peradilan*. Sinar Grafika.
- Asosiasi Penyelenggara Jasa Internet Indonesia (APJII). (2022). Penetrasi Internet Indonesia. [https://databoks.katadata.co.id/datapublish/2022/06/10/apjii-penetrasi-internet-indonesia-capai-7702-pada-2022#:~:text=Asosiasi%20Penyelenggara%20Jasa%20Internet%20Indonesia%20\(APJII\)%20baru%20saja%20merilis%20laporan,02%25%20pada%202021%2D2022](https://databoks.katadata.co.id/datapublish/2022/06/10/apjii-penetrasi-internet-indonesia-capai-7702-pada-2022#:~:text=Asosiasi%20Penyelenggara%20Jasa%20Internet%20Indonesia%20(APJII)%20baru%20saja%20merilis%20laporan,02%25%20pada%202021%2D2022).
- Choo, K. K. R. (2008). Organised crime groups in cyberspace: a typology. *Trends in organized crime*, 11, 270-295.
- Creutzfeldt, N., Mason, M., & McConnachie, K. (Eds.). (2019). *Routledge handbook of socio-legal theory and methods*. Routledge.
- Dioza, R. (2019). *Kebijakan Kriminal Penanganan Cyber Crime Pada Satuan Reserse Kriminal Polres Aceh Tenggara* (Doctoral dissertation).

- Hasbullah, M. A. (2022). Identifying the Effects of Cybercrime on Business Laws: Implications for Businesses and Consumers. *International Journal of Cyber Criminology*, 16(2), 119-130.
- Irawati, A., Fadholi, H. B., Alamsyah, A. N., Dwipayana, D. P., & Muslih, M. (2021, August). Urgensi Cyber Law dalam Kehidupan Masyarakat Indonesia Di Era Digital. In *Proceeding of Conference on Law and Social Studies*.
- Mauladi, K. F., Laut Mertha Jaya, I. M., & Esquivias, M. A. (2022). Exploring the link between cashless society and cybercrime in Indonesia. *Journal of Telecommunications and the Digital Economy*, 10(3), 58-76.
- McGuire, M., & Dowling, S. (2013). Cyber crime: A review of the evidence. *Summary of key findings and implications. Home Office Research report*, 75, 1-35.
- Mentari, N., & Hudi, N. (2022, April). Prevention of Financial Crime after Covid 19. In *Ahmad Dahlan International Conference on Law and Social Justice* (Vol. 1, No. 1).
- Posner, E. A. (2000). Law and social norms: The case of tax compliance. *Virginia Law Review*, 1781-1819.
- Prayogo, G., & Chornous, Y. (2020). Conceptualization of Future Cryptocurrency Laws in Indonesia and Ukraine. *Lex Publica*, 7(2), 56-68.
- Prayudi, Y., & Riadi, I. (2018). Digital Forensics Workflow as A Mapping Model for People, Evidence, and Process in Digital Investigation. *International Journal of Cyber-Security and Digital Forensics*, 7(3), 294-305.
- Prayudi, Y., Ashari, A., & Priyambodo, T. K. (2015). A proposed digital forensics business model to support cybercrime investigation in Indonesia. *International Journal of Computer Network and Information Security*, 7(11), 1-8.
- Rajput, B., & Rajput, B. (2020). Exploring the Phenomenon of Cyber Economic Crime. *Cyber Economic Crime in India: An Integrated Model for Prevention and Investigation*, 53-78.

- Rao, M. S., & Satpathy, S. C. (2020). Digital Forensics and Digital Investigation to Form a Suspension Bridge Flanked by Law Enforcement, Prosecution, and Examination of Computer Frauds and Cybercrime. In *Big Data Analytics and Computing for Digital Forensic Investigations* (pp. 21-41). CRC Press.
- Renzi, C. (2022). *Money Laundering Plus Cybercrime Equals Cyber-Laundering: How Institutions Can Balance the Equation* (Doctoral dissertation, Utica University).
- Subektiningsih, S., & Hariyadi, D. (2022). The Role of Digital Forensic Experts in Cybercrime Investigations in Indonesia Based on The Scopus Research Index. *Building of Informatics, Technology and Science (BITS)*, 4(3), 1665-1670.
- Sukardi, S. (2022). Reconstruction of Financial Crime Investigation Methods in Law Enforcement in The Era of the Industrial Revolution 4.0. *Unnes Law Journal: Jurnal Hukum Universitas Negeri Semarang*, 8(1), 133-158.
- Vinayakumar, R., Alazab, M., Srinivasan, S., Pham, Q. V., Padannayil, S. K., & Simran, K. (2020). A visualized botnet detection system based deep learning for the internet of things networks of smart cities. *IEEE Transactions on Industry Applications*, 56(4), 4436-4456.
- Wang, J., & Chen, J. (2019, October). Preventing Financial Illegality and Crime by Using Internet Technology. In *2019 3rd International Conference on Data Science and Business Analytics (ICDSBA)* (pp. 206-212). IEEE.
- Wardani, Andhira, Mahrus Ali, and Jaco Barkhuizen. "Money Laundering through Cryptocurrency and Its Arrangements in Money Laundering Act." *Lex Publica* 9, no. 2 (2022): 49-66.
- Wiratraman, H. P. (2019). The challenges of teaching comparative law and socio-legal studies at Indonesia's law schools. *Asian Journal of Comparative Law*, 14(S1), S229-S244.
- Xavier, B. I. O. Y., & Escach-Dubourg, T. (2022). A Hermeneutic Reading of Law and Legal Theory: Regarding Paul Ricœur. *Meta-theory of Law*, 235.

Yanto, Oksidelfa. "Criminal Charges and Sanctions on Defamation Crime as Cyber Crime in the Information Technology Development." *Lex Publica* 7, no. 2 (2020): 24-43.

4. Acceptance & Galley proof



Ahmad Syaufi <asyaufi.fh.unlam@gmail.com>

[IJCC] Decision - Accept Submission

Editor IJCC <Editor@cybercrimejournal.com>

23 Maret 2023 pukul 14.58

Kepada: Ahmad Syaufi <asyaufi.fh.unlam@gmail.com>

Dear Syaufi,

We have reached a decision regarding your submission to International Journal of Cyber Criminology, "Employing Forensic Techniques in Proving and Prosecuting Cross-border Cyber-financial Crimes".

Our decision is to: Accept Submission

Submission URL:

<https://cybercrimejournal.com/menuscrypt/index.php/cybercrimejournal/authorDashboard/submission/136>

Username: asyaufi

If you have any questions, please contact me.

Thank you for considering this journal as a venue for your work.

Best regards,

International Journal of Cyber Criminology

<https://www.cybercrimejournal.com/>



Ahmad Syaafi <asyaafi.fh.unlam@gmail.com>

[IJCC] Send to Production

Editor IJCC <Editor@cybercrimejournal.com>

26 Maret 2023 pukul 15.56

Kepada: Ahmad Syaafi <asyaafi.fh.unlam@gmail.com>

Dear Syaafi,

Congratulations on the acceptance of your manuscript, "Employing Forensic Techniques in Proving and Prosecuting Cross-border Cyber-financial Crimes" in International Journal of Cyber Criminology. Your manuscript is now being prepared for production. With the online journal management system that we are using, you will be able to track its progress through the editorial process by logging in to the journal web site:

Submission URL:

<https://cybercrimejournal.com/menuscript/index.php/cybercrimejournal/authorDashboard/submission/136>

Username: asyaafi

If you have any questions, please contact me.

Thank you for considering this journal as a venue for your work.

Best regards,

International Journal of Cyber Criminology

<https://www.cybercrimejournal.com/>



Copyright © 2023 International Journal of Cyber Criminology –ISSN: 0974–2891
January –June 2023. Vol. 17(1): 72–85. DOI: 10.5281/zenodo.4766605
Publisher & Editor-in-Chief –K. Jaishankar / Open Access (Authors / Readers No Pay Journal).
This is a Diamond Open Access article distributed under the terms of the Creative Commons Attribution-NonCommercial-ShareAlike 4.0 International (CC-BY-NC-SA 4.0) License, which permits unrestricted non-commercial use, distribution, and reproduction in any medium, provided the original work is properly cited.



Employing Forensic Techniques in Proving and Prosecuting Cross-Border Cyber-Financial Crimes

Ahmad Syaufi¹

Universitas Lambung Mangkurat, Indonesia

Mursidah²

SMAN 8 Banjarmasin, Indonesia

Aurora Fatimatuz Zahra³

Universitas Muhammadiyah Yogyakarta, Indonesia

Fatham Mubina Iksir Gholi⁴

Universitas Diponegoro, Indonesia

Abstract

Cyber-financial crimes across borders pose a big challenge to law enforcement, particularly in developing countries like Indonesia. They affect the economy, society and the financial sector, thus forensic techniques are essential in their investigation and prosecution. This study aims to explore the significance of forensic techniques in prosecuting cross-border cyber-financial crimes in Indonesia, discussing the legal basis for digital forensic investigations, the police's role, and the challenges they face. The research employed a qualitative method and investigated Forensic Techniques and Cross-Border Cyber-Financial Crimes by comprehensively searching relevant scholarly publications including academic journals, reports, and books using various academic databases and screening the studies based on their relevance and quality. This study shows that forensic techniques are crucial for tackling cyber-financial crimes across borders in Indonesia. Law enforcement must have a legal grounding and expertise in digital forensic investigations, from collecting to presenting evidence in court. However, there are challenges such as insufficient resources, training, and cooperation between countries that law enforcers face. This study emphasizes the significance of using

¹ Faculty of Law, Universitas Lambung Mangkurat, Indonesia
Email: asyaufi.fh.unlam@gmail.com (Corresponding Author)

² SMAN 8 Banjarmasin, Indonesia

³ Faculty of Law, Universitas Muhammadiyah Yogyakarta, Indonesia

⁴ Faculty of Law, Universitas Diponegoro, Indonesia

forensic techniques to address cross-border cyber-financial crimes in Indonesia. It underscores the importance of law enforcement agencies having a legal basis and knowledge of digital forensics investigations and the role of police and law enforcers.

Keywords: *Forensic Techniques; Cyber-Financial Crimes; Cyber Crimes, Indonesia*

Introduction

In recent years, cyber-financial crimes across borders have become a significant challenge for law enforcement agencies worldwide, including in developing countries such as Indonesia (Mauladi, Laut Merta Jaya, & Esquivias, 2022; Mentari & Hudi, 2022). These crimes not only impact the financial sector but also have adverse effects on the economy and society as a whole. Forensic techniques have proven to be essential in the investigation and prosecution of these types of crimes.

