Social Science and Everant Journal Humanities Journal

ISSN: 2456-2653

https://sshjournal.com/

Impact Factor: 2024: 6.576
2023: 5.731

Volume 09 Issue 06 Jun 2025 DOI: https://doi.org/10.18535/sshj.v9i06.1889

Exploring the Challenges Faced by the Cavite Provincial Police Office in Cybercrime Investigation

Katherine B. Custodio

Received 02-05-2025
Revised 09-05-2025
Accepted 04-06-2025
Published 07-06-2025

Copyright: ©2025 The Authors. This is an open access article under the CC BY-NC-ND license
https://creativecommons.org/licenses/by-nc-nd/4.0/

Abstract

This study explored the challenges faced by the Philippine National Police (PNP) in investigating cybercrime cases within the Cavite Provincial Police Office. Employing a qualitative interpretative phenomenological analysis (IPA) approach, the research aimed to understand the lived experiences and perceptions of five cybercrime investigators regarding their operational difficulties. Data was collected through semi-structured interviews, which were transcribed and analyzed thematically under the Social Construction of Technology (SCOT) framework. Findings revealed that investigators encountered significant obstacles, including inadequate technological tools, outdated infrastructure, limited resources, insufficient specialized training, and rapidly evolving cyber threats. The study also identified coping strategies employed by personnel, such as continuous professional development, technological adaptation, and advocacy for increased support. The results underscored the need for comprehensive capacity building, modernization of tools, and sustained funding to enhance the efficiency and effectiveness of cybercrime investigations. The study concluded with recommendations to strengthen training programs, improve infrastructure, and foster interagency collaboration, ultimately aiming to bolster the PNP's capability to combat the growing menace of cybercrime.

Keyword: Cybercrime, Investigation Challenges, Cavite Provincial Police Office, Resources, Training, Technology, Digital Forensics, Capacity Building, Law Enforcement, Cyber Threats

Introduction

In today's digital age, cybercrime has emerged as one of the most challenging issues faced by law enforcement agencies worldwide. As technology continues to evolve, so too do the methods and tactics employ by cybercriminals. The Philippines, like many developing nations, has experienced a significant rise in cybercrime incidents over the past decade. With the growing number of people accessing the internet for banking, communication, business, and entertainment, the country has become increasingly vulnerable to cyber threats such as online fraud, identity theft, cyberbullying, hacking, and various forms of digital scams (Santos, 2020).

Argosino (2024). Reported that the PNP Anti-Cybercrime Group (ACG) recorded a total of 4,469 cybercrime incidents from January to March 2024, reflecting a 21.84% increase compared to the 3,668 cases documented in the last quarter of 2023. According to ACG chief Maj. Gen. Sidney Hernia, online selling scams were the most prevalent, accounting for 990 cases. This was followed by 319 cases of investment scams and 309 cases of debit and credit card fraud, among other cybercriminal activities. Combating cybercrime has become an essential and difficult responsibility for the Philippine National Police (PNP), due to cybercriminals' increased proficiency, the anonymity of the internet, and the complexities of digital evidence.

The increase in cybercrime has shown substantial shortcomings in the PNP's ability to successfully combat these rising threats. Although the Anti-Cybercrime Group (ACG) was formed in 2013 to combat cybercrime, the PNP continues to confront several problems when investigating and prosecuting cybercrime crimes. The current cybercrime office is still limited, and only regional offices have equipment while complete support of resources are only available in the national headquarters.

According to Fajardo et al. (2025), Philippine National Police (PNP) encounters enormous challenges when conducting cybercrime investigations. The lack of specialized training among police personnel who are responsible for conducting these investigations is an important issue. Many officers lack the necessary knowledge and skills to effectively combat cyber-related offenses. Ongoing training programs are being implemented through Regional Anti-Cybercrime Units (RACUs), as noted by PNP spokesperson Col. Jean Fajardo. However, there is an enormous gap in expertise among regions. This training shortage is made worse by the PNP's inadequate technological structure and limited resources.

Based on the records of the PNP Cybercrime Unit, cybercrime cases came to 21,300 in 2023 from 13,890 in 2022. From July 2022 to January 2024, online scams led with 15,937 cases, followed by illegal access at 4,821, and identity theft at 2,384. The challenges, such as limited resources, technological support, and human resource skills need immediate attention to effectively address cyber threats. (*Philippine National Police Anti-Cybercrime Group (PNP-ACG).*

Considering there were six progressive cities in the Cavite area Imus, Bacoor, General Trias, Carmona, Tanza, and Naic the need to strengthen the cybercrime unit had been recognized as a priority. This study aimed to explore the various challenges that the Philippine National Police encountered in investigating cybercrime cases. It examined how the PNP’s existing resources and capabilities had been insufficient in addressing the growing number of cyber threats, and it focused on the difficulties law enforcement experienced in dealing with cybercriminals. Understanding these issues would help us better understand the cybercrime investigation and suggest solutions to improve the PNP's efficacy.

Background of the Study

Philippine National Police (PNP), through the Cavite Provincial Police Office, plays a vital role in addressing and preventing these threats. However, the rapid pace at which cybercrime evolves has left many law enforcement bodies struggling to keep up. Cybercrime investigations require specialized knowledge, proper training, and modern tool resources that are often scarce in local police stations. Previous studies and reports have pointed out the lack of technological preparedness and the need for capacity-building programs within the PNP when dealing with cyber threats (Gonzales & Reyes, 2019).

However, despite the urgency of addressing cybercrime, the CPPO faces significant limitations. The lack of modern equipment, insufficient digital forensic tools, undertrained personnel, and the absence of dedicated cybercrime units in many municipalities hinder cybercrime investigations. According to the Department of Information and Communications Technology (DICT), many police stations in the country, especially in provincial areas, struggle with outdated systems and lack the technical skills necessary to investigate sophisticated cyber offenses (DICT, 2021).

Resources Limitation

Based on stated by J. Li (2021). Resource Limitations for Cybercrime in the Philippines: The Philippine National Police (PNP) and other law enforcement organizations frequently lack the financial and technological resources needed to effectively investigate and respond to cybercrimes, and the broader public's knowledge of cybersecurity threats and safe online conduct is seriously lacking. Since many Filipinos still don't know how to defend themselves against frequent dangers like phishing and identity theft, hackers may easily take advantage of them.

As per Widodo et al. (2024) analysis, Resource constraints pose a great hindrance to the worldwide attempts to fight cybercrime. Inadequate financial allocation is one of the major problems because these are meant to support cybersecurity systems for the proper investigation and acquisition of evidence regarding crimes committed using technologies. This problem is particularly observed in the underdeveloped countries that are struggling due to limited funds for training programs, modern technologies, and the creation of specialized cybersecurity ncies. The nation's capacity to build strong cybersecurity policies and proper handling of cyberattacks are not present due to budgetary imbalance.

McKoy, C. (2021), pointed out that law enforcement personnel addressing typical crimes see the readiness of law enforcement organizations to combat cybercrime at local level as an enormous obstacle. Cybercrime investigations need to be carried out by a specialized division or agency equipped with the appropriate expertise and resources, therefore excluding patrol personnel due to their insufficient training and knowledge necessary for conducting such investigations. additional issues that limited officers' ability to address computer-related incidents locally, including financial constraints, political factors, inadequate training, and the duration required to investigate cybercrimes at the local level. In the study conducted by Alastal, et al (2023), it was stated that cyber investigators encounter many difficulties in terms of investigation of internet crimes. Law enforcers need a deeper understanding of the technical and sociotechnical obstacles they encounter; the availability of the quantity and quality of information technology infrastructure and the cyber skills of investigators are necessary to support the investigators.

According to Pasinhon and Donato (2024), the limited availability of modern forensic tools and methods, including those needed for data recovery and tracking dummy accounts, presents a significant challenge for PNP staff in managing cybercrime cases.

Based on the Blancaflor et al. (2023), the effectiveness of digital forensics in combating cybercrime is demonstrated using evolving digital forensics trends, such as cloud, social media, IoT, and network forensics. Given the continuous advancement of technology and the global threat of cyberattacks and criminal activity, the Philippines could significantly benefit from establishing adequate infrastructure to potentially reduce the nation's vulnerability to attacks and minimize damage.

Alghamdi's (2021), pointed out that there is a shortage and insufficient number of skilled and forensic investigators and qualified forensic staff, and it causes the process of digital forensics to be compromised. Acquiring evidence related to digital forensics requires competent and high standard technology to produce scientifically sound evidence, therefore issues regarding the lack of well-trained forensic investigators is a big challenge.

Oville et al. (2024) found that cyber cops' pandemic experiences included performing duties amidst the pandemic, maintaining a good image, and facing personnel and supply shortages. Their solutions involved cyber cops' initiative and extending strategies. Their goals were to apply modern technology and increase organizational support.Significantly shorter while still conveying the main findings of the study regarding the cyber cops' experiences, challenges, solutions, and goals during the pandemic.

Technological Challenges

Based on J. Li said (May 20, 2021) More and more crooks with different goals are using the internet to do bad things, which puts the whole country at risk. The terrible truth was made worse by the fast-changing computer technologies and methods. Even worse, it is becoming more vulnerable to these kinds of threats as it updates its economic and key infrastructure systems. This means that it needs to rely more on national and global computer network growth. This gives hackers more chances to attack and puts the country's important infrastructure and economic systems at risk of terrible threats that could have terrible results.

Borges, E. (2024, February). Highlights that Cybercriminals are constantly adapting their approaches, making it challenging for investigators to keep up with new technology and strategies. This requires regular training for law enforcement officers.

According to a study by Moolayil et al. (2023), computer forensics is an important part of the fight against hacking because it gives people the tools and standards they need to look through and judge digital data. Forensics experts have a hard time analyzing and processing cybercrimes quickly and effectively because technology is changing so quickly, and people are using more and more devices.

Based on Viraja & Purandare, (2021). Cybercrime is any illicit activity involving a network, computer, or networked device. Regarding criminal spread, cybercrime is the biggest sector globally. While some cybercrimes are carried out straight against computers to destroy or disable them, others use computers or networks to distribute malware, unauthorized information, photos, or other content; some cybercrimes are distributed and done to acquire profit for hackers. Cybercrimes year by year are witnessing a growth in magnitude and sophistication as well as in regularity since technology is evolving rapidly and there is a huge need to solve the challenges these crimes present.

In the research study by Apakar et al. (2024), the author expressed that complex hacking methods pose major problems for experts who investigate cybercrime. Criminal detectives have a hard time keeping up with the growing online risks. They also found that technology is a big problem when it comes to investigating hacking. The legal issue is how looking at people's records can invade their privacy. Individual privacy rights that were at odds with each other had to be investigated, which was hard and led to the creation of processes for handling personal data. Informing the public of cyber risks, safe online behaviors, and the processes for reporting cybercrimes to law enforcement agencies.

Nouh, et al (2019) found that law enforcement faces significant challenges investigating cybercrime due to criminals' technological adaptability and constant innovation; investigators require advanced technical knowledge to effectively combat these offenses. Amoo, et al (2024), conducted a study to evaluate the emphasized the importance of building a strong and flexible global cooperation in efficiently addressing cyber threats in the modern digital age wherein technology develops. Coordinated measures are essential as the government, law enforcement, businesses and people in the community all have shared responsibility for cybersecurity. The changing character of cyber threats calls for a proactive and team strategy to keep ahead of enemies. In

the study conducted by Rakha (2023), the author expressed that there should be proper guidelines and rules for managing digital evidence to help law enforcement agencies and policy makers create legal frameworks suited to combat cybercrime because digital forensics are crucial and relevant for criminal investigations so there should be developed standardized rules and procedures in obtaining and management of digital evidence.Azam et al. (2023) states that process changes like using hash values, ensuring chain of custody, and quick data analysis boost investigation success.

Prakash (2021) says that there are hardware and software solutions for cloud and edge computers in digital forensics. To make the study more technical, a short introduction to cryptography and encryption methods for Cloud/Edge forensic investigation was added. This was along with a short primer on cryptography and basic rules for forensic procedures for dealing with changed sound files, hidden files, picture files, or images using steganography. It is very important to know how useful and quick regular digital tools are at different stages of the research process.

Bankova (2021) highlights that digital transformation has made cybercrime a global concern. Businesses face increasing difficulty in preventing hacker attacks, leading to significant financial losses. The study focuses on industries like banking and insurance, which are highly digitalized and therefore more vulnerable. It also emphasizes the need to consider expert opinions on addressing cybercrime.

Sarkar et al. (2023) note that growing digitalization enables cybercriminals, making many countries easy targets. A lack of standard procedures and tools hinders investigations. Their TTP-based framework offers strategies to aid investigators and support cyber peace.

Training and Knowledge Gaps

According to Calinawan (2024). One of the most significant issues is a lack of sufficient training for law enforcement agents tasked to investigate cybercrimes. Many officers at local police stations lack the training required to successfully respond to cyber-related occurrences. According to PNP spokesperson Col. Jean Fajardo, Regional Anti-Cybercrime Units (RACUs) are now conducting training programmes, although many staff have yet to finish them. This information gap can result in inefficient investigations and a reduced possibility of successful convictions.

Siddiqua (2024) notes that a key challenge for the PNP is the lack of specialized cybercrime training, leaving many investigators unprepared for complex digital cases. While programs like RACU training and cybersecurity desks exist, PNP spokesperson Col. Jean Fajardo states that many officers have yet to complete the necessary training.

Yar and Steinmetz (2019) conducted a study to investigate such crimes that will often require specialized technical knowledge and skills and that there is present little indication that police have appropriate training and competency.

Button et al. (2020) found that while interest in cybersecurity is growing, it often doesn't lead to safer behavior due to a lack of clear guidance or referrals to the right resources—missing a chance to reduce cybercrime. Improving police training on cybercrime, standardizing responses, and clarifying investigation roles can better support victims and may increase reporting rates by addressing the perception that police are ineffective.Based on akdemir et.al 2020 Given the networked global character of the Internet, which seriously challenges law enforcement of cybercrime, addressing cybercrime calls for knowledge and cybersecurity abilities. Previous police cybercrime investigations showed that local police personnel lack technical knowledge, which naturally impacted the battle against cybercrime by means of specialized cybercrime units, police agencies keep improving their capacity to fight cybercrime. Still, there is a shortage of empirical studies looking through the prism of professional police officers employed in cybercrime units at policing issues of economic cybercrime. This empirical study fills up the knowledge vacuum in literature.

Martin, though (2022). The police and other groups are realizing that cybercrime is a big problem that continues to grow worse. To fight and get rid of hacking, it is very important to demonstrate to police officers how to do it. Because of cyber-attacks, the problem is getting worse, and we need to find good answers. The police officers' travels to different places taught them a lot about cybercrime, which they then used at work to come up with ways to stop cybercrime. With the help of scientific study, Moustakas came up with the main idea and the theories that explain hacking.

As explained by Bossler et al. (2019), one big difference between cybercrimes and regular crimes is that investigators need to be trained and taught how to better understand cybercrime cases. This has a big effect on how confident they are in their ability to handle cybercrime cases. Police and people in general should treat hacking with the same level of concern as other crimes.

Curtis and Oxburgh (2022) explain that while cybercrime is a growing concern, it remains poorly understood by both law enforcement and researchers. UK government estimates suggest that cybercrime victims are unlikely to report incidents due to a lack of confidence in the police's ability to handle such crimes. The study highlights issues within the police force, including a lack of awareness about cybercrime. By reviewing existing research, this study provides a comprehensive view of cybercrime, identifying key technological, personal, societal, and situational factors, and discusses how this understanding could help address current research challenges.

Paek (2021) emphasizes that police need to redefine their roles and rethink how they monitor and prevent illegal online activities. The study highlights the importance of officers having the knowledge, acceptance, interest, and proper attitude to effectively address the seriousness and impact of cybercrime on society, safety, and security.

According to Horan and Saiedian (2021), study about the cybercrime investigation's landscape, difficulties and future research. The study indicates that police personnel must become familiar and knowledgeable of the several tools, their purposes and to know what vital information they can offer that can assist with apprehension of suspect and evidence digital forensics are changing and that criminal investigations depend more on technology thus. The study also underlines how machine learning and automation enable the investigators to classify and identify the evidence and hasten the gathering of other materials.

Jocson and Espiritu (2023), highlight that as the Philippines becomes more digital, law enforcement needs urgent training in cybersecurity and digital forensics to keep up with evolving cybercrimes. They also highlight that fighting cybercrime requires cooperation between government agencies and international partners, but conflicting priorities and poor communication often make teamwork difficult.

Viraya and Purandare (2021) note that in the digital age, it's hard to imagine life without the Internet. As technology becomes a bigger part of daily life, cybercrimes have also increased. With the rise of social media and the use of vast amounts of data, sensitive information like trade secrets, privacy concerns, and security issues are increasingly at risk.

The study of Nishniannidze's (2022), aimed to find out if there are studies on some fresh issues of cybercrime and the causes behind obsolete laws. The gravity of cybercrime as a new kind of crime and the issue that can develop with this crime must be treated in a timely manner to eliminate its negative influence on the protection of citizen's privacy and rights. Due to the rising number of victims of cybercrime, it is advised to investigate it from all angles including legal and scientific ones.

As explained by Arifi (2020) in his study entitled Cybercrime: A Challenge for Law Enforcement, stated that the laws which pertains to cybercrime need to be updated to prevent and regulate the offenders since some of them are one step ahead in using technology to perpetrate crimes. Cybercrime also changes daily and is fast expanding all over the world; so, government and law enforcers should increase their collaboration in handling offenders and evidence. Finally, there must be efficient knowledge, experts, and sufficient tools that will be effective in handling cases and evidence regarding cybercrime. Chigada and Madzinga (2021) highlight that cybercrime affects global security, with growing threats and vulnerabilities, especially during the pandemic. They stress the need for cybercrime officers to assess security needs, identify gaps, and develop strategies to counter cyberattacks.

As stated by Moloney et al. (2022), cybercrime is among the fastest changing and expanding worldwide societal issues that every country is facing today. It affects and victimize the elderly, women, and children which fall prey to frauds, abuse in the form of harassment, stalking and sexual exploitation. Cybercrime includes activities of identity theft, financial fraud and scams, child pornography, drug and violent felonies, and espionage. Law enforcement departments are important as a front line and responsible in dealing with and assisting the most vulnerable populations and the challenges in their full capacity. According to Agunos and Diaz's (2019), study on the skills of the Philippine National Police in the province of Bataan: Basis for professional development plan, the respondents of the study believe they require technical support for their investigative works. They advise organizing deliberate seminars on investigative skills and training courses on related areas. According to De Paoli and Associates (2020), Cybercrime policing is still a difficult task with no "off-the-peg" solutions easily embraced with any certainty of success. Adding to the corpus of empirical studies on the topic of policing cybercrime, this paper has demonstrated that officials in specialized (usually high-tech) units across many nations view comparable issues that are typical of front-line officers.

In the study conducted by Ashawana, et. al. (2023), there is a need for digital modularization and analysis of its relevance in overcoming the identified challenges, such as integrating a structured query language database in the framework to augment the conservation and maintenance because this will help to address the challenges and issues regarding the identity of a person. Vitus, E. N. (2023), pointed out that computer hacking hurts society more than it aids. This means that governments, companies, and individuals must all work together right away to bring those responsible for such offenses to justice. As computers and communication tools get better, hacking is more likely to happen. It is very important to protect yourself from cybercrime because anyone could be a target, and it can cost a person or a company a lot of money very quickly.

The study by Ramazanov et al. (2020) shows that electronic evidence is useful for more than just finding digital crimes like data theft, network penetration, and illegal online transactions. Digital evidence can also be used to find crimes that happened in the real world, like theft, attack, accidents, and murder. Businesses also use computer forensics to keep track of data about system or network intrusions to find and punish cybercriminals.