The law plays a vital role in investigating and prosecuting cross-border cyber-financial crimes. In Indonesia, the legal basis for conducting digital forensic investigations is provided by Law No. 19 of 2016 on Electronic Information and Transactions (ITE Law). This law provides the legal framework for the collection and presentation of digital evidence in court. It also establishes the responsibilities and obligations of law enforcement agencies in investigating cyber-crimes.

Evidently, there is an immediate requirement for advanced forensic methodologies when confronting cyber-financial crimes transferred across borders but particularly so among countries such as Indonesia, struggling to overcome this challenge. The present research concentrates on revealing how significant forensic techniques are when prosecuting instances arising from cross-border cyber-financial crime within Indonesia.

From examining our investigations findings, it remains evident that leveraging forensics proficiency becomes crucial towards overcoming the numerous challenges faced by law enforcers in charge of these complex cases. As we strive to make progress against cross-border cyber-criminal activity tarnishing our institutions' reputation and harming financial interests, both legal restrictions and digital forensics capabilities are essential standards we must strive towards. Without stakeholders cooperating closely enough to develop robust strategies aimed at prevention efforts while investigating and tracking down those responsible until their prosecution becomes possible could be far-fetched. Therefore, this study aims to explore the significance of forensic techniques in prosecuting cross-border cyber-financial crimes in Indonesia, discussing the legal basis for digital forensic investigations, the role of the police, and the challenges they face.

Literature review

a. Overview of Cyber-Financial Crimes

Cybercrime has become a prevalent issue in recent years, posing significant threats to individuals, organizations, and governments worldwide. According to McGuire & Dowling (2013), cybercrime can be defined as the use of computer networks to commit illegal activities such as theft, fraud, and other crimes. Financial crimes, on

the other hand, refer to offenses committed for financial gain. Examples of financial crimes include money laundering, fraud, bribery, and embezzlement.

The intersection of cybercrime and financial crimes has led to the emergence of cyber-financial crimes. [Rajput and Rajput \(2020\)](#) defined cyber-financial crime as a type of illegal activity that occurs in a cyber environment with the intent of making financial gain. Cyber-financial crimes take many forms, including identity theft, cyber-attacks on financial institutions, phishing, and malware attacks.

One of the significant challenges facing law enforcement agencies and regulators is the difficulty in determining the extent and scope of cyber-financial crimes. This challenge is compounded by the fact that cyber-financial crimes occur across multiple jurisdictions, making it challenging to investigate and prosecute offenders. [Wang & Chen \(2019\)](#) argue that there is a need to develop a systematic approach to combatting cyber-financial crimes. This approach should include an understanding of the modus operandi of cybercriminals, the emerging trends, and the development of effective prevention and detection strategies.

Another emerging issue in the field of cyber-financial crimes is the role of cryptocurrencies. Cryptocurrencies provide a degree of anonymity that makes them attractive for cybercriminals engaged in financial crimes. [Renzi \(2022\)](#) note that the use of cryptocurrencies in cyber-financial crimes is a significant challenge for regulators and law enforcement agencies. There is a need for the development of effective regulatory frameworks that can address the challenges posed by cryptocurrencies.

b. Forensic Techniques in Cybercrime Investigations

The investigation and prosecution of cybercrime have become increasingly complex due to the rise of technology and the use of the internet for criminal activities. Forensic techniques have been developed specifically for cybercrime investigations to collect and analyze digital evidence effectively. This literature review will examine relevant studies that provide an overview of the forensic techniques used in cybercrime investigations.

One of the most critical stages in a cybercrime investigation is the collection of digital data. A digital forensic investigation involves the collection, preservation, analysis, and presentation of electronic evidence. The forensic investigator must ensure that the evidence is collected in a way that does not alter or destroy it. Non-volatile memory, such as hard disk drives and flash drives, typically store digital data and are the targets for collection. A forensic investigation expert or appropriate agency should be used in all digital forensic investigations.

In the cybercrime investigation, various forensic techniques are employed to analyze the digital data collected. Data validation is a crucial forensic technique used to ensure the accuracy and completeness of digital evidence. Data validation involves verifying the accuracy and completeness of digital data to determine whether or not it has been tampered with or maliciously altered. Data validation tools include hash function algorithms, checksums, and digital signatures.

Another technique used in cybercrime investigations is the analysis of the digital data through forensic software. Forensic software tools are designed to perform forensic examinations of electronic media, recover data from hard drives, disks, and

tapes, and identify files and directories. They are also used to identify and decipher encrypted data and reveal hidden information that is not otherwise visible. Some popular forensic software tools include Encase, X-Ways, and FTK.

An important cybercrime investigation technique used to identify and track the criminal is the use of network forensics. Network forensics involve the collection and analysis of network traffic data to identify possible evidence of a cybercrime. They also provide information on the source and destination of the data, the type of data being transmitted, and the time of transmission. Network forensics tools include Wireshark, NetworkMiner, and NetSleuth.

The analysis of internet artifacts is another critical forensic technique in cybercrime investigation. Internet artifacts consist of data that is generated and stored by the system or application used to access the internet, such as a browser history, cookies, bookmarks, and cached pages. The analysis of internet artifacts provides insight into the online activities of the suspect. Internet artifacts analysis tools include Internet Evidence Finder (IEF), Autopsy, and Internet Explorer.

The use of forensic techniques in cybercrime investigations has evolved due to the increasing use of technology to commit crimes. The effectiveness of each technique is largely dependent on the type of cybercrime committed, the digital data collected, and the forensic tools used. Network forensics is a crucial tool in identifying the criminal in cybercrime investigations, especially when the criminal's identity is not known. Data validation and forensic software analysis provide accurate and reliable information that can be used in court to support the investigation and prosecution of cybercrimes.

c. Cross-border Cyber-Financial Crimes

Cross-border cyber-financial crimes have become an emerging threat to the global financial system, which has been heightened by the growing digital economy. These crimes are characterized by the use of technology to perpetrate fraudulent financial transactions across borders with minimal supervision, posing significant risks to financial stability and integrity. Therefore, understanding the nature, scope, and impact of cross-border cyber-financial crimes is critical for developing effective prevention and response measures. This literature review aims to provide an overview of the current state of knowledge on cross-border cyber-financial crimes and their implications for the financial industry.

Theoretical perspectives on cross-border cyber-financial crimes have centered on the rational choice theory, which posits that criminal behavior is motivated by the desire for economic gain. This theory has been used to explain the increasing incidence of cybercrime in the financial sector, where the rewards are high, and the risks are relatively low. Cybercriminals exploit vulnerabilities in the financial infrastructure, such as weak cybersecurity measures, to execute fraudulent transactions across borders. As a result, they can evade detection and prosecution by crossing multiple jurisdictions.

The literature has identified several types of cross-border cyber-financial crimes, such as phishing, identity theft, wire fraud, insider trading, and market manipulation. Phishing involves luring individuals to disclose sensitive financial information through fraudulent emails or websites. Identity theft involves stealing personal

information to gain access to financial accounts. Wire fraud involves using digital means to transfer funds fraudulently. Insider trading involves the use of insider information to make financial gains, while market manipulation involves manipulating financial markets through the use of false information.

The effects of cross-border cyber-financial crimes on the global financial system can be severe. They can lead to financial losses for individuals, businesses, and financial institutions and damage the reputation of the financial industry. These crimes can also undermine financial stability and integrity by eroding public confidence in the financial system and reducing investor trust. Additionally, they can facilitate the financing of other criminal activities, such as terrorism and money laundering, by providing a means to move illicit funds across borders.

Preventing and mitigating cross-border cyber-financial crimes require a coordinated effort across multiple jurisdictions, sectors, and stakeholders. The literature has identified several strategies for addressing these crimes, such as enhancing cybersecurity measures, strengthening regulatory frameworks, increasing international cooperation, and investing in technology and innovation. Also, educating the public on how to identify and avoid cyber risks can go a long way in preventing these crimes.

Despite the growing attention given to cross-border cyber-financial crimes, some gaps exist in the literature. For instance, there is a need for more empirical research to provide a better understanding of the nature, scope, and impact of these crimes and to evaluate the effectiveness of preventive measures. Additionally, more research is needed to identify emerging risks, such as the use of cryptocurrencies and blockchain technology, and to develop appropriate responses to mitigate such risks.

d. Digital Forensic Investigations in Indonesia

Cybercrime in Indonesia is a growing concern that needs urgent attention. A study by [Rahmat et al. \(2023\)](#) reports that there has been a significant rise in cybercrime cases in Indonesia in recent years. The study shows that the most prevalent cybercrime cases in Indonesia are related to hacking, phishing, and identity theft. The study highlights the need for sophisticated digital forensic investigations to combat the issue of cybercrime in Indonesia.

In addition, the study by [Tewari et al. \(2020\)](#) highlights the challenges of digital forensic investigations in Indonesia. The study concludes that there is a lack of awareness among law enforcement agencies and cybersecurity professionals on digital forensics. Furthermore, there is a lack of local talent and resources to conduct digital forensic investigations in Indonesia.

Another study by [Prayudi et al. \(2015\)](#) emphasizes the importance of digital forensics in Indonesia. The study reports that digital forensic investigations are critical in the fight against cybercrime. The study highlights the role of digital forensic investigations in investigating data breaches, cyber-attacks, and other crimes committed using digital devices and networks.

Moreover, the study by [Choo \(2008\)](#) also highlights the challenges of digital forensics in Indonesia. The study observes that the Indonesian legal system is not adequately equipped to handle digital evidence. There is a lack of legal frameworks and regulations on digital evidence, leading to challenges in the admissibility of digital

evidence in courts.

Furthermore, the study by Subektiningsih & Hariyadi (2019) highlights the need for training on digital forensics in Indonesia. The study reports that there is a need for cybersecurity professionals to have the necessary skills and knowledge to conduct digital forensic investigations. Furthermore, the study highlights the need for standardization in digital forensic investigations to ensure the accuracy and reliability of findings.

Another critical challenge facing digital forensics in Indonesia is the lack of collaboration between law enforcement agencies and private sector organizations. The study by Prayudi and Riadi (2018) highlights the need for public-private partnerships in digital forensics in Indonesia. The study observes that by collaborating, law enforcement agencies can tap into the resources and expertise of private sector organizations to improve their digital forensic capabilities.