The research of Alonso-Fernandez et al. (2021) claims that among the best instruments available to researchers for online investigations is social media. Data gleaned from social media accounts or sites can support research. It provides an abundance of material about personal life and businesses, not only common people but also criminals and their activities.

Based on study by Raaijmakers (2019). Machine learning has changed how crimes are investigated and how people are tracked. It can be used for studying in several ways. Machine learning gives experts teach their computers to find parts of crimes in data from places like social media or security cams. This method can be used for online identity. Using machine learning, it teaches computers what patterns they can look for in a crime to figure out what kind of criminal group might be responsible.

As per Mishra et al., (2022), to help to reduce the rising vulnerabilities and cyber threats in the online environment. Cybersecurity laws have been passed in several nations all around to protect the interests of their people, companies, and governments in the digital realm. Though their criteria and scope differ, these laws usually have as their shared purpose improving cybersecurity.

Additionally, Annadurai et al., (2022), the devices have brought about many benefits for mankind that have driven large investments. But certain people, sometimes referred to as cybercriminals, have taken advantage of technological advancements to create fresh kinds of digital-era offenses. The more proactive nature of cybercriminals brought about by ICT and internet connectivity has resulted in a spike in computer crimes.

According to M. Ali, et al. (2023) This idea is centered on making sure that private and sensitive data remains hidden and just available to authorized systems or people. It seeks to stop illegal access, sharing of private information, or exposing delicate data. Data classification, access restrictions, and encryption are among the ways one could attain confidentiality. Integrity guarantees that data stays dependable and correct.

Pasinhon and Donato (2024) stated That limited advanced forensic tool and approach presents one of the difficulties the staff members are facing in managing cybercrime cases. Data recovery and forensic analysis on computer devices and other ICT-related seized by the PNP need digital forensic tools.

Based on Gomez et.al. 2024, the empirical findings of the study show a link between these elements and research success rates; so, it is essential to give technological improvement and innovation initiatives top priority. workforce proficiency. Combining technology knowledge and resources with research will improve countering cybercrime outcomes investigations; consequently, adopting and using new and developing technologies will help to boost these results. Fighting cybercrime in the Philippines depends on newly developing technologies. Dereck et al. (2020) highlighted the need for police to adapt functionally to the digital and post-digital era, considering the physical context in which these adaptations occur. Their workshop with cybercrime investigators—some outside the police force—revealed four important organizational and cultural factors: police management and leadership, avoiding overly complex divisions between cyber and traditional policing, upholding ethics, and improving knowledge, training, and development.

As per Gom-gom-o Jr. (2024). Officers often have a heavy workload and pressure from their roles, which makes it difficult for them to devote all their attention to investigating cybercrimes. Because of such pressure, police may neglect to give cyber investigations sufficient time while they balance other responsibilities.

The study by Tithi et al. (2024) shows that the biggest problem is getting the right information about crime. Officers also deal with a lot of workplace issues, such as a lack of resources, too much work, stress, a toxic work environment, and money worries. They also deal with a lot of environmental issues, such as problems with working together and cooperating. in addition, rita joviland (2024). The Cybercrime Investigation and Coordinating Centre (CICC) of the Philippine government is currently in the process of acquiring tools that are specifically designed to combat financial technology crimes. The objective of these instruments is to improve the government's ability to investigate and analyze financial transactions associated with cybercrimes, thereby facilitating the more effective tracking of illicit funds, even when they get absorbed into exchanges.

Fajardo et. al (2025). Pointed out that the challenges encountered by the PNP-ACG are more systemic in nature and not primarily driven by individual or demographic characteristics. The study concludes with suggestions for how to improve the PNP-ACG in the region by doing a full organizational assessment, creating a strong digital forensic management system, running programs to develop people's skills, and working together with other groups to deal with the problems that were discovered.

In addition, Nelufule et al. (2024). The challenges of digital forensics have a substantial impact on the justice system, as a lack of reliable digital evidence can lead to miscarriages of justice for both the accused and victims of crime. A comprehensive framework is provided to solve these difficulties, focusing on continual innovation, collaboration, and cybersecurity training and awareness.

The researcher aimed to identify the challenges police faced in investigating cybercrime, noting that inadequate training, limited resources, and fast-changing technology hindered effective enforcement. Understanding these issues helped develop better strategies to improve police performance and create safer digital environments.

Theoretical Framework

This study is anchored in the Social Construction of Technology (SCOT) theory developed by Wiebe Bijker and Trevor Pinch in the mid-1980s., which provides a lens to understand the challenges faced by the Cavite Provincial Police Office in investigating cybercrime cases. According to SCOT, cultural, social, and institutional circumstances influence how technology is developed, interpreted, and used rather than only its technical aspects. In this sense, the idea highlights how technology is impacted by the demands, beliefs, and behaviors of many social groups rather than being neutral or self-directing (Klein & Kleinman, 2020).

Through SCOT, the Cavite Provincial Police Office's difficulties—such as low levels of computer literacy, a dearth of sophisticated equipment, inadequate training, financial limitations, and poor interagency coordination—are seen as socially constructed issues rather than just technical ones. Additionally, the tendency to continue using outdated or ineffective techniques may be an aspect of institutional stabilization, a process outlined in SCOT whereby specific technological practices become "locked in" because they are accepted by the organization due to limited resources, policy, or habit rather than because they are the best.

The Social Construction of Technology (SCOT) theory provides a significant framework for understanding the issues that police officers encounter while fighting cybercrime. The key Principles of SCOT (1) Interpretive Flexibility this diversity may lead to misunderstanding regarding the roles and obligations in preventing cybercrime and investigations. (2) Relevant Social Groups the Philippine National Police (PNP) has established trained professional's cybercrime units; however, these units frequently confront difficulties because of lacking resources and training. (3) Technologies get stabilized Over time, various interpretations of technology gain dominance. In the police, this might result in established approaches for dealing with cybercrime, which may not adapt rapidly to evolving threats or technology.

This study's SCOT foundation highlights that combating cybercrime successfully involves more than simply acquiring cutting-edge technology; it also calls for an awareness of the institutional structures, social processes, and interpretations that shape the adoption and use of such technologies. Using this theoretical framework, the study can get a greater understanding of the ways in which social and technical factors interact with local law enforcement.

Such a concept is reflected in the research paradigm in Figure 1

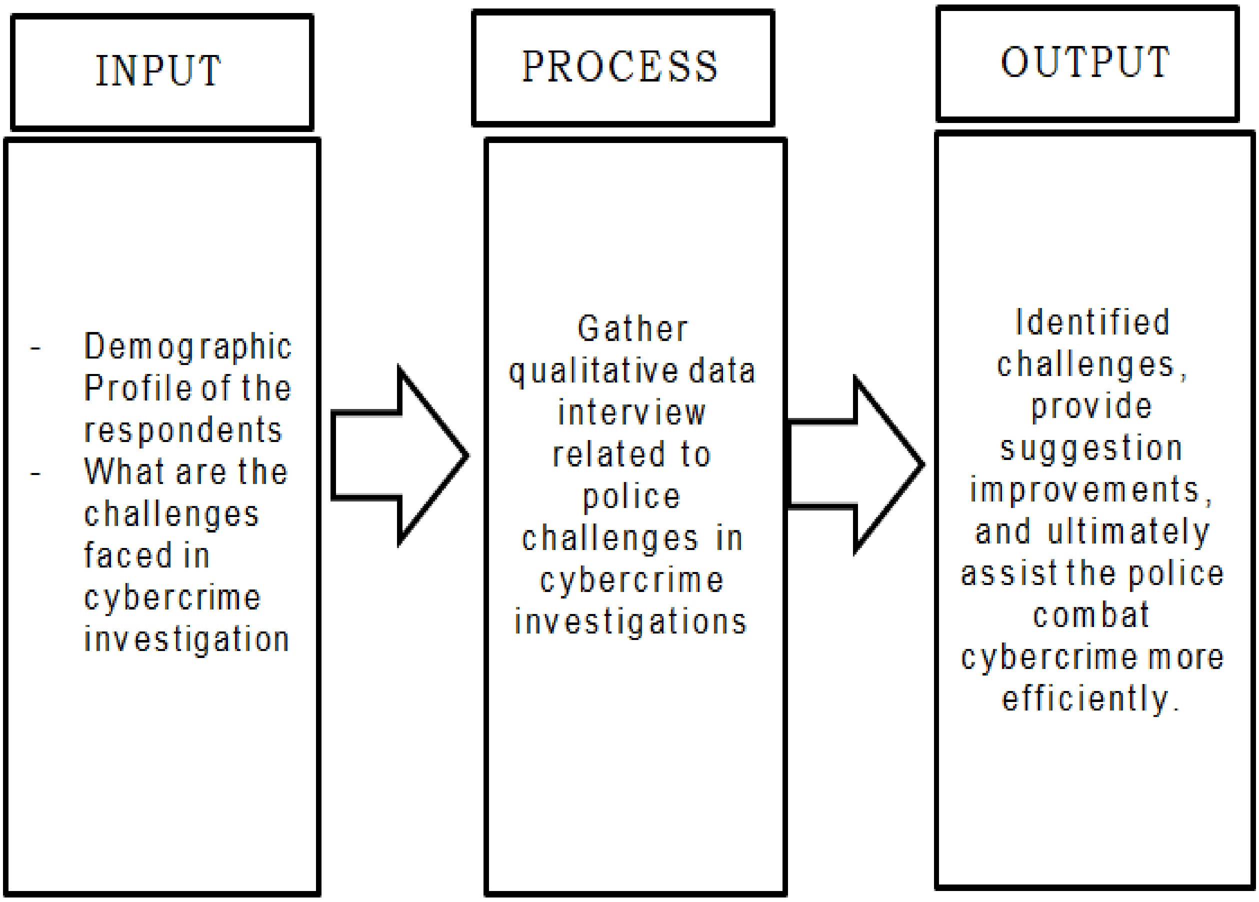

INPUT
- Demographic Profile of the respondents
- What are the challenges faced in cybercrime investigation
PROCESS
Gather qualitative data interview related to police challenges in cybercrime investigations
OUTPUT
Identified challenges, provide suggestion improvements, and ultimately assist the police combat cybercrime more efficiently.

Figure 1: Research Paradigm

Therefore, the researcher determined the profile of the respondents in terms of sex, age, their position or rank, and the number of cybercrime cases handled related to the topic on Exploring the challenges faced by the investigators on cases related to cybercrime in the Cavite provincial police office. The interview process itself presented unique challenges that must be navigated to gather reliable and meaningful data. The findings of this study provided insights into these challenges and the overall effectiveness of the police in handling cybercrime cases.

Statement of Purpose

The study aims to determine the extent of challenges faced by the cybercrime office in Cavite Provincial Police. Specifically, it aims to answer the following questions:

1. What is the demographic profile of the respondent?

1.1 Age

1.2 Gender

1.3 Baccalaureate degree

1.4 Rank/Position

1.5 Year of service as an investigator cybercrime unit

1.6 Number of cybercrime cases handled

2. What are the challenges encountered when investigating cybercrime cases? In terms of

2.1 Technical limitations

2.2 Human resource issues

2.3 Facilities and infrastructure limitations

2.4 Financial constraints

2.5 Other relevant challenges as perceived by respondents

3. What coping mechanisms or strategies do investigators employ to manage the challenges?

4. What recommendations would you suggest for improving the overall capacity of the PNP in addressing cybercrime?

Objective of the study

This study is aimed at:

1. To describe the demographic profile of the PNP personnel involved in cybercrime investigation, including their age, gender, rank/position, years of service in the cybercrime unit, number of cases handled.
2. To identify and analyze the challenges encountered by investigators when investigating cybercrime cases, specifically in terms of technical limitations, human resource issues, organizational and institutional challenges, financial constraints, and other relevant challenges as perceived by the respondents.
3. To assess the perceived relevance and effectiveness of current training programs available to the Cybercrime Unit in addressing real-world cybercrime incidents.
4. To explore the coping mechanisms and strategies employed by investigators to manage the challenges encountered in cybercrime investigations.
5. To gather and propose recommendations for improving the overall capacity of the Philippine National Police (PNP) in addressing cybercrime effectively.

Significance of the study

This study merited the following:

Philippine National Police. Gained significant knowledge of the specific challenges encountered by its officers, which will facilitate the development of targeted training programs and strategies to improve their effectiveness in fighting cybercrime.

Police administrators and policymakers. This study provided insight on the institutional and structural problems influencing cybercrime units' effectiveness. It may help guide choices about how to allocate resources, coordinate among agencies, develop expertise, and create policies that meet the technical needs of modern law enforcement.

Local Government Unit. Was able to create or amend policies supporting local law enforcement in combatting cybercrime using the results of the research. By advocating better funding, training, and technology locally, they may help ensure that their communities are better protected.

Educational Institutions. The study can be utilized to revise the curricula of schools and universities, particularly those that offer programs in information technology, criminology, and law enforcement. This will guarantee that future professionals have the necessary skills to face the challenges caused by cybercrime.

Future Researchers. The findings of this study served as a foundation or point of reference for future research on the difficulties faced by the Philippine National Police when investigating cybercrime crimes.

Scope and Delimitation of the Study

The main goal of this study is to explore the challenges that the Cavite Provincial Police Office's (CPPO) cybercrime investigators encounter when investigating cybercrime cases. The study mainly looks at the challenges and obstacles that investigators have while investigating cases involving cybercrimes, such as technological, training, and financial constraints. Officers actively involved in cybercrime investigations were interviewed to collect qualitative data for the research, which will only focus on the investigators' point of view.

focus on how these investigators tackle the complex issues of modern cybercrime, focusing their capacity to adjust to quickly changing technological advancements and encounter the challenges and evolving characteristics of digital criminal activity. By focusing on cybercrime investigators, the study will provide insight into their challenges and challenges while carrying out investigations in the province.

This study focuses solely on the experiences of Cavite police officers involved in cybercrime investigations. It does not cover other agencies or technical solutions but instead examines the practical challenges and resource limitations faced by the local police in addressing cybercrimes.

Definition of Terms

For a better understanding of this study, the following terms were defined according to how they were being used in the study:

Challenges. Defined as the difficulties, obstacles, or barriers that police personnel encounter while investigating cybercrime. The issues may be technological, procedural, legal, financial, or connected to training and resources.

Cybercrime. Is the term used to describe illicit activities carried out via networks or computers. This covers a wide range of crimes, including phishing, internet fraud, identity theft, and hacking. To properly handle the considerable dangers that cybercrime poses to both people and businesses, specialist investigation techniques are required.

Cybersecurity. It is the protection of computer systems, networks, and data against cyberattacks, damage, or unauthorized access. In cybercrime investigations, it refers to the methods and techniques used to protect information and systems against crimes such as hacking, data breaches, and malware assaults.

Cybercrime Investigation. It is a systematic approach to locating, evaluating, and reducing crimes using computers. It entails obtaining digital evidence, protecting its integrity, and putting it together in a way that is appropriate for court. Investigators use a range of instruments and methods, such as digital forensics, to identify the offenders and their intentions.

Digital Forensics. A field within forensic science specialized to data analysis and recovery from digital devices. Evidence from computers, cellphones, servers, and other electronic devices used in cybercrimes can be gathered in this way. The procedure guarantees that digital evidence is stored so that it may be used in court while keeping its integrity.

Philippine National Police. The Philippine National Police (PNP) is the national police agency in charge of keeping peace and order, enforcing laws, and preventing and investigating crimes, including cybercrimes, across the country.

Police officer. Are PNP employees in charge of maintaining public safety, enforcing laws, managing investigations, and handling crises. In the framework of this research, it especially refers to individuals assigned to conduct investigations into cybercrimes.

Technical expertise. Referring to the professional expertise and skills needed for investigating and understanding digital crimes. This involves understanding programming, networking on computers, digital forensics, and the technical aspects of internet platforms.

Methodology

This part of the paper includes the process on when, where and how the study will be done, the materials needed to be used, and who are the respondents or participants of the study.

Research Design

This study explored the challenges faced by the Cavite Provincial Police Office in investigating cybercrime cases using a qualitative method, specifically an interpretative phenomenological design, to understand officers' experiences.

Qualitative research methods offer unique advantages for exploring complex issues, allowing researchers to draw on interpersonal skills and subjective insights to deepen their understanding (Alase, 2017). Tenny et al. (2022) emphasized that qualitative research is particularly valuable for investigating real-world problems, providing rich data on participants' experiences, perceptions, and behaviors, focusing on the "how" and "why" rather than just quantitative measures. This study employed qualitative research with Interpretative Phenomenological Analysis (IPA), a method described by Creswell and Creswell (2017) as ideal for deeply exploring the meanings individuals assign to social or human issues, collecting data in context, and analyzing it inductively to identify broader themes.

IPA was well-suited for this study, which aimed to explore the lived experiences of police officers handling cybercrime cases. It allowed the researcher to examine participants' personal and social perspectives, capturing their shared experiences meaningfully. By focusing on their viewpoints, IPA supported a deeper, unbiased understanding of their challenges (Alase, 2017). According to Smith and Fieldsend (2021), IPA is a collaborative and theory-neutral method that helps uncover the meanings individuals assign to their experiences, making it ideal for exploring complex and subjective issues.

Research Locale

The study was conducted at the Cavite Provincial Police Office to explore the challenges faced by the Philippine

National Police (PNP) in investigating cybercrime cases. The researcher chose the police investigator from the Cybercrime Unit because they will offer an in-depth understanding of the challenges encountered by the Cavite Provincial Police Office in the investigation of cybercrime. This will enable the researcher to gather firsthand insights into the resource limitations, technical skills gaps, and infrastructure inadequacies experienced by the PNP in combating cybercrime. Their personal experiences, specialized training, legal knowledge, and collaborative efforts will provide an indispensable source of information for this research (De Guzman, et.al 2024).

Sampling Technique

The researcher adopted purposive sampling techniques by selecting five respondents who were directly involved in cybercrime investigations within the PNP, specifically from the Cavite Provincial Police Office, who have been with the unit for three to six years and handling cybercrime cases. This method was chosen to ensure that the respondents had sufficient experience and knowledge regarding the challenges faced in cybercrime case investigations (Campbell et al., 2020).

Research Instrument

A research instrument refers to any tool that researchers utilize to gather, evaluate, and analyze data pertinent to the subject of a research investigation (Nolfi, 2019).

The researcher carefully crafted questions based on each statement of the problem, adjusting the number of questions depending on the kind of information needed. To make sure the questions were clear, relevant, and aligned with the study’s goals, three experts in cybercrime and law enforcement reviewed and validated the interview guide. These expert-approved, researcher-made questions were then used during the interview sessions. This process helped ensure that the data gathered truly reflected the challenges faced by the PNP in investigating cybercrime, adding to the credibility and trustworthiness of the study’s findings.

The selected data collection technique for this research involved utilizing semi-structured interviews. This method provided adaptability in questioning, enabling the researchers to deeply explore participants' experiences, viewpoints, and interpretations regarding the challenges faced by the PNP in cybercrime case investigations.

In a semi-structured interview, the interviewer followed a planned set of questions or themes while keeping flexibility in the order and words of questions, as well as the depth of exploration. These interviews often began with broad, open-ended inquiries designed to enable participants to express their experiences, viewpoints, and opinions openly (Sadulski, J. 2024).

This approach allowed the researchers to acquire rich, detailed qualitative data that showed the complexities and specific challenges encountered by the PNP during cybercrime investigations.

As the interviews progressed, the interviewer delved deeper into specific topics, posed follow-up questions to clarify responses, or explored new lines of discussion. This approach fostered a natural and conversational exchange between the interviewer and participant, building rapport and trust. Consequently, it facilitated the collection of more nuanced and comprehensive data.