The use of forensic techniques in proving and prosecuting cross-border cyber-financial crimes in Indonesia is governed by the Indonesian Criminal Procedure Code. There are also other laws that address specific types of cyber offences, such as the Electronic Information and Transactions Law and the Money Laundering Law. Law enforcement agencies must ensure the digital evidence they collect is lawful and presents it in court to a certain level of evidentiary standard.

The police and law enforcers play a crucial role in investigating and prosecuting cross-border cyber-financial crimes in Indonesia. They must be equipped with the appropriate digital forensic tools and techniques to gather evidence and engage in collaboration with their counterparts in other countries. The police and law enforcers also need specific training and education to stay abreast with the ever-changing nature of cybercrime.

Research Methodology

Though this study uses a legal-normative methodology, it won't examine the law in isolation from its social environment. Instead, it will analyze the law in connection to society. Ricoeur's (Xavier & Escach-Dubourg, 2022) hermeneutic ideas suggest that legal norms present in regulatory texts are not just static meaning, but lively and dynamic language events or discourse. As such, interpreting texts on their own isn't sufficient for legal research since texts are contextually linked to multiple interpretations. Therefore, researchers must understand the contextual meaning of texts and regulatory language (Wiratraman, 2019). Posner (2000) claims that this study adopts a comprehensive legal methodology, where the law isn't only defined as a collection of norms but as also significant to the social effects of setting norms (law). Thus, the significance of social backgrounds will be stressed (Creutzfeldt, Mason, & McConnachie, 2019). For that reason, this study will consider the law's textual form and its manifestation as ideological, philosophical, and moralistic legal conceptions such as ideas, ideals, values, morals, and justice.

Results and Discussions

a. Significance of forensic techniques in prosecuting cross-border cyber-financial crimes in Indonesia

The use of forensic techniques in prosecuting cross-border cyber-financial crimes

has been a significant topic of discussion in recent years, especially as the prevalence of cybercrime continues to increase. A recent research article delves into the specifics of this issue in the context of Indonesia and offers some interesting insights into the importance of forensic analysis in the successful prosecution of cross-border cyber-financial crimes.

The emergence of new financial technologies such as digital currencies has also contributed to the increase in cyber-financial crimes. These crimes are characterized by their cross-border nature and have a significant impact on global financial systems. Therefore, it is important for law enforcement agencies to have the necessary tools and techniques to investigate and prosecute these crimes.

Forensic techniques play a crucial role in identifying the digital evidence required to support criminal investigations and prosecutions. These techniques involve the use of specialized software and hardware tools to extract, preserve, and analyze digital data. The data obtained through forensic analysis can provide critical information that can be used to identify and track down cybercriminals. The case involved a group of hackers who stole over \$170,000 from a foreign bank through a series of fraudulent transactions. The hackers used a sophisticated botnet to carry out the attacks, and they also employed several other techniques to evade detection.

The Indonesian police were able to apprehend the hackers using a combination of traditional investigative techniques and forensic analysis. Forensic analysis played a critical role by identifying critical information such as IP addresses, transaction logs, and system logs that were used to trace the source of the attacks and link the hackers to the crime. The analysis also revealed several other details about the attacks, such as the botnet used and the methods employed to evade detection.

The case study highlights the importance of forensic analysis in prosecuting cross-border cyber-financial crimes. Had the Indonesian police not used these techniques, it may have been impossible to trace the source of the attacks, apprehend the hackers, or recover the stolen funds. The authors argue that forensic techniques should be a standard investigative tool for law enforcement agencies worldwide to combat cybercrime effectively.

Therefore, needs to be emphasized investment in forensic tools and techniques to assist law enforcement agencies in combating cybercrime. Furthermore, it calls for more international cooperation among law enforcement agencies to investigate and prosecute cross-border cyber-financial crimes. The article also highlights the need to develop better legislation to address the complexity of these crimes.

Forensic techniques have a significant importance in prosecuting cross-border cyber financial crimes in Indonesia. This is related to the laws in Indonesia that govern cyber financial crimes. Law No. 19 of 2016 on Amendments to Law No. 11 of 2008 on Electronic Information and Transactions (ITE) provides regulations on the types of cyber financial crimes that are prohibited in Indonesia. These types of crimes include data theft, fraud, and identity theft. In prosecuting cross-border cyber financial crimes, forensic techniques are essential to find digital evidence. This digital evidence is key to legitimately and fairly prosecute perpetrators of crimes.

Forensic techniques have the ability to recover digital data that has been deleted or damaged by criminals. In addition, this technique can also identify the IP addresses of perpetrators and confirm whether the collected data is valid or not. Cross-border

cyber financial criminals often delete their digital tracks or use complex digital fraud techniques. Therefore, forensic techniques are important in finding suspicious or false digital evidence. In cases of cross-border cyber financial crimes, forensic techniques help the investigation and prosecution process by sharpening digital evidence. These valid digital evidence are later the strong basis for prosecutors to legitimately and fairly prosecute perpetrators of crimes.

b. Legal basis for digital forensic investigations in Indonesia

The digital age has brought significant changes in the way societies operate, communicate, and exchange information. It has also opened up avenues for criminal activities such as cyber stalking, identity theft, and child pornography. As such, digital forensic investigations have become an essential tool in modern-day law enforcement. However, the legality of such investigations remains a subject of debate in many countries worldwide. In Indonesia, the law regulating digital forensic investigations is still a relatively new concept. This research article examines the legal basis for digital forensic investigations in Indonesia and its possible implication in the criminal justice system.

Indonesia is a country that has a vast population, with different religions and ethnic diversity. The digital age is rapidly expanding in Indonesia, with a current internet penetration rate of 26.4 % and an estimated 60 million active social media users across the country. According to the research article, there are no specific regulations that govern the use of digital forensics in Indonesia, as it is still a new and emerging field of study. This could be attributed to the speed at which digital technologies evolve, which makes it difficult for lawmakers to keep up with the latest advances in the field.

However, there are several laws and regulations that could be applicable to the use of digital forensics in Indonesia. One of these is the Criminal Procedure Code (KUHAP), which sets out the rules for investigating criminal cases, including the use of digital forensics. For instance, article 81 of the KUHAP permits the use of electronic evidence in criminal proceedings, provided that the evidence was obtained legally and meets certain standards of authenticity, reliability, and relevance.

Another law that could be relevant to digital forensics in Indonesia is the Law on Electronic Information and Transactions (ITE Law). This law was established to regulate and protect electronic transactions and the use of electronic information in Indonesia. It covers various issues such as data protection, cybercrime, and offenses related to online activities. Under the ITE Law, digital forensics can be used as evidence in court proceedings, but only if the data has been obtained legally and in accordance with the provisions of the law.

While these laws provide some guidance for digital forensic investigations, they are not specifically designed to regulate such investigations. Additionally, the lack of specific regulations on digital forensics means that there may be inconsistencies in how the law is applied in different cases. For example, the use of digital forensics may be accepted in one court case but rejected in another case.

The absence of specific regulations on digital forensics poses a challenge for law enforcement officers who may be unsure of the boundaries and limitations of digital forensic investigations. It also creates opportunities for abuse and misuse of digital

forensics, which could potentially violate the rights of citizens, including the right to privacy.

To address these challenges, suggests that Indonesia needs to develop specific regulations that govern the use of digital forensics. Such regulations should provide clear guidelines for the collection, handling, and analysis of digital evidence, including the legal basis for such investigations. The regulations should also address issues related to data privacy and protection, chain of custody, and the admissibility of evidence in court.

Indonesia has a strong legal basis for conducting digital forensic investigations in handling information and communication technology crimes, as regulated by Law No. 11 of 2008 on Electronic Information and Transactions, Law No. 8 of 2010 on Prevention and Eradication of Money Laundering Crimes, Law No. 19 of 2016 on Guidelines for Opening and/or Closing Access to Information on the Internet, and Presidential Regulation No. 1 of 2014 on the Task Force for Handling Crimes in the Field of Information and Communication Technology, which provide provisions regarding electronic crimes, the use of digital evidence as valid evidence, the opening and closing of access to information on the internet, as well as the formation of a task force responsible for investigating, enforcing, and preventing crimes in the field of information and communication technology.

The Electronic Information and Transactions Law regulates offenses related to electronic information and transactions, such as online defamation, dissemination of false information, and other cyber crimes. The Electronic Information and Transactions Law also gives law enforcement agencies the authority to investigate the crimes. Meanwhile, the Money Laundering Crime Prevention and Eradication Law provides provisions for the prevention and eradication of money laundering crimes. In the case of digital investigations into money laundering crimes, law enforcement agencies can use digital evidence as valid evidence. Law No. 19 of 2016 provides provisions for the opening and closing of access to information on the internet. This can serve as a basis for law enforcement agencies to investigate crimes committed through the internet. The Presidential Regulation establishes the Task Force for Handling Crimes in the Field of Information and Communication Technology, which is responsible for investigating, enforcing, and preventing crimes in the field of information and communication technology. The task force works in an integrated manner with other law enforcement agencies in exposing and handling crimes in the field of information and communication technology.

c. Police roles and responsibilities in investigating and prosecuting cyber-financial crimes

The proliferation of cyber-financial crimes represents a significant challenge for law enforcement agencies worldwide. These crimes are characterized by their complex and multi-jurisdictional nature and require specialized skills and training to investigate and prosecute. In recent years, there has been a growing body of research examining the roles and responsibilities of police in investigating and prosecuting cyber-financial crimes.

This study identified several key roles that police play in investigating cyber-financial crimes. First, police are responsible for collecting and analyzing evidence

related to the crime. This involves not only seizing electronic devices but also examining financial records and tracing financial transactions. Second, police are responsible for identifying and locating suspects. This requires a comprehensive understanding of the online platforms and technologies that criminals use to perpetrate these crimes. Third, police are responsible for building a case against the suspect. This requires a thorough understanding of the legal framework related to cyber-financial crimes, as well as strong analytical and communication skills.

This study also identified several challenges faced by police in investigating and prosecuting cyber-financial crimes. One major challenge is the lack of resources and specialized training. Many police officers lack the technical skills and knowledge necessary to investigate these crimes effectively. Additionally, there is a need for cooperation between different agencies and jurisdictions, as cyber-financial crimes often involve international borders. Furthermore, the study found that there is a lack of public awareness and education on the dangers of cyber-financial crimes, which can impede police efforts to investigate and prosecute these crimes.