Data Analysis

This study will use thematical analysis of the issues faced by the Philippine National Police (PNP) in investigating cybercrime cases that may be created using the Interpretative Phenomenological Analysis (IPA) which are used to interpret, specify the meaning and analyze the data.

The data analysis procedure involves a systematic strategy to interpret the qualitative data obtained from interviews about the issues faced by the Philippine National Police (PNP) in cybercrime investigations. The researcher transcribed all recordings verbatim and then carefully reviewed the transcripts to familiarize themselves with the data. Using thematic analysis, the researcher found, classified, and categorized repeating patterns and major themes that emerged from the participants' narratives (Kassai, 2019; Smith, 1990).

As referenced by Braun and Clarke in Mihas (2023), a theme captures a significant aspect of the data systematically, regardless of whether that theme reflects the majority perception (Scharp &amp; Sanders, 2019, p. 1). These themes were further developed and conceptually aligned with one another, prioritizing the generation of significance over quantity while assessing consistency to identify

patterns.

Thematic analysis, as described by Caulfield (2023), is a qualitative data analysis method applied to textual materials such as interview transcripts. The researchers closely examined the data to identify recurring themes topics, ideas, and patterns of meaning using a six-step process: familiarization, coding, theme generation, theme review, theme definition and naming, and writing up. This process mitigated confirmation bias during the analysis.

Data analysis followed the Interpretative Phenomenological Analysis (IPA) approach to understand the lived experiences of participants regarding the challenges faced by the PNP in cybercrime investigations. Data familiarization began with repeated readings of interview transcripts to gain a comprehensive understanding of the participants' narratives.

Next, the researcher engaged in detailed initial noting by systematically examining each line of the interview and, making descriptive, linguistic, and conceptual comments related to the challenges faced by the PNP in cybercrime investigations. This thorough analysis allowed for a deep exploration of participants' accounts, capturing their detailed experiences and insights. Through this process, possible themes were identified by recognizing patterns, recurring ideas, and significant statements that reflected the major challenges encountered by the PNP.

Subsequently, the researchers linked sub-themes, organizing major themes from all participants; narratives to draw relationships within the data. Techniques such as abstraction (grouping similar themes) and subsumption (identifying overarching themes) helped highlight broader patterns in the data. This step synthesized the findings to highlight the challenges faced by the PNP in cybercrime investigation.

To ensure validity, reflexivity was employed throughout the research on the obstacles faced by the PNP in cybercrime investigation. As the sole researcher, a careful review of personal biases, assumptions, and perspectives was conducted to prevent influencing the interpretation of the findings. Regular reflection on how background and perceptions might affect the analysis was maintained to uphold neutrality. To validate the findings, feedback was obtained from relevant literature, cybercrime investigation experts, and peer reviewers to ensure that the interpretations accurately represented the challenges encountered by the PNP. These measures contributed to establishing credibility and reliability in the study's conclusions, resulting in a comprehensive and trustworthy understanding of the difficulties faced in cybercrime investigations.

Data Gathering Procedure

The researcher writes a letter address to the PNP Provincial Director of Cavite requesting for the conduct of study within his area of responsibility particularly the Cybercrime Unit. After securing approval, another letter was sent to the head of the Cybercrime Unit informing them of the intention of the researcher and schedule a meeting discussing the details of the study. A letter of request to the prospective participant discussing the research procedure and the intent to invite for an interview was distributed and consent was secured.

Furthermore, data collection procedures were outlined, how their information will be utilized, and giving participants the option to withdraw from the study at any time without consequences After securing the consent. The meeting with the participants was set up based on their respective availability and a written consent was secured to ensure compliance with confidentiality, including the signing of the non-disclosure agreement.

The researcher also discussed the objective of why the study is being conducted, the methods of research. With the participants' approval and consent, the interviews were recorded for accurate transcription. Each interview lasted approximately 1 hour and some were even longer, depending on the flow of the conversation and topics discussed.

The researcher also utilized written and typed notes to help the researcher track important points for future use in data analysis. The questions for the respondents were reviewed and structured in a respectful and clear manner to provide respondents the flexibility and freedom to express their ideas and opinions. To protect the data collected, stringent measures were implemented. The use of secure digital platforms for data storage, such as encrypted databases, is essential in preventing unauthorized access. Physical records were kept in locked filing cabinets, accessible only to the researcher.

After approval and finalization of the study, all records both physical and digital will be properly disposed of through shredding and secure data deletion using compliant data-wiping software. Backup copies of sensitive information will also be wiped out. These ethical measures protect participant rights and ensure data security. Additionally, obtaining approval from an institutional review board (IRB) or ethics committee before starting the research confirms that ethical standards are met, enhancing the study's credibility and integrity. This approach safeguards participant confidentiality, prevents data misuse, and maintains the integrity of the research. It also fosters trust among participants and stakeholders, ensuring the study adheres to ethical standards and regulatory requirements.

Ethical Considerations

The researcher ensured that all ethical considerations were meticulously addressed throughout the study. Participants were asked to fill out an informed consent form, which served as the basis for their voluntary participation. The researcher provided sufficient information about their involvement, ensuring transparency and understanding. The set of questions was carefully designed to avoid being offensive or discriminatory, respecting the feelings and emotions of the participants. In referencing related literature, the researcher acknowledged the authors, demonstrating adherence to academic integrity. The researcher committed to maintaining the highest levels of objectivity, honesty, and integrity in presenting the results. The study underwent a thorough review process by the Institutional Ethics Review Board.

Ethical considerations in the informed consent were strictly followed, including maintaining participant confidentiality by anonymizing data. Participants were informed of potential risks such as physical harm, emotional distress, or time loss (Barrow et al., 2022). These measures ensured ethical conduct and protected participants' well-being and rights.

Results and Analysis

This chapter summarizes and analyzes the findings from in-depth interviews with selected Cavite Provincial Police Office officials involved in cybercrime investigations. The research problems enumerated in Chapter I serve as the presentation guides.

Table 1. Demographic Profile

Respondent No.	Age (Year)	Sex	Degree	Rank/ Position	Year of service as a Cybercrime investigator	Number cases handled (per week)
Officer 1	35	Male	Bs Criminology	Police Staff Sergeant	4	30
Officer 2	34	Male	Bs Criminology	Police Staff Sergeant	4	20
Officer 3	31	Male	Bs Criminology	Police Corporal	3	15
Officer 4	30	Male	Bs Information Technology	Police Corporal	3	15
Officer 5	35	Female	Bs Information Technology	Police Chief Master Sergeant	3	10

This table presents the demographic and professional background of the five respondents involved in the study, concentrating on their age, gender, rank/position, and experience as cybercrime investigators.

Demographic Profile of Respondents

The participants of this study consisted of five (5) officers from the Cavite Provincial Police Office assigned to cybercrime investigation units. The respondents' demographic profile is critical in determining the scope and type of the issues they face, as various backgrounds, experiences, and organizational positions influence their approach to cybercrime investigations.

Age and Sex

The selected participants' ages ranged from 30 to 35 years old. The bulk of the police were male, which is consistent with the national demographics of law enforcement professionals in specialized units. Although gender was not expressly identified as a barrier in cybercrime investigations, it is critical to recognize that both male and female officers face similar systemic problems in their work environments. This composition mirrors findings from Nouh et al. (2019) who noted that cybercrime investigation remains a male-dominated field globally, although female participation is steadily increasing.

Educational Background

The highest educational attainment among respondents includes degrees in Criminology and Information Technology, highlighting a mix of traditional law enforcement education and specialized technical training pertinent to cybercrime investigations.

Rank/Position

Respondents' ranks varied, including Police Corporal, Police Staff Sergeant, and Police Chief Master Sergeant. This rank distribution is crucial because it demonstrates that obstacles exist at numerous organizational levels, not just for field investigators but also for supervisory officers. While higher-ranking officers had considerable administrative clout, they noted structural challenges such as a lack of up-to-date technologies, a manpower shortfall, and insufficient legal help when working with online platforms.

Years of Service in Cybercrime Investigation

The participants' years of service ranged from one (3) year to six (6) years in the field of cybercrime investigation. This variation allowed the study to capture a comprehensive range of experiences, from novice cybercrime investigators still undergoing foundational training to more seasoned officers who have witnessed the technological shifts in cyber-offending tactics over the years.

Number and Type of Cybercrime Cases Handled

Participants reported processing a rising number of cybercrime cases each weekly, ranging from 10 to 30 cases per officer. Common incidents included online fraud, cyber libel, identity theft, phishing, and cases of online sexual exploitation. Notably, numerous respondents emphasized the difficulty of dealing with multiple charges at the same time, such as identity theft and financial fraud.

Emerging Themes: Challenges Encountered by Cybercrime Investigators

The use of thematic analysis using Interpretative Phenomenological Analysis (IPA) identified severe concerns concerning the Cavite Provincial Police Office's cybercrime investigator. These findings are examined in line of the theoretical understanding based on the Social Construction of Technology

(SCOT) framework, which emphasizes how the social context shapes technology, including law enforcement systems, resources, and institutional capacity.