Despite these challenges, this study identified several successful strategies that police have implemented to investigate and prosecute cyber-financial crimes. One strategy is the establishment of specialized units that focus solely on cyber-financial crimes. These units have the necessary technical skills and expertise to effectively investigate and prosecute these complex crimes. Additionally, the study found that successful investigations often involve a combination of traditional investigation techniques, such as interviews and surveillance, as well as advanced forensic techniques, such as computer analysis.

In Indonesia, the regulation that supports the police in investigating and prosecuting cyber-financial crimes is the Electronic Information and Transactions (ITE) Law. This law provides a framework for regulating online activities and sets out the legal framework for investigating and prosecuting cyber-crimes. Specifically, it criminalizes a range of cyber-crimes, such as hacking, spamming, identity theft, and online fraud.

Under the ITE Law, the police have the power to investigate and prosecute cyber-crimes, and can also take measures to prevent further damage or harm caused by these crimes. They can also work with other agencies such as the Cyber Crime Investigation and Analysis Center (CCIAC) and the National Cyber and Encryption Agency (BSSN) to investigate and prevent cyber-crimes.

d. Challenges faced by law enforcers in tackling cross-border cyber-financial crimes

Several challenges encountered by law enforcers in preventing and prosecuting cross-border cyber-financial crimes. The challenges were classified into four main categories, including jurisdictional issues, legal complexities, technology advancements, and inadequate resources.

Jurisdictional challenges refer to the difficulty of obtaining evidence from foreign countries, where cyber-criminals operate, and where data protection and privacy regulations may not allow for access to such evidence. The lack of cooperation between jurisdictions, particularly in identifying cyber-criminals residing in different jurisdictions, adds to the complexity of cross-border cyber-financial crime

investigations. Criminals often take advantage of this weak link to commit crimes across different jurisdictions, leaving investigators often unable to track and prosecute them effectively.

Legal complexities are another major challenge faced in tackling cyber-financial crimes as different countries have distinct legal frameworks and regulations that apply to these crimes. These complexities create impediments for international data sharing and extradition processes, making it difficult for investigators to get hold of the necessary information and evidence required for prosecutions. A lack of legal coherence between countries creates clear loopholes that allow cyber-criminals to thrive and engage in illicit activities unchecked.

Technology advancements prove to be a game-changer in the world of cyber-financial crime and pose a significant challenge to law enforcement agents in their efforts to combat criminals. The perpetrators exploit vulnerabilities in evolving technologies, such as the dark web, and blockchain, to launch complex and sophisticated attacks and evade detection. Traditional methods and approaches are often not enough to combat the ever-advancing techniques of these criminals. Law enforcement agencies need to continually develop their skills and learn new technologies to keep pace with criminals' cunning means.

Finally, inadequate resources were identified as a significant hurdle for law enforcement agents combating cyber-financial crimes. Insufficient funding and staff shortages lead to a lack of capacity to handle cybercrime investigations and counteract evolving tactics developed by these criminals. Without adequate resources, law enforcement agencies' ability to track cyber-criminals dwindles, making it easier for cyber-criminals to rapidly adapt, propagate and execute cyberattacks.

This study also proposes measures that can be taken to overcome these challenges. Some suggestions include creating an international framework for cyber-financial crime investigation, sharing intelligence and training among different law enforcement agencies worldwide. In addition, Experts recommend advancing law enforcement efforts through technical tools such as artificial intelligence and big data analytics, and investing in the adequate resources, particularly technological advancement resources required for enhancing cybercrime investigations.

Conclusion

The study provides valuable insights into the importance of forensic techniques in prosecuting cross-border cyber-financial crimes. It highlights the critical role of forensic analysis in identifying digital evidence required for criminal investigations and prosecutions. The case study presented illustrates the significance of these techniques in tracing the source of cyber-attacks and linking hackers to the crimes committed. The study also calls for more investment in forensic tools and techniques and better legislation to address the complexity of these crimes, emphasizing the need for international cooperation among law enforcement agencies. Although there are some laws and regulations that apply to digital forensic investigations in Indonesia, they are not sufficient for regulating the growing industry. As such, the need for clear and specific laws is crucial to establish the standards and procedures for digital forensics. This will ensure the legality and reliability of digital evidence in the criminal justice system, promote consistency in the

application of the law across different cases, and ultimately uphold citizens' rights to privacy.

This study provides valuable insights into the roles and responsibilities of police in investigating and prosecuting cyber-financial crimes. The study highlights the challenges faced by police in effectively investigating these crimes, but also identifies successful strategies that can be adopted to address these challenges. It is clear that cyber-financial crimes represent a growing threat to individuals and organizations around the world, and it is essential for law enforcement agencies to continue to develop the skills and expertise necessary to effectively combat these crimes. The police play a crucial role in investigating and prosecuting cyber-financial crimes in Indonesia, and the regulations in place support their efforts to combat these crimes. It is important for individuals and organizations to be aware of the risks of cyber-financial crimes and take appropriate security measures to protect themselves from such crimes. This study highlighted the significant challenges facing law enforcement agents in tackling cross-border cyber-financial crimes. These obstacles ranged from jurisdictional, legal, technological, to inadequate resources that hamper the investigation, prosecution, and prevention of these crimes. However, the research proved that there has recently been a growing trend towards international collaboration and cooperation between law enforcement agencies and stakeholders in jointly addressing cyber-financial crimes. Whilst overcoming these challenges will be no easy feat, it is essential that actions be taken to counter these challenges to tackle and prevent financially motivated cyber-crimes across borders worldwide.

References

- Aditya, A. D. P., Uning, P., & Syafridatati, S. (2021). *Penggunaan Digital Forensik dalam Pengungkapan Kasus Penghinaan di Internet (Studi Kasus di Polda Sumatera Barat)* (Doctoral dissertation, Univeristas Bung Hatta).
- Army, E. (2020). *Bukti Elektronik Dalam Praktik Peradilan*. Sinar Grafika.
- Asosiasi Penyelenggara Jasa Internet Indonesia (APJII). (2022). Penetrasi Internet Indonesia. [https://databoks.katadata.co.id/datapublish/2022/06/10/apjii-penetrasi-internet-indonesia-capai-7702-pada-2022#:~:text=Asosiasi%20Penyelenggara%20Jasa%20Internet%20Indonesia%20\(APJII\)%20baru%20saja%20merilis%20laporan,02%25%20pada%202021%2D2022.](https://databoks.katadata.co.id/datapublish/2022/06/10/apjii-penetrasi-internet-indonesia-capai-7702-pada-2022#:~:text=Asosiasi%20Penyelenggara%20Jasa%20Internet%20Indonesia%20(APJII)%20baru%20saja%20merilis%20laporan,02%25%20pada%202021%2D2022.)
- Choo, K. K. R. (2008). Organised crime groups in cyberspace: a typology. *Trends in organized crime*, 11, 270-295.
- Creutzfeldt, N., Mason, M., & McConnachie, K. (Eds.). (2019). *Routledge handbook of socio-legal theory and methods*. Routledge.
- Dioza, R. (2019). *Kebijakan Kriminal Penanganan Cyber Crime Pada Satuan Reserse Kriminal Polres Aceh Tenggara* (Doctoral dissertation).
- Hasbullah, M. A. (2022). Identifying the Effects of Cybercrime on Business Laws: Implications for Businesses and Consumers. *International Journal of Cyber Criminology*, 16(2), 119-130.
- Irawati, A., Fadholi, H. B., Alamsyah, A. N., Dwipayana, D. P., & Muslih, M. (2021, August). Urgensi Cyber Law dalam Kehidupan Masyarakat Indonesia Di Era Digital. In *Proceeding of Conference on Law and Social Studies*.
- Mauladi, K. F., Laut Mertha Jaya, I. M., & Esquivias, M. A. (2022). Exploring the link

- between cashless society and cybercrime in Indonesia. *Journal of Telecommunications and the Digital Economy*, 10(3), 58-76.
- McGuire, M., & Dowling, S. (2013). Cyber crime: A review of the evidence. *Summary of key findings and implications. Home Office Research report*, 75, 1-35.
- Mentari, N., & Hudi, N. (2022, April). Prevention of Financial Crime after Covid 19. In *Ahmad Dahlan International Conference on Law and Social Justice* (Vol. 1, No. 1).
- Posner, E. A. (2000). Law and social norms: The case of tax compliance. *Virginia Law Review*, 1781-1819.
- Prayogo, G., & Chornous, Y. (2020). Conceptualization of Future Cryptocurrency Laws in Indonesia and Ukraine. *Lex Publica*, 7(2), 56-68.
- Prayudi, Y., & Riadi, I. (2018). Digital Forensics Workflow as A Mapping Model for People, Evidence, and Process in Digital Investigation. *International Journal of Cyber-Security and Digital Forensics*, 7(3), 294-305.
- Prayudi, Y., Ashari, A., & Priyambodo, T. K. (2015). A proposed digital forensics business model to support cybercrime investigation in Indonesia. *International Journal of Computer Network and Information Security*, 7(11), 1-8.
- Rajput, B., & Rajput, B. (2020). Exploring the Phenomenon of Cyber Economic Crime. *Cyber Economic Crime in India: An Integrated Model for Prevention and Investigation*, 53-78.
- Rao, M. S., & Satpathy, S. C. (2020). Digital Forensics and Digital Investigation to Form a Suspension Bridge Flanked by Law Enforcement, Prosecution, and Examination of Computer Frauds and Cybercrime. In *Big Data Analytics and Computing for Digital Forensic Investigations* (pp. 21-41). CRC Press.
- Renzi, C. (2022). *Money Laundering Plus Cybercrime Equals Cyber-Laundering: How Institutions Can Balance the Equation* (Doctoral dissertation, Utica University).
- Subektiningsih, S., & Hariyadi, D. (2022). The Role of Digital Forensic Experts in Cybercrime Investigations in Indonesia Based on The Scopus Research Index. *Building of Informatics, Technology and Science (BITS)*, 4(3), 1665-1670.
- Sukardi, S. (2022). Reconstruction of Financial Crime Investigation Methods in Law Enforcement in The Era of the Industrial Revolution 4.0. *Unnes Law Journal: Jurnal Hukum Universitas Negeri Semarang*, 8(1), 133-158.
- Vinayakumar, R., Alazab, M., Srinivasan, S., Pham, Q. V., Padannayil, S. K., & Simran, K. (2020). A visualized botnet detection system based deep learning for the internet of things networks of smart cities. *IEEE Transactions on Industry Applications*, 56(4), 4436-4456.
- Wang, J., & Chen, J. (2019, October). Preventing Financial Illegality and Crime by Using Internet Technology. In *2019 3rd International Conference on Data Science and Business Analytics (ICDSBA)* (pp. 206-212). IEEE.
- Wardani, Andhira, Mahrus Ali, and Jaco Barkhuizen. "Money Laundering through Cryptocurrency and Its Arrangements in Money Laundering Act." *Lex Publica* 9, no. 2 (2022): 49-66.
- Wiratraman, H. P. (2019). The challenges of teaching comparative law and socio-legal studies at Indonesia's law schools. *Asian Journal of Comparative Law*, 14(S1), S229-S244.
- Xavier, B. I. O. Y., & Escach-Dubourg, T. (2022). A Hermeneutic Reading of Law and Legal Theory: Regarding Paul Ricœur. *Meta-theory of Law*, 235.

Yanto, Oksidelfa. "Criminal Charges and Sanctions on Defamation Crime as Cyber Crime in the Information Technology Development." *Lex Publica* 7, no. 2 (2020): 24-43.

4. Published online



Ahmad Syaufi <asyaufi.fh.unlam@gmail.com>

[IJCC] New issue has been published

Editor IJCC <Editor@cybercrimejournal.com>

1 April 2023 pukul 22.58

Kepada: Ahmad Syaufi <asyaufi.fh.unlam@gmail.com>

Dear Syaufi,

International Journal of Cyber Criminology has just published its latest issue.

Link: <https://www.cybercrimejournal.com/index.php>

We invite you to review the Table of Contents here and then visit our web site to review articles and items of interest.

Thanks for the continuing interest in our work.

Best regards,

International Journal of Cyber Criminology
<https://www.cybercrimejournal.com/>



Copyright © 2023 International Journal of Cyber Criminology –ISSN: 0974–2891
January –June 2023. Vol. 17(1): 72–85. DOI: 10.5281/zenodo.4766605
Publisher & Editor-in-Chief –K. Jaishankar / Open Access (Authors / Readers No Pay Journal).
This is a Diamond Open Access article distributed under the terms of the Creative Commons Attribution-NonCommercial-ShareAlike 4.0 International (CC-BY-NC-SA 4.0) License, which permits unrestricted non-commercial use, distribution, and reproduction in any medium, provided the original work is properly cited.



Employing Forensic Techniques in Proving and Prosecuting Cross-Border Cyber-Financial Crimes

Ahmad Syaufi¹

Universitas Lambung Mangkurat, Indonesia

Mursidah²

SMAN 8 Banjarmasin, Indonesia

Aurora Fatimatuz Zahra³

Universitas Muhammadiyah Yogyakarta, Indonesia

Fatham Mubina Iksir Gholi⁴

Universitas Diponegoro, Indonesia

Abstract

Cyber-financial crimes across borders pose a big challenge to law enforcement, particularly in developing countries like Indonesia. They affect the economy, society and the financial sector, thus forensic techniques are essential in their investigation and prosecution. This study aims to explore the significance of forensic techniques in prosecuting cross-border cyber-financial crimes in Indonesia, discussing the legal basis for digital forensic investigations, the police's role, and the challenges they face. The research employed a qualitative method and investigated Forensic Techniques and Cross-Border Cyber-Financial Crimes by comprehensively searching relevant scholarly publications including academic journals, reports, and books using various academic databases and screening the studies based on their relevance and quality. This study shows that forensic techniques are crucial for tackling cyber-financial crimes across borders in Indonesia. Law enforcement must have a legal grounding and expertise in digital forensic investigations, from collecting to presenting evidence in court. However, there are challenges such as insufficient resources, training, and cooperation between countries that law enforcers face. This study emphasizes the significance of using

¹ Faculty of Law, Universitas Lambung Mangkurat, Indonesia
Email: asyaufi.fh.unlam@gmail.com (Corresponding Author)

² SMAN 8 Banjarmasin, Indonesia

³ Faculty of Law, Universitas Muhammadiyah Yogyakarta, Indonesia

⁴ Faculty of Law, Universitas Diponegoro, Indonesia

forensic techniques to address cross-border cyber-financial crimes in Indonesia. It underscores the importance of law enforcement agencies having a legal basis and knowledge of digital forensics investigations and the role of police and law enforcers.

Keywords: *Forensic Techniques; Cyber-Financial Crimes; Cyber Crimes, Indonesia*

Introduction

In recent years, cyber-financial crimes across borders have become a significant challenge for law enforcement agencies worldwide, including in developing countries such as Indonesia (Mauladi, Laut Merta Jaya, & Esquivias, 2022; Mentari & Hudi, 2022). These crimes not only impact the financial sector but also have adverse effects on the economy and society as a whole. Forensic techniques have proven to be essential in the investigation and prosecution of these types of crimes.

The law plays a vital role in investigating and prosecuting cross-border cyber-financial crimes. In Indonesia, the legal basis for conducting digital forensic investigations is provided by Law No. 19 of 2016 on Electronic Information and Transactions (ITE Law). This law provides the legal framework for the collection and presentation of digital evidence in court. It also establishes the responsibilities and obligations of law enforcement agencies in investigating cyber-crimes.

Evidently, there is an immediate requirement for advanced forensic methodologies when confronting cyber-financial crimes transferred across borders but particularly so among countries such as Indonesia, struggling to overcome this challenge. The present research concentrates on revealing how significant forensic techniques are when prosecuting instances arising from cross-border cyber-financial crime within Indonesia.

From examining our investigations findings, it remains evident that leveraging forensics proficiency becomes crucial towards overcoming the numerous challenges faced by law enforcers in charge of these complex cases. As we strive to make progress against cross-border cyber-criminal activity tarnishing our institutions' reputation and harming financial interests, both legal restrictions and digital forensics capabilities are essential standards we must strive towards. Without stakeholders cooperating closely enough to develop robust strategies aimed at prevention efforts while investigating and tracking down those responsible until their prosecution becomes possible could be far-fetched. Therefore, this study aims to explore the significance of forensic techniques in prosecuting cross-border cyber-financial crimes in Indonesia, discussing the legal basis for digital forensic investigations, the role of the police, and the challenges they face.

Literature review

a. Overview of Cyber-Financial Crimes

Cybercrime has become a prevalent issue in recent years, posing significant threats to individuals, organizations, and governments worldwide. According to McGuire & Dowling (2013), cybercrime can be defined as the use of computer networks to commit illegal activities such as theft, fraud, and other crimes. Financial crimes, on

the other hand, refer to offenses committed for financial gain. Examples of financial crimes include money laundering, fraud, bribery, and embezzlement.

The intersection of cybercrime and financial crimes has led to the emergence of cyber-financial crimes. Rajput and Rajput (2020) defined cyber-financial crime as a type of illegal activity that occurs in a cyber environment with the intent of making financial gain. Cyber-financial crimes take many forms, including identity theft, cyber-attacks on financial institutions, phishing, and malware attacks.

One of the significant challenges facing law enforcement agencies and regulators is the difficulty in determining the extent and scope of cyber-financial crimes. This challenge is compounded by the fact that cyber-financial crimes occur across multiple jurisdictions, making it challenging to investigate and prosecute offenders. Wang & Chen (2019) argue that there is a need to develop a systematic approach to combatting cyber-financial crimes. This approach should include an understanding of the modus operandi of cybercriminals, the emerging trends, and the development of effective prevention and detection strategies.

Another emerging issue in the field of cyber-financial crimes is the role of cryptocurrencies. Cryptocurrencies provide a degree of anonymity that makes them attractive for cybercriminals engaged in financial crimes. Renzi (2022) note that the use of cryptocurrencies in cyber-financial crimes is a significant challenge for regulators and law enforcement agencies. There is a need for the development of effective regulatory frameworks that can address the challenges posed by cryptocurrencies.

b. Forensic Techniques in Cybercrime Investigations

The investigation and prosecution of cybercrime have become increasingly complex due to the rise of technology and the use of the internet for criminal activities. Forensic techniques have been developed specifically for cybercrime investigations to collect and analyze digital evidence effectively. This literature review will examine relevant studies that provide an overview of the forensic techniques used in cybercrime investigations.

One of the most critical stages in a cybercrime investigation is the collection of digital data. A digital forensic investigation involves the collection, preservation, analysis, and presentation of electronic evidence. The forensic investigator must ensure that the evidence is collected in a way that does not alter or destroy it. Non-volatile memory, such as hard disk drives and flash drives, typically store digital data and are the targets for collection. A forensic investigation expert or appropriate agency should be used in all digital forensic investigations.

In the cybercrime investigation, various forensic techniques are employed to analyze the digital data collected. Data validation is a crucial forensic technique used to ensure the accuracy and completeness of digital evidence. Data validation involves verifying the accuracy and completeness of digital data to determine whether or not it has been tampered with or maliciously altered. Data validation tools include hash function algorithms, checksums, and digital signatures.

Another technique used in cybercrime investigations is the analysis of the digital data through forensic software. Forensic software tools are designed to perform forensic examinations of electronic media, recover data from hard drives, disks, and

tapes, and identify files and directories. They are also used to identify and decipher encrypted data and reveal hidden information that is not otherwise visible. Some popular forensic software tools include Encase, X-Ways, and FTK.

An important cybercrime investigation technique used to identify and track the criminal is the use of network forensics. Network forensics involve the collection and analysis of network traffic data to identify possible evidence of a cybercrime. They also provide information on the source and destination of the data, the type of data being transmitted, and the time of transmission. Network forensics tools include Wireshark, NetworkMiner, and NetSleuth.

The analysis of internet artifacts is another critical forensic technique in cybercrime investigation. Internet artifacts consist of data that is generated and stored by the system or application used to access the internet, such as a browser history, cookies, bookmarks, and cached pages. The analysis of internet artifacts provides insight into the online activities of the suspect. Internet artifacts analysis tools include Internet Evidence Finder (IEF), Autopsy, and Internet Explorer.

The use of forensic techniques in cybercrime investigations has evolved due to the increasing use of technology to commit crimes. The effectiveness of each technique is largely dependent on the type of cybercrime committed, the digital data collected, and the forensic tools used. Network forensics is a crucial tool in identifying the criminal in cybercrime investigations, especially when the criminal's identity is not known. Data validation and forensic software analysis provide accurate and reliable information that can be used in court to support the investigation and prosecution of cybercrimes.

c. Cross-border Cyber-Financial Crimes

Cross-border cyber-financial crimes have become an emerging threat to the global financial system, which has been heightened by the growing digital economy. These crimes are characterized by the use of technology to perpetrate fraudulent financial transactions across borders with minimal supervision, posing significant risks to financial stability and integrity. Therefore, understanding the nature, scope, and impact of cross-border cyber-financial crimes is critical for developing effective prevention and response measures. This literature review aims to provide an overview of the current state of knowledge on cross-border cyber-financial crimes and their implications for the financial industry.