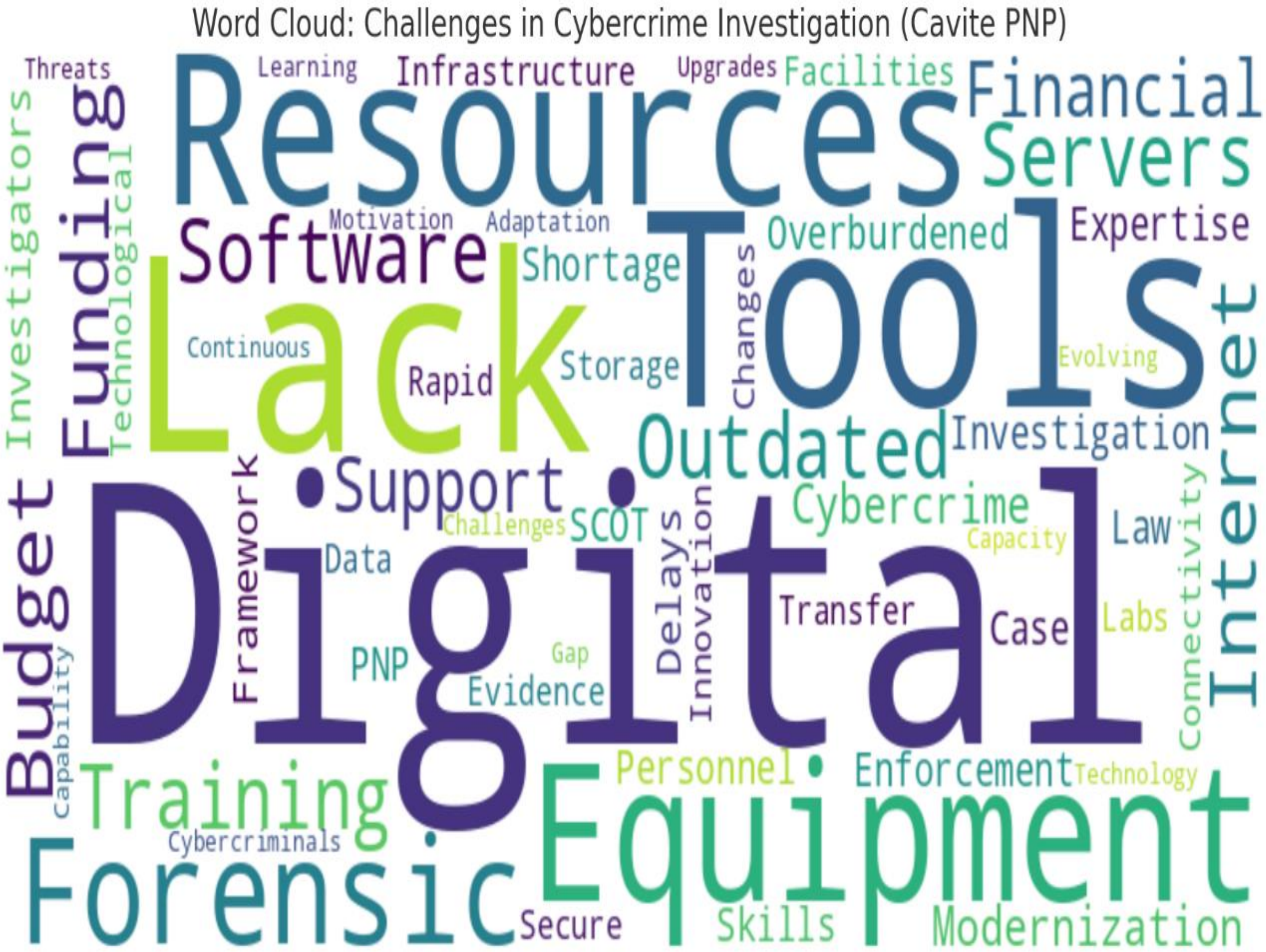


Figure 2. **Word cloud: Challenges Encountered by Cybercrime Investigators**

The word cloud visually highlights the most recurring and important concerns related to the challenges faced by the Cavite PNP in cybercrime investigations. Prominent words like **"resources," "tools," "funding," "digital," "forensic," "training,"** and **"technology"** reflect core issues such as lack of equipment, outdated systems, limited expertise, and rapid technological change. These challenges emphasize the urgent need for financial support, capacity building, and continuous learning to strengthen law enforcement's ability to combat evolving cyber threats.

This SCOT-based analysis reinforces that technological effectiveness in cybercrime investigation is socially constructed, and without addressing the underlying institutional and social structures, even the most advanced tools may fail to deliver meaningful change. This resource and skill gap not only weakens the PNP's investigative capacity but also makes it difficult to keep pace with evolving cybercriminal methods, which are often sophisticated and transnational. Therefore, the word cloud strongly conveys the urgent call for investment in law enforcement technology, improved access to quality training, and sustainable funding to enhance cybercrime response capabilities.

Technical limitations

A predominant challenge identified by the Cavite Provincial Police Office (PPO) in cybercrime investigations pertains to the significant gap between investigators' expertise and the technological resources available to them. This master theme, "Lack of Tools and Resources for Cybercrime Investigation," encapsulates several interconnected issues that hinder effective digital evidence collection, analysis, and case resolution. In vivo, one officer 1 lamented, *"Rarely do we have members in the PNP with knowledge in this area, but we do have some knowledge. The problem is, we lack the tools."* which directly reflects the core issue of resource scarcity. This sentiment underscores how the lack of modern forensic tools hampers the effective collection, preservation, and analysis of digital evidence, thereby impeding case resolution.

The investigative team has consistently expressed concerns regarding the inadequacy and obsolescence of their current tools and equipment. Officer 2 noted, *"Our resources are still insufficient, particularly high-tech tools needed for modern investigations,"* highlighting the gap in advanced technology. Officer 4 further elaborated, *"Our equipment mainly consists of secondhand computers; only one is new, and we lack access to modern digital forensic tools. Digital forensics is still relatively new to us."* These remarks emphasize that the hardware being used is largely outdated, which hampers the efficiency and reliability of digital forensic processes. Such outdated equipment not only causes delays in investigations but also increases the risk of compromising digital evidence integrity an essential factor in cybercrime cases.

The officer highlighted a notable deficiency in access to advanced forensic software necessary for tackling sophisticated cyber threats. Officer 3 emphasized this issue: *"We do not have enough modern tools yet."* This limited access impedes investigators' ability to utilize the latest technological solutions that are pivotal in analyzing complex cyber activities. The lack of updated tools constrains their capacity to keep pace with rapidly evolving cybercriminal tactics, thus reducing investigative effectiveness.

From a theoretical perspective, the SCOT framework interprets these technological challenges as socially constructed issues, influenced by institutional priorities and resource allocation. The persistent use of outdated tools and limited funding exemplifies how social, political, and economic factors stabilize and reinforce the "technology lock-in," preventing the adoption of innovative solutions necessary for modern cybercrime investigations.

Human resource issues

The shortage of qualified personnel and the consequent overextension of investigators represent a significant challenge in cybercrime response, with respondents highlighting that the rising volume of cases exceeds current expertise and capacity. Officer 2 emphasized the growing need for more specialized personnel due to increasing cybercrime incidents, stating, "With the increase in cybercrime, we need more expert personnel" while officer 4 noted the impact on workload and investigation completion, saying, *"We are severely lacking. Due to the volume of work, we, cybercrime investigators, often struggle to finish all the cases."* This personnel gap compromises the quality and timeliness of investigations, as officer 5 observed, *"We cannot always focus on each case individually, which causes investigations to take longer."* indicating that investigators are often overwhelmed, leading to delays and potential lapses in evidence management.

This scenario exemplifies the SCOT framework's concept of "technology stabilization," where institutional practices have become entrenched and resistant to change, despite the increasing complexity and demand for specialized digital skills in cybercrime investigation.

Furthermore, the personnel shortage has broader implications beyond case resolution. It affects organizational morale, staff retention, and the attractiveness of cybercrime investigation as a career path. Investigators working under persistent overload may experience burnout, leading to higher turnover rates and a less experienced workforce, which exacerbates the cycle of inadequate capacity.

This observation aligns with prior research by Bossler et al. (2019) and Akinduko & Odeyemi (2021), both of which identify the insufficient number of well-trained investigators as a major obstacle to effective cybercrime law enforcement. Bossler et al. (2019) point out that without adequate expertise in digital forensics, cybersecurity, and cyber law, law enforcement agencies find it difficult to keep up with the rapidly changing nature of cyber threats, leading to delays, errors in interpreting digital evidence, and a decline in overall effectiveness in resolving cybercrimes. Similarly, Akinduko & Odeyemi (2021) highlight the importance of specialized training and continuous professional development for cybercrime investigators, suggesting that the absence of such training hampers law enforcement's ability to respond quickly and effectively to complex cyber incidents.

Facilities and infrastructure limitations

Another critical challenge identified pertains to inadequate infrastructure and facilities essential for digital evidence analysis. Respondents revealed that the current laboratory conditions, server rooms, and storage capabilities are insufficient to support the volume and complexity of cybercrime investigations. Officer 2 stated, *"Honestly, there is a lack of facilities and inventory. For example, our labs, such as the server rooms, are insufficient, which affects our ability to analyze digital evidence effectively."* highlighting the infrastructural deficits that hinder timely and secure digital forensic work.

The absence of dedicated, application, reliable internet connectivity and complete infrastructure is needed the ability to secure, store, transfer, and analyze digital evidence. Officer 3 emphasized, *"We need secure storage servers and a reliable internet connection to speed up data transfer." which underscores the importance of robust infrastructure for operational efficiency.* Without these facilities, digital evidence becomes vulnerable to tampering, loss, or delays in processing, ultimately affecting the integrity of investigations.

Beyond operational delays, the infrastructural inadequacies also affect investigator morale and motivation. Investigators working under subpar conditions may experience frustration and decreased job satisfaction, leading to higher turnover rates and difficulty attracting qualified personnel. This creates a vicious cycle where insufficient infrastructure leads to lower morale, further exacerbating human resource shortages.

Applying SCOT, this theme illustrates how social and institutional factors such as budget limitations and organizational priorities result in stabilized but inadequate infrastructure. The lack of investment reflects societal decisions that have not prioritized the technological needs of law enforcement, thus creating a social environment where outdated or insufficient facilities persist.

Consistent with the findings of Doe and Smith (2022), inadequate infrastructure hampers digital forensic capabilities, leading to delays and increased risks of evidence compromise. The need for improved facilities is critical in aligning technological capabilities with the demands of modern cyber investigations.

Financial constraints

The main theme is that financial constraints significantly hinder the effectiveness of cybercrime investigation units. Respondents often cover personal expenses like transportation, which lowers motivation and responsiveness. Officer 1's statement, *"All of our transportation expenses are covered by us."* highlights the lack of operational allowances, adding financial strain on investigators. This situation affects morale and hampers their ability to carry out timely and efficient investigations.