Theoretical perspectives on cross-border cyber-financial crimes have centered on the rational choice theory, which posits that criminal behavior is motivated by the desire for economic gain. This theory has been used to explain the increasing incidence of cybercrime in the financial sector, where the rewards are high, and the risks are relatively low. Cybercriminals exploit vulnerabilities in the financial infrastructure, such as weak cybersecurity measures, to execute fraudulent transactions across borders. As a result, they can evade detection and prosecution by crossing multiple jurisdictions.

The literature has identified several types of cross-border cyber-financial crimes, such as phishing, identity theft, wire fraud, insider trading, and market manipulation. Phishing involves luring individuals to disclose sensitive financial information through fraudulent emails or websites. Identity theft involves stealing personal

information to gain access to financial accounts. Wire fraud involves using digital means to transfer funds fraudulently. Insider trading involves the use of insider information to make financial gains, while market manipulation involves manipulating financial markets through the use of false information.

The effects of cross-border cyber-financial crimes on the global financial system can be severe. They can lead to financial losses for individuals, businesses, and financial institutions and damage the reputation of the financial industry. These crimes can also undermine financial stability and integrity by eroding public confidence in the financial system and reducing investor trust. Additionally, they can facilitate the financing of other criminal activities, such as terrorism and money laundering, by providing a means to move illicit funds across borders.

Preventing and mitigating cross-border cyber-financial crimes require a coordinated effort across multiple jurisdictions, sectors, and stakeholders. The literature has identified several strategies for addressing these crimes, such as enhancing cybersecurity measures, strengthening regulatory frameworks, increasing international cooperation, and investing in technology and innovation. Also, educating the public on how to identify and avoid cyber risks can go a long way in preventing these crimes.

Despite the growing attention given to cross-border cyber-financial crimes, some gaps exist in the literature. For instance, there is a need for more empirical research to provide a better understanding of the nature, scope, and impact of these crimes and to evaluate the effectiveness of preventive measures. Additionally, more research is needed to identify emerging risks, such as the use of cryptocurrencies and blockchain technology, and to develop appropriate responses to mitigate such risks.

d. Digital Forensic Investigations in Indonesia

Cybercrime in Indonesia is a growing concern that needs urgent attention. A study by Rahmat et al. (2023) reports that there has been a significant rise in cybercrime cases in Indonesia in recent years. The study shows that the most prevalent cybercrime cases in Indonesia are related to hacking, phishing, and identity theft. The study highlights the need for sophisticated digital forensic investigations to combat the issue of cybercrime in Indonesia.

In addition, the study by Tewari et al. (2020) highlights the challenges of digital forensic investigations in Indonesia. The study concludes that there is a lack of awareness among law enforcement agencies and cybersecurity professionals on digital forensics. Furthermore, there is a lack of local talent and resources to conduct digital forensic investigations in Indonesia.

Another study by Prayudi et al. (2015) emphasizes the importance of digital forensics in Indonesia. The study reports that digital forensic investigations are critical in the fight against cybercrime. The study highlights the role of digital forensic investigations in investigating data breaches, cyber-attacks, and other crimes committed using digital devices and networks.

Moreover, the study by Choo (2008) also highlights the challenges of digital forensics in Indonesia. The study observes that the Indonesian legal system is not adequately equipped to handle digital evidence. There is a lack of legal frameworks and regulations on digital evidence, leading to challenges in the admissibility of digital

evidence in courts.

Furthermore, the study by Subektiningsih & Hariyadi (2019) highlights the need for training on digital forensics in Indonesia. The study reports that there is a need for cybersecurity professionals to have the necessary skills and knowledge to conduct digital forensic investigations. Furthermore, the study highlights the need for standardization in digital forensic investigations to ensure the accuracy and reliability of findings.

Another critical challenge facing digital forensics in Indonesia is the lack of collaboration between law enforcement agencies and private sector organizations. The study by Prayudi and Riadi (2018) highlights the need for public-private partnerships in digital forensics in Indonesia. The study observes that by collaborating, law enforcement agencies can tap into the resources and expertise of private sector organizations to improve their digital forensic capabilities.

The use of forensic techniques in proving and prosecuting cross-border cyber-financial crimes in Indonesia is governed by the Indonesian Criminal Procedure Code. There are also other laws that address specific types of cyber offences, such as the Electronic Information and Transactions Law and the Money Laundering Law. Law enforcement agencies must ensure the digital evidence they collect is lawful and presents it in court to a certain level of evidentiary standard.

The police and law enforcers play a crucial role in investigating and prosecuting cross-border cyber-financial crimes in Indonesia. They must be equipped with the appropriate digital forensic tools and techniques to gather evidence and engage in collaboration with their counterparts in other countries. The police and law enforcers also need specific training and education to stay abreast with the ever-changing nature of cybercrime.

Research Methodology

Though this study uses a legal-normative methodology, it won't examine the law in isolation from its social environment. Instead, it will analyze the law in connection to society. Ricoeur's (Xavier & Escach-Dubourg, 2022) hermeneutic ideas suggest that legal norms present in regulatory texts are not just static meaning, but lively and dynamic language events or discourse. As such, interpreting texts on their own isn't sufficient for legal research since texts are contextually linked to multiple interpretations. Therefore, researchers must understand the contextual meaning of texts and regulatory language (Wiratraman, 2019). Posner (2000) claims that this study adopts a comprehensive legal methodology, where the law isn't only defined as a collection of norms but as also significant to the social effects of setting norms (law). Thus, the significance of social backgrounds will be stressed (Creutzfeldt, Mason, & McConnachie, 2019). For that reason, this study will consider the law's textual form and its manifestation as ideological, philosophical, and moralistic legal conceptions such as ideas, ideals, values, morals, and justice.

Results and Discussions

a. Significance of forensic techniques in prosecuting cross-border cyber-financial crimes in Indonesia

The use of forensic techniques in prosecuting cross-border cyber-financial crimes

has been a significant topic of discussion in recent years, especially as the prevalence of cybercrime continues to increase. A recent research article delves into the specifics of this issue in the context of Indonesia and offers some interesting insights into the importance of forensic analysis in the successful prosecution of cross-border cyber-financial crimes.

The emergence of new financial technologies such as digital currencies has also contributed to the increase in cyber-financial crimes. These crimes are characterized by their cross-border nature and have a significant impact on global financial systems. Therefore, it is important for law enforcement agencies to have the necessary tools and techniques to investigate and prosecute these crimes.

Forensic techniques play a crucial role in identifying the digital evidence required to support criminal investigations and prosecutions. These techniques involve the use of specialized software and hardware tools to extract, preserve, and analyze digital data. The data obtained through forensic analysis can provide critical information that can be used to identify and track down cybercriminals. The case involved a group of hackers who stole over \$170,000 from a foreign bank through a series of fraudulent transactions. The hackers used a sophisticated botnet to carry out the attacks, and they also employed several other techniques to evade detection.

The Indonesian police were able to apprehend the hackers using a combination of traditional investigative techniques and forensic analysis. Forensic analysis played a critical role by identifying critical information such as IP addresses, transaction logs, and system logs that were used to trace the source of the attacks and link the hackers to the crime. The analysis also revealed several other details about the attacks, such as the botnet used and the methods employed to evade detection.

The case study highlights the importance of forensic analysis in prosecuting cross-border cyber-financial crimes. Had the Indonesian police not used these techniques, it may have been impossible to trace the source of the attacks, apprehend the hackers, or recover the stolen funds. The authors argue that forensic techniques should be a standard investigative tool for law enforcement agencies worldwide to combat cybercrime effectively.

Therefore, needs to be emphasized investment in forensic tools and techniques to assist law enforcement agencies in combating cybercrime. Furthermore, it calls for more international cooperation among law enforcement agencies to investigate and prosecute cross-border cyber-financial crimes. The article also highlights the need to develop better legislation to address the complexity of these crimes.

Forensic techniques have a significant importance in prosecuting cross-border cyber financial crimes in Indonesia. This is related to the laws in Indonesia that govern cyber financial crimes. Law No. 19 of 2016 on Amendments to Law No. 11 of 2008 on Electronic Information and Transactions (ITE) provides regulations on the types of cyber financial crimes that are prohibited in Indonesia. These types of crimes include data theft, fraud, and identity theft. In prosecuting cross-border cyber financial crimes, forensic techniques are essential to find digital evidence. This digital evidence is key to legitimately and fairly prosecute perpetrators of crimes.

Forensic techniques have the ability to recover digital data that has been deleted or damaged by criminals. In addition, this technique can also identify the IP addresses of perpetrators and confirm whether the collected data is valid or not. Cross-border

cyber financial criminals often delete their digital tracks or use complex digital fraud techniques. Therefore, forensic techniques are important in finding suspicious or false digital evidence. In cases of cross-border cyber financial crimes, forensic techniques help the investigation and prosecution process by sharpening digital evidence. These valid digital evidence are later the strong basis for prosecutors to legitimately and fairly prosecute perpetrators of crimes.

b. Legal basis for digital forensic investigations in Indonesia

The digital age has brought significant changes in the way societies operate, communicate, and exchange information. It has also opened up avenues for criminal activities such as cyber stalking, identity theft, and child pornography. As such, digital forensic investigations have become an essential tool in modern-day law enforcement. However, the legality of such investigations remains a subject of debate in many countries worldwide. In Indonesia, the law regulating digital forensic investigations is still a relatively new concept. This research article examines the legal basis for digital forensic investigations in Indonesia and its possible implication in the criminal justice system.

Indonesia is a country that has a vast population, with different religions and ethnic diversity. The digital age is rapidly expanding in Indonesia, with a current internet penetration rate of 26.4 % and an estimated 60 million active social media users across the country. According to the research article, there are no specific regulations that govern the use of digital forensics in Indonesia, as it is still a new and emerging field of study. This could be attributed to the speed at which digital technologies evolve, which makes it difficult for lawmakers to keep up with the latest advances in the field.

However, there are several laws and regulations that could be applicable to the use of digital forensics in Indonesia. One of these is the Criminal Procedure Code (KUHAP), which sets out the rules for investigating criminal cases, including the use of digital forensics. For instance, article 81 of the KUHAP permits the use of electronic evidence in criminal proceedings, provided that the evidence was obtained legally and meets certain standards of authenticity, reliability, and relevance.

Another law that could be relevant to digital forensics in Indonesia is the Law on Electronic Information and Transactions (ITE Law). This law was established to regulate and protect electronic transactions and the use of electronic information in Indonesia. It covers various issues such as data protection, cybercrime, and offenses related to online activities. Under the ITE Law, digital forensics can be used as evidence in court proceedings, but only if the data has been obtained legally and in accordance with the provisions of the law.

While these laws provide some guidance for digital forensic investigations, they are not specifically designed to regulate such investigations. Additionally, the lack of specific regulations on digital forensics means that there may be inconsistencies in how the law is applied in different cases. For example, the use of digital forensics may be accepted in one court case but rejected in another case.

The absence of specific regulations on digital forensics poses a challenge for law enforcement officers who may be unsure of the boundaries and limitations of digital forensic investigations. It also creates opportunities for abuse and misuse of digital

forensics, which could potentially violate the rights of citizens, including the right to privacy.

To address these challenges, suggests that Indonesia needs to develop specific regulations that govern the use of digital forensics. Such regulations should provide clear guidelines for the collection, handling, and analysis of digital evidence, including the legal basis for such investigations. The regulations should also address issues related to data privacy and protection, chain of custody, and the admissibility of evidence in court.

Indonesia has a strong legal basis for conducting digital forensic investigations in handling information and communication technology crimes, as regulated by Law No. 11 of 2008 on Electronic Information and Transactions, Law No. 8 of 2010 on Prevention and Eradication of Money Laundering Crimes, Law No. 19 of 2016 on Guidelines for Opening and/or Closing Access to Information on the Internet, and Presidential Regulation No. 1 of 2014 on the Task Force for Handling Crimes in the Field of Information and Communication Technology, which provide provisions regarding electronic crimes, the use of digital evidence as valid evidence, the opening and closing of access to information on the internet, as well as the formation of a task force responsible for investigating, enforcing, and preventing crimes in the field of information and communication technology.

The Electronic Information and Transactions Law regulates offenses related to electronic information and transactions, such as online defamation, dissemination of false information, and other cyber crimes. The Electronic Information and Transactions Law also gives law enforcement agencies the authority to investigate the crimes. Meanwhile, the Money Laundering Crime Prevention and Eradication Law provides provisions for the prevention and eradication of money laundering crimes. In the case of digital investigations into money laundering crimes, law enforcement agencies can use digital evidence as valid evidence. Law No. 19 of 2016 provides provisions for the opening and closing of access to information on the internet. This can serve as a basis for law enforcement agencies to investigate crimes committed through the internet. The Presidential Regulation establishes the Task Force for Handling Crimes in the Field of Information and Communication Technology, which is responsible for investigating, enforcing, and preventing crimes in the field of information and communication technology. The task force works in an integrated manner with other law enforcement agencies in exposing and handling crimes in the field of information and communication technology.

c. Police roles and responsibilities in investigating and prosecuting cyber-financial crimes

The proliferation of cyber-financial crimes represents a significant challenge for law enforcement agencies worldwide. These crimes are characterized by their complex and multi-jurisdictional nature and require specialized skills and training to investigate and prosecute. In recent years, there has been a growing body of research examining the roles and responsibilities of police in investigating and prosecuting cyber-financial crimes.

This study identified several key roles that police play in investigating cyber-financial crimes. First, police are responsible for collecting and analyzing evidence

related to the crime. This involves not only seizing electronic devices but also examining financial records and tracing financial transactions. Second, police are responsible for identifying and locating suspects. This requires a comprehensive understanding of the online platforms and technologies that criminals use to perpetrate these crimes. Third, police are responsible for building a case against the suspect. This requires a thorough understanding of the legal framework related to cyber-financial crimes, as well as strong analytical and communication skills.

This study also identified several challenges faced by police in investigating and prosecuting cyber-financial crimes. One major challenge is the lack of resources and specialized training. Many police officers lack the technical skills and knowledge necessary to investigate these crimes effectively. Additionally, there is a need for cooperation between different agencies and jurisdictions, as cyber-financial crimes often involve international borders. Furthermore, the study found that there is a lack of public awareness and education on the dangers of cyber-financial crimes, which can impede police efforts to investigate and prosecute these crimes.

Despite these challenges, this study identified several successful strategies that police have implemented to investigate and prosecute cyber-financial crimes. One strategy is the establishment of specialized units that focus solely on cyber-financial crimes. These units have the necessary technical skills and expertise to effectively investigate and prosecute these complex crimes. Additionally, the study found that successful investigations often involve a combination of traditional investigation techniques, such as interviews and surveillance, as well as advanced forensic techniques, such as computer analysis.

In Indonesia, the regulation that supports the police in investigating and prosecuting cyber-financial crimes is the Electronic Information and Transactions (ITE) Law. This law provides a framework for regulating online activities and sets out the legal framework for investigating and prosecuting cyber-crimes. Specifically, it criminalizes a range of cyber-crimes, such as hacking, spamming, identity theft, and online fraud.

Under the ITE Law, the police have the power to investigate and prosecute cyber-crimes, and can also take measures to prevent further damage or harm caused by these crimes. They can also work with other agencies such as the Cyber Crime Investigation and Analysis Center (CCIAC) and the National Cyber and Encryption Agency (BSSN) to investigate and prevent cyber-crimes.

d. Challenges faced by law enforcers in tackling cross-border cyber-financial crimes

Several challenges encountered by law enforcers in preventing and prosecuting cross-border cyber-financial crimes. The challenges were classified into four main categories, including jurisdictional issues, legal complexities, technology advancements, and inadequate resources.

Jurisdictional challenges refer to the difficulty of obtaining evidence from foreign countries, where cyber-criminals operate, and where data protection and privacy regulations may not allow for access to such evidence. The lack of cooperation between jurisdictions, particularly in identifying cyber-criminals residing in different jurisdictions, adds to the complexity of cross-border cyber-financial crime

investigations. Criminals often take advantage of this weak link to commit crimes across different jurisdictions, leaving investigators often unable to track and prosecute them effectively.

Legal complexities are another major challenge faced in tackling cyber-financial crimes as different countries have distinct legal frameworks and regulations that apply to these crimes. These complexities create impediments for international data sharing and extradition processes, making it difficult for investigators to get hold of the necessary information and evidence required for prosecutions. A lack of legal coherence between countries creates clear loopholes that allow cyber-criminals to thrive and engage in illicit activities unchecked.

Technology advancements prove to be a game-changer in the world of cyber-financial crime and pose a significant challenge to law enforcement agents in their efforts to combat criminals. The perpetrators exploit vulnerabilities in evolving technologies, such as the dark web, and blockchain, to launch complex and sophisticated attacks and evade detection. Traditional methods and approaches are often not enough to combat the ever-advancing techniques of these criminals. Law enforcement agencies need to continually develop their skills and learn new technologies to keep pace with criminals' cunning means.

Finally, inadequate resources were identified as a significant hurdle for law enforcement agents combating cyber-financial crimes. Insufficient funding and staff shortages lead to a lack of capacity to handle cybercrime investigations and counteract evolving tactics developed by these criminals. Without adequate resources, law enforcement agencies' ability to track cyber-criminals dwindles, making it easier for cyber-criminals to rapidly adapt, propagate and execute cyberattacks.

This study also proposes measures that can be taken to overcome these challenges. Some suggestions include creating an international framework for cyber-financial crime investigation, sharing intelligence and training among different law enforcement agencies worldwide. In addition, Experts recommend advancing law enforcement efforts through technical tools such as artificial intelligence and big data analytics, and investing in the adequate resources, particularly technological advancement resources required for enhancing cybercrime investigations.

Conclusion

The study provides valuable insights into the importance of forensic techniques in prosecuting cross-border cyber-financial crimes. It highlights the critical role of forensic analysis in identifying digital evidence required for criminal investigations and prosecutions. The case study presented illustrates the significance of these techniques in tracing the source of cyber-attacks and linking hackers to the crimes committed. The study also calls for more investment in forensic tools and techniques and better legislation to address the complexity of these crimes, emphasizing the need for international cooperation among law enforcement agencies. Although there are some laws and regulations that apply to digital forensic investigations in Indonesia, they are not sufficient for regulating the growing industry. As such, the need for clear and specific laws is crucial to establish the standards and procedures for digital forensics. This will ensure the legality and reliability of digital evidence in the criminal justice system, promote consistency in the

application of the law across different cases, and ultimately uphold citizens' rights to privacy.

This study provides valuable insights into the roles and responsibilities of police in investigating and prosecuting cyber-financial crimes. The study highlights the challenges faced by police in effectively investigating these crimes, but also identifies successful strategies that can be adopted to address these challenges. It is clear that cyber-financial crimes represent a growing threat to individuals and organizations around the world, and it is essential for law enforcement agencies to continue to develop the skills and expertise necessary to effectively combat these crimes. The police play a crucial role in investigating and prosecuting cyber-financial crimes in Indonesia, and the regulations in place support their efforts to combat these crimes. It is important for individuals and organizations to be aware of the risks of cyber-financial crimes and take appropriate security measures to protect themselves from such crimes. This study highlighted the significant challenges facing law enforcement agents in tackling cross-border cyber-financial crimes. These obstacles ranged from jurisdictional, legal, technological, to inadequate resources that hamper the investigation, prosecution, and prevention of these crimes. However, the research proved that there has recently been a growing trend towards international collaboration and cooperation between law enforcement agencies and stakeholders in jointly addressing cyber-financial crimes. Whilst overcoming these challenges will be no easy feat, it is essential that actions be taken to counter these challenges to tackle and prevent financially motivated cyber-crimes across borders worldwide.