Furthermore, participants emphasized the critical lack of sufficient funding to acquire and upgrade essential technological tools. Officer 2 mentioned, *"The challenge is the funding support needed to purchase equipment."* and officer 3 pointed out, *"There is really a need for funding support to update the tools required by the investigators."* highlighting the urgent need for financial resources to purchase modern forensic software and high-performance hardware systems. Without adequate funding, investigators are forced to rely on outdated equipment, which hampers their ability to analyze complex cybercrimes effectively. Outdated tools can cause delays in investigations, reduce the accuracy of digital evidence analysis, and ultimately decrease the overall success rate in solving cybercrimes.

This issue aligns with the findings of Widodo et al. (2024) and Jocson and Espiritu (2023), who highlight that insufficient funding is a major barrier to advancing law enforcement's technological capabilities. Without adequate financial resources, efforts to modernize equipment, upgrade software, and expand investigative capacities are severely limited. This financial shortfall hampers the ability of cybercrime units to keep pace with evolving digital threats, ultimately restricting their effectiveness and progress in combating complex cybercrimes.

The implications of these financial constraints are far-reaching. Limited funding not only constrains the acquisition of cutting-edge technology but also affects ongoing training, capacity building initiatives, and the recruitment of specialized personnel. Furthermore, investigators working under resource-limited conditions may experience decreased morale, which can lead to higher turnover and a reduced sense of organizational support.

Challenges Posed by Rapid Technological Changes

The main theme, "Challenges Posed by Rapid Technological Changes," discusses how hard it is for the Philippine National Police to keep up with how quickly criminal technology changes. Cybercriminals are always coming up with new ways to do bad things such as digital tools, platforms, and techniques to improve quickly. Law enforcement agencies like the PNP are often left behind when it comes to new technology because they don't have enough funding, training, or system upgrades.

The rapid evolution of cyber threats presents an ongoing challenge to law enforcement. Respondents expressed anxiety over the swift pace at which cybercriminals develop new methods. Officer 2 remarked, *"Every time we adopt new technology, cybercriminals also quickly find ways to exploit it".* illustrating the continuous race between technological advancement and criminal adaptation.

This constant arms race creates a scenario where investigators struggle to keep pace with emerging techniques such as hacking, phishing, and social engineering. The speed of technological change often outstrips the capacity of police units to adapt through training or infrastructure upgrades. From a social construction perspective, this dynamic demonstrates how societal pressures such as the need to combat innovative cyber threats drive the ongoing development and stabilization of investigative tools and procedures.

This highlights the SCOT (Social Construction of Technology) concept that technology is dynamic and shaped by ongoing social and technical forces. In cybercrime investigation, law enforcement agencies must engage in continuous development, training, and adaptation to keep pace with rapidly evolving digital threats. Without sustained efforts to update skills and tools, investigations risk becoming obsolete as cybercriminals adopt new methods. Horan and Saiedian (2021) and Moloney et al. (2022) emphasize that ongoing innovation and learning are crucial for overcoming limitations in current knowledge and technological capabilities. By embracing continuous improvement, law enforcement can better respond to emerging cyber threats and enhance their investigative effectiveness.

Assess the current training programs available to the Cybercrime Unit

The current training programs available to the Cybercrime Unit show both strengths and areas for improvement. Based on participant feedback, the programs generally provide foundational knowledge, particularly through courses on the fundamentals of cybercrime and technical aspects of investigations. These offerings have been described as "helpful," especially when delivered through formal channels like police schooling or agency-led seminars.

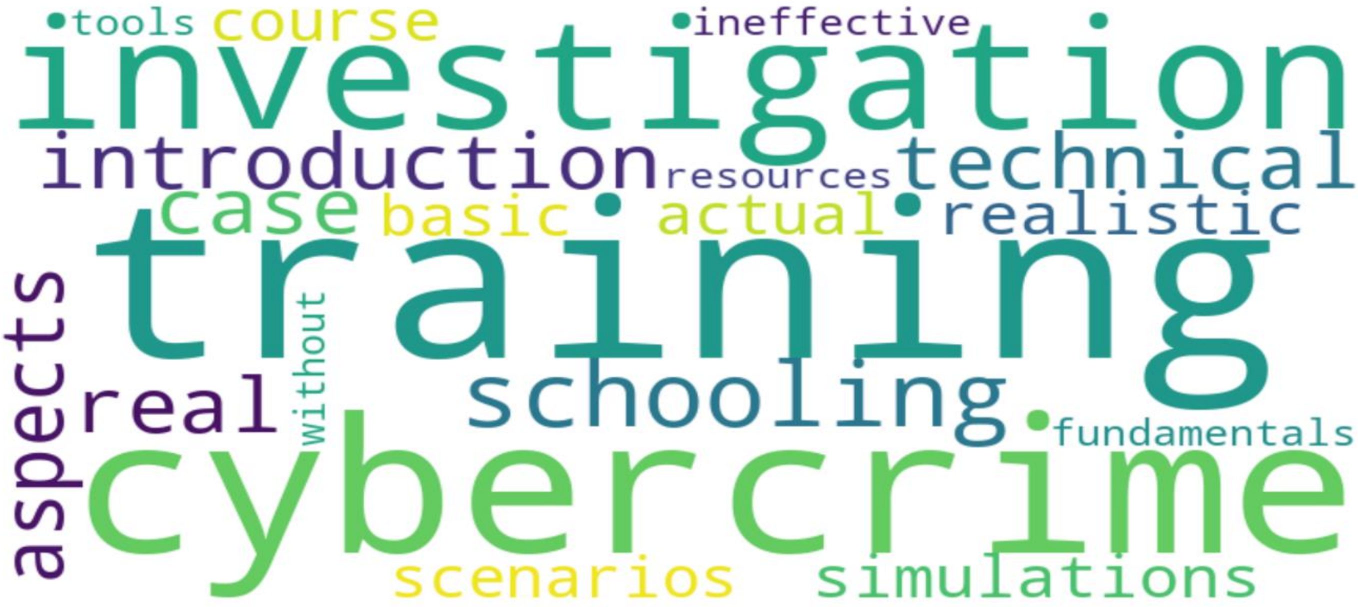


Figure 3. **Word cloud: Assess the perceived relevance and effectiveness of current training programs**

The word cloud visually represents the most frequently mentioned and thematically significant words derived from participants' in vivo statements regarding the effectiveness and challenges of their training programs in cybercrime investigation. Prominent words such as **"training," "cybercrime," "investigation," "tools,"** and **"real-case simulations"** highlight the core areas emphasized by the participants.

The prominence of the word **"training"** reflects the participants' focus on the overall quality and structure of the training they receive. Words like **"cybercrime"** and **"investigation"** underscore the specific domain in which the training is applied, while **"tools"** indicate a perceived gap in resources needed to conduct effective investigations. Additionally, the appearance of **"real-case simulations"** and **"realistic scenarios"** reveals the value that trainees place hands on, practical experiences over purely theoretical instruction.

This visualization supports the thematic findings in the table, particularly the subthemes such as *"Perceived Gaps in Current Training"* and *"Training Without Resources is Ineffective."* It provides a quick yet meaningful snapshot of participant priorities and the areas where improvements are most needed. In essence, the word cloud helps to reinforce the narrative that while training exists, its effectiveness is hindered without adequate tools and realistic, experiential learning.

Table 3. Assess the perceived relevance and effectiveness of current training programs

Master Theme	**Themes**	**In Vivo Statements**	**Participants**
Training and Professional Development	Perceived Gaps in Current Training	*"Wala pa ma'am lahat kami introduction to cybercrime lang."*	P1
		"Ok naman yung sa training or schooling namin, provided naman po ni PNP… helpful naman especially technical aspects." *"Actually, ma'am yung real-case simulations during training yung pinaka-nakatulong kasi na-expose kami sa mga Realistic scenarios, kaya mas handa kami sa Actual investigations."*	P2 P3
		May basic cybercrime course ako na Tinuturo nila yung mga fundamentals ng cybercrime Schooling kaya ok naman training	P4

	Training Without Resources is Ineffective	*Marami nga mgatraining pero,* *Wala naman kaming mga tools na pwede sana Magamit naming sa investigation.*	P5

Training and Professional Development

The master theme "Training and Professional Development" emphasizes the crucial role of ongoing education, skills enhancement, and formal capability-building for PNP personnel assigned to cybercrime investigation. As technology advances rapidly, so do the techniques used by cybercriminals—requiring investigators to continuously adapt and upgrade their knowledge and competencies. Grobler and Louwrens (2022) highlight the importance of regular training needs analysis to align law enforcement skills with rapidly evolving digital threats.

This approach ensures that personnel remain current with the latest investigative methods and cyber defense strategies, thereby enhancing their effectiveness in combating cybercrimes. Additionally, continuous professional development fosters a culture of learning within law enforcement, which is essential for maintaining operational readiness and adapting to the complex and dynamic nature of cyber threats. According to Albrecht et al. (2019), ongoing training not only improves technical proficiency but also boosts investigators' confidence and decision-making capabilities, ultimately leading to more successful case resolutions and improved cybersecurity resilience.

Perceived Gaps in Current Training

The respondents unanimously acknowledged the importance of training but pointed out significant limitations in the current programs. P1 remarked, *"Wala pa ma'am lahat kami introduction to cybercrime lang,"* indicating that the existing training provides only a superficial overview of cybercrime, primarily at an introductory level. This suggests that the training content is not sufficiently specialized or advanced to meet the complexities of modern cyber threats. Such a gap leaves investigators underprepared for handling sophisticated digital crimes, which continually evolve in techniques and scope.

Participants also expressed appreciation for the foundational training supplied by the PNP. P2 stated, *"Ok naman yung sa training or schooling namin, provided naman po ni PNP…* helpful naman especially technical aspects," reflecting that current programs serve as useful starting points. Similarly, P4 added, *"May basic cybercrime course ako na tinuturo nila yung mga fundamentals ng cybercrime. Schooling kaya ok naman training."* These statements highlight that while basic knowledge is being imparted, it is insufficient for tackling the advanced and dynamic nature of cybercrimes.