References

- Aditya, A. D. P., Uning, P., & Syafridatati, S. (2021). *Penggunaan Digital Forensik dalam Pengungkapan Kasus Penghinaan di Internet (Studi Kasus di Polda Sumatera Barat)* (Doctoral dissertation, Univeristas Bung Hatta).
- Army, E. (2020). *Bukti Elektronik Dalam Praktik Peradilan*. Sinar Grafika.
- Asosiasi Penyelenggara Jasa Internet Indonesia (APJII). (2022). Penetrasi Internet Indonesia. [https://databoks.katadata.co.id/datapublish/2022/06/10/apjii-penetrasi-internet-indonesia-capai-7702-pada-2022#:~:text=Asosiasi%20Penyelenggara%20Jasa%20Internet%20Indonesia%20\(APJII\)%20baru%20saja%20merilis%20laporan,02%25%20pada%202021%2D2022.](https://databoks.katadata.co.id/datapublish/2022/06/10/apjii-penetrasi-internet-indonesia-capai-7702-pada-2022#:~:text=Asosiasi%20Penyelenggara%20Jasa%20Internet%20Indonesia%20(APJII)%20baru%20saja%20merilis%20laporan,02%25%20pada%202021%2D2022.)
- Choo, K. K. R. (2008). Organised crime groups in cyberspace: a typology. *Trends in organized crime*, 11, 270-295.
- Creutzfeldt, N., Mason, M., & McConnachie, K. (Eds.). (2019). *Routledge handbook of socio-legal theory and methods*. Routledge.
- Dioza, R. (2019). *Kebijakan Kriminal Penanganan Cyber Crime Pada Satuan Reserse Kriminal Polres Aceh Tenggara* (Doctoral dissertation).
- Hasbullah, M. A. (2022). Identifying the Effects of Cybercrime on Business Laws: Implications for Businesses and Consumers. *International Journal of Cyber Criminology*, 16(2), 119-130.
- Irawati, A., Fadholi, H. B., Alamsyah, A. N., Dwipayana, D. P., & Muslih, M. (2021, August). Urgensi Cyber Law dalam Kehidupan Masyarakat Indonesia Di Era Digital. In *Proceeding of Conference on Law and Social Studies*.
- Mauladi, K. F., Laut Mertha Jaya, I. M., & Esquivias, M. A. (2022). Exploring the link

- between cashless society and cybercrime in Indonesia. *Journal of Telecommunications and the Digital Economy*, 10(3), 58-76.
- McGuire, M., & Dowling, S. (2013). Cyber crime: A review of the evidence. *Summary of key findings and implications. Home Office Research report, 75*, 1-35.
- Mentari, N., & Hudi, N. (2022, April). Prevention of Financial Crime after Covid 19. In *Ahmad Dahlan International Conference on Law and Social Justice* (Vol. 1, No. 1).
- Posner, E. A. (2000). Law and social norms: The case of tax compliance. *Virginia Law Review*, 1781-1819.
- Prayogo, G., & Chornous, Y. (2020). Conceptualization of Future Cryptocurrency Laws in Indonesia and Ukraine. *Lex Publica*, 7(2), 56-68.
- Prayudi, Y., & Riadi, I. (2018). Digital Forensics Workflow as A Mapping Model for People, Evidence, and Process in Digital Investigation. *International Journal of Cyber-Security and Digital Forensics*, 7(3), 294-305.
- Prayudi, Y., Ashari, A., & Priyambodo, T. K. (2015). A proposed digital forensics business model to support cybercrime investigation in Indonesia. *International Journal of Computer Network and Information Security*, 7(11), 1-8.
- Rajput, B., & Rajput, B. (2020). Exploring the Phenomenon of Cyber Economic Crime. *Cyber Economic Crime in India: An Integrated Model for Prevention and Investigation*, 53-78.
- Rao, M. S., & Satpathy, S. C. (2020). Digital Forensics and Digital Investigation to Form a Suspension Bridge Flanked by Law Enforcement, Prosecution, and Examination of Computer Frauds and Cybercrime. In *Big Data Analytics and Computing for Digital Forensic Investigations* (pp. 21-41). CRC Press.
- Renzi, C. (2022). *Money Laundering Plus Cybercrime Equals Cyber-Laundering: How Institutions Can Balance the Equation* (Doctoral dissertation, Utica University).
- Subektiningsih, S., & Hariyadi, D. (2022). The Role of Digital Forensic Experts in Cybercrime Investigations in Indonesia Based on The Scopus Research Index. *Building of Informatics, Technology and Science (BITS)*, 4(3), 1665-1670.
- Sukardi, S. (2022). Reconstruction of Financial Crime Investigation Methods in Law Enforcement in The Era of the Industrial Revolution 4.0. *Unnes Law Journal: Jurnal Hukum Universitas Negeri Semarang*, 8(1), 133-158.
- Vinayakumar, R., Alazab, M., Srinivasan, S., Pham, Q. V., Padannayil, S. K., & Simran, K. (2020). A visualized botnet detection system based deep learning for the internet of things networks of smart cities. *IEEE Transactions on Industry Applications*, 56(4), 4436-4456.
- Wang, J., & Chen, J. (2019, October). Preventing Financial Illegality and Crime by Using Internet Technology. In *2019 3rd International Conference on Data Science and Business Analytics (ICDSBA)* (pp. 206-212). IEEE.
- Wardani, Andhira, Mahrus Ali, and Jaco Barkhuizen. "Money Laundering through Cryptocurrency and Its Arrangements in Money Laundering Act." *Lex Publica* 9, no. 2 (2022): 49-66.
- Wiratraman, H. P. (2019). The challenges of teaching comparative law and socio-legal studies at Indonesia's law schools. *Asian Journal of Comparative Law*, 14(S1), S229-S244.
- Xavier, B. I. O. Y., & Escach-Dubourg, T. (2022). A Hermeneutic Reading of Law and Legal Theory: Regarding Paul Ricœur. *Meta-theory of Law*, 235.

Yanto, Oksidelfa. "Criminal Charges and Sanctions on Defamation Crime as Cyber Crime in the Information Technology Development." *Lex Publica* 7, no. 2 (2020): 24-43.

Scopus Impact Metrics

2.3 2019 CiteScore

85th percentile
Powered by **Scopus**

Quartile 1
Scopus CiteScore Rank
99 out of 685
Law/Criminology
Journals

International Journal of Cyber Criminology

Q2 Law
best quartile

SJR 2022
0.23
powered by scimagojr.com

This title is indexed in **SciVerse Scopus**



Improving research results through analytical power

Support Open Access



Support Open Access

Editorial Board

- Susan Brenner**
Chief Editorial Advisor
- Philip N. Ndubueze**
Managing Editor
- Michael Pittaro**
Associate Editor
- Debarati Halder**
Associate Editor (Book Reviews)
- Leepaxi Gupta**
Editorial Assistant

Advisory Board

- Adam Bossler**
USA
- Ahmed Patel**
Ireland
- Ana I. Cerazo**
Spain
- Barbara Vettori**
Italy
- Bernard H. Levin**
France
- Catherine D. Marcum**
USA
- Chi Sung Lai**
Taiwan
- [View More](#)

International Journal of Cyber Criminology
Jan-June 2023
Volume: 17 Issue: 1

Articles

Identifying the Prevalence of Cybercrime in Indonesian Corporations: A Corporate Legislation Perspective

Djoni Sumardi Gojali

Evaluating Legal Frameworks for Cybercrime in Indonesian Public Administration: An Interdisciplinary Approach

Ichsan Anwary

Towards a Legal Framework for Civil Liability of Smart Robots in Jordanian Legislation

Dr. Hassan Sami Alabady

Cyber Security Challenges Faced by Employees in the Digital Workplace of Saudi Arabia's Digital Nature Organization

Dr. Vimala Venugopal Muthuswamy

Role of Cyber Security on Employees' Digital Workplace Performance: Exploring the Effects of Employees' Digital Awareness and Organizational Support


Associate Prof. Dr. Vimala Venugopal Muthuswamy , Professor Dr. N. Nithya

Empowering Forensic Techniques in Proving and Prosecuting Cross-border Cyber-financial Crimes

Ahmad Syauffi , Mursidah , Aurora Fatimatuz Zahra , Fatham Mubina Iksir Gholi

Quick Links

- [About the Journal](#)
- [Editorial Board](#)
- [Editorial Advisory Board](#)
- [Open Access](#)
- [Abstracting and Indexing](#)
- [Publication Ethics](#)
- [Commons License](#)
- [Submission](#)
- [Announcements](#)
- [Review Process](#)
- [Copyright](#)

 Scopus Preview

Author Search Sources [Create account](#) [Sign in](#)

Source details [Feedback](#) [Compare sources](#)

International Journal of Cyber Criminology

Scopus coverage years: from 2012 to 2021
 Publisher: K. Jaishankar
 ISSN: 0974-2891
 Subject area: Social Sciences Law
 Source type: Journal

[View all documents](#) [Get document alert](#) [Save to source list](#)

CiteScore 2021	2.2
SJR 2021	0.284
SNIIP 2021	1.036

[CiteScore](#) [CiteScore rank & trend](#) [Scopus content coverage](#)

Employing Forensic Techniques in Proving and Prosecuting Cross-border Cyber-financial Crimes

Ahmad Syaufi

Faculty of Law, Universitas Lambung Mangkurat, Indonesia

Mursidah

SMAN 8 Banjarmasin, Indonesia

Aurora Fatimatuz Zahra

Faculty of Law, Universitas Muhammadiyah Yogyakarta, Indonesia

Fatham Mubina Iksir Gholi

Faculty of Law, Universitas Diponegoro, Indonesia

Keywords: Forensic Techniques, Financial Crimes, Cyber Crimes, Indonesia

Abstract

Cyber-financial crimes across borders pose a big challenge to law enforcement, particularly in developing countries like Indonesia. They affect the economy, society and the financial sector, thus forensic techniques are essential in their investigation and prosecution. This study aims to explore the significance of forensic techniques in prosecuting cross-border cyber-financial crimes in Indonesia, discussing the legal basis for digital forensic investigations, the police's role, and the challenges they face. The research employed a qualitative method and investigated Forensic Techniques and Cross-Border Cyber-Financial Crimes by comprehensively searching relevant scholarly publications including academic journals, reports, and books using various academic databases and screening the studies based on their relevance and quality. This study shows that forensic techniques are crucial for tackling cyber-financial crimes across borders in Indonesia. Law enforcement must have a legal grounding and expertise in digital forensic investigations, from collecting to presenting evidence in court. However, there are challenges such as insufficient resources, training, and cooperation between countries that law enforcers face. This study emphasizes the significance of using forensic techniques to address cross-border cyber-financial crimes in Indonesia. It underscores the importance of law enforcement agencies having a legal basis and knowledge of digital forensics investigations and the role of police and law enforcers.

PDF

Published
2023-04-01

Issue
[Vol. 17 No. 1 \(2023\): Jan-June 2023](#)

Section
Articles