Pasinhon and Donato (2024) underscore that access to modern forensic tools is essential for translating theoretical knowledge into practical, operational capabilities within law enforcement agencies. When investigators lack the necessary technological resources, even comprehensive training programs risk becoming superficial or ineffective, as there are no functional tools to apply learned skills in real investigations.

Training Without Resources is Ineffective

A critical challenge identified is the disconnect between training and practical resource availability. P5 pointed out*, "Marami nga mga training pero wala naman kaming mga tools na* *pwede sana magamit namin sa investigation,"* illustrating that training alone is insufficient without the necessary technological resources. This gap severely limits the application of learned skills, as investigators lack access to digital forensic software, specialized tools, and hardware essential for effective case investigation.

This challenge exemplifies the social construction of technology, where the perception of what constitutes "adequate training" is shaped by organizational resource availability. The institutional focus on training without parallel investments in tools creates a misalignment, leading to underutilization of skills and frustration among investigators.

This mismatch between training and practical application creates a frustrating dynamic for investigators. According to the SCOT (Social Construction of Technology) framework underpinning this study, the interpretive flexibility of technology explains how institutional perceptions of what constitutes & adequate training; differ greatly from frontline investigators' needs. While administrative agencies may perceive introductory courses as sufficient, investigators themselves experience technology as a rapidly evolving and highly specializeddomain requiring continuous, real-world based skill development.

Need for Advanced and Updated Training Resources

The provided word cloud visually represents the most frequently mentioned concepts by participants regarding digital forensic training. The size and prominence of words in the cloud indicate their importance and how often they were referenced in the data. Overall, the visualization underscores the participants' collective emphasis on the critical need to enhance digital forensic capacity through updated, comprehensive, and advanced training methods. It highlights key themes such as foundational knowledge, continuous education, specialized skills, and practical application of tools, all aimed at equipping law enforcement officers to better combat evolving cyber threats.

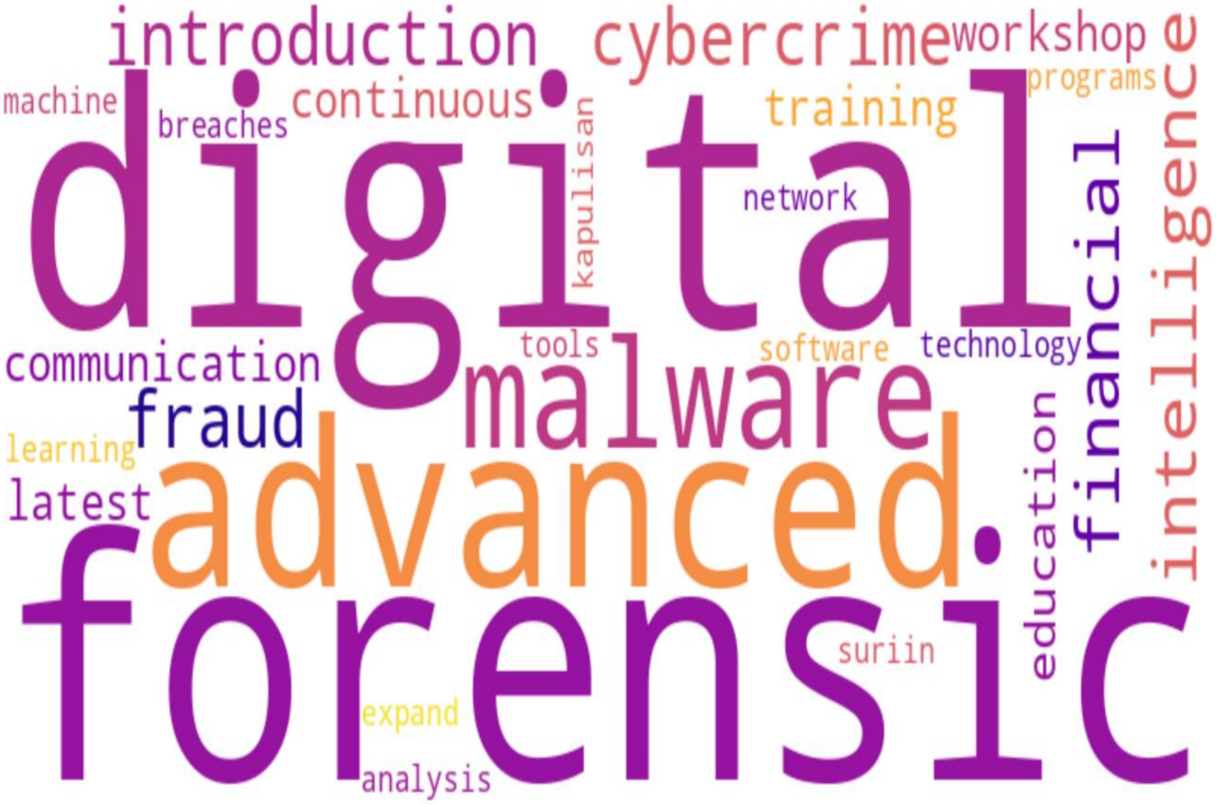


Figure 4. **Word cloud: Need for Advanced and Updated Training Resources**

This passage describes a word cloud that visually displays the most frequently mentioned ideas and concepts shared by participants regarding the training needs for digital forensics. In a word cloud, words that appear more often are shown larger and more prominently, indicating their importance in the data. The overall message from the word cloud is that there is a strong consensus on the need to improve digital forensic capabilities through more updated and advanced training programs.

Participants emphasize the importance of starting with basic understanding. Words like "Introduction," "cybercrime," "digital forensic," "financial fraud," and "intelligence"

Continuous Education and New Technologies There's a clear call for ongoing learning, indicated by terms such as "continuous," "education," "training," and "workshop." Participants want regular updates to keep pace with rapidly evolving technology. Keywords like "machine learning" and "software" highlight the importance of familiarizing officers with modern investigative tools that can improve their effectiveness.

Participants desire more advanced and specialized modules. The word "expands" paired with "advanced digital forensic" suggests a need to go beyond basic knowledge. This includes training on complex topics like "malware analysis" and "network breaches," reflecting the increasing sophistication of cyber threats and the need for targeted expertise. The focus here is on practical skills. Words such as "tools," "malware programs," and "network" emphasize hands-on training with real software and systems.

Table 4. Additional upgraded training

Master Theme	Themes	In Vivo Statements	Participants
Need for Advanced and Updated Digital Forensic Training	Introduction and Foundational Topics	*"Yan apat ma'am yung introduction to cybercrime, digital forensic and financial fraud, intelligence communication."*	P1
	Continuous Education in New Technologies	*"Continuous education or additional training workshop On the latest technology machine learning Digital forensic software is more effectively."*	P2
	Expansion of Advanced Digital Forensics	*"More on advanced digital forensic training i expand pa."*	P3
	Specialized	*"Para ma enchance siguro yung training sa Malware analysis kasi*	P4

	Malware and Network Security Training Utilization of Advanced Tools	*matutunan ng mga kapulisan kung paano suriin ang malware programs at paano kumakalat yan mga yan at kung paano maiiwasan at kung paano maiiwasan ang mga network breaches.”* *"Advanced digital forensic tools".*	P5

Need for Advanced and Updated Training Resources

The master theme "Need for Advanced and Updated Training Resources" represents the participants’ collective recognition of the critical necessity for continuous, more advanced training to ensure their skills remain current and effective in tackling cybercrime investigations. This aligns with the SCOT perspective, highlighting how law enforcement agencies actively shape and are shaped by technological advancements, necessitating ongoing adaptation through training.

Introduction and Foundational Topics

The theme "Introduction and Foundational Topics" was reflected in the statement: *"Yan apat ma’am yung introduction to cybercrime, digital forensic and financial fraud, intelligence communication."* (P1). This indicates that practitioners still regarded basic digital forensic areas as essential, emphasizing the importance of foundational knowledge in their training. P1 highlighted the need to reinforce these core topics, suggesting that there was either a gap in initial training or a necessity to refresh fundamental concepts among practitioners.

Continuous Education in New Technologies

The theme "Continuous Education on New Technologies" was derived from P2’s statement: *"Continuous education or additional training workshop on the latest technology, machine learning, digital forensic software is more effective."*

This statement highlights that P2 recognized the importance of ongoing training to keep up with rapidly evolving technological trends, including machine learning and advanced digital forensic software.

Expansion of Advanced Digital Forensics

The theme "Expansion of Advanced Digital Forensics" was derived from P3’s statement: "More on advanced digital forensic training i expand pa." This indicated that P3 sought more comprehensive and in-depth training in advanced digital forensics, suggesting that the existing training programs were viewed as too basic or inadequate for managing complex investigations. P3’s desire to expand training efforts reflected an understanding of the necessity to develop more specialized skills and knowledge to effectively confront the increasingly sophisticated nature of digital crimes.

Specialized Malware and Network Security Training

P4 emphasized the need to enhance training in malware analysis, noting that *"para ma-enhance siguro yung training sa malware analysis... kung paano suriin ang malware. at kung paano maiiwasan ang mga network* *breaches."* This statement demonstrated an understanding that malware impacts networks, and that proper analysis is essential in preventing breaches. It highlighted a practical requirement for law enforcement to develop deeper expertise in malware and network security to effectively address cyber threats.

Utilizing advanced digital forensic tools

P5 emphasized the importance of advanced digital forensic tools by simply stating, "Advanced digital forensic tools," highlighting the need for better access and proficiency. This supports the theme that modern training should focus on practical, hands-on use of such tools.

.

Coping Mechanisms and Strategies of Cybercrime Investigators

To effectively address the numerous challenges faced in cybercrime investigations, law enforcement officers employ various coping mechanisms and strategies. These approaches help them manage constraints such as limited resources, outdated tools, personnel shortages, and the rapid pace of technological change. Understanding these strategies provides insight into how investigators sustain their operational effectiveness despite systemic limitations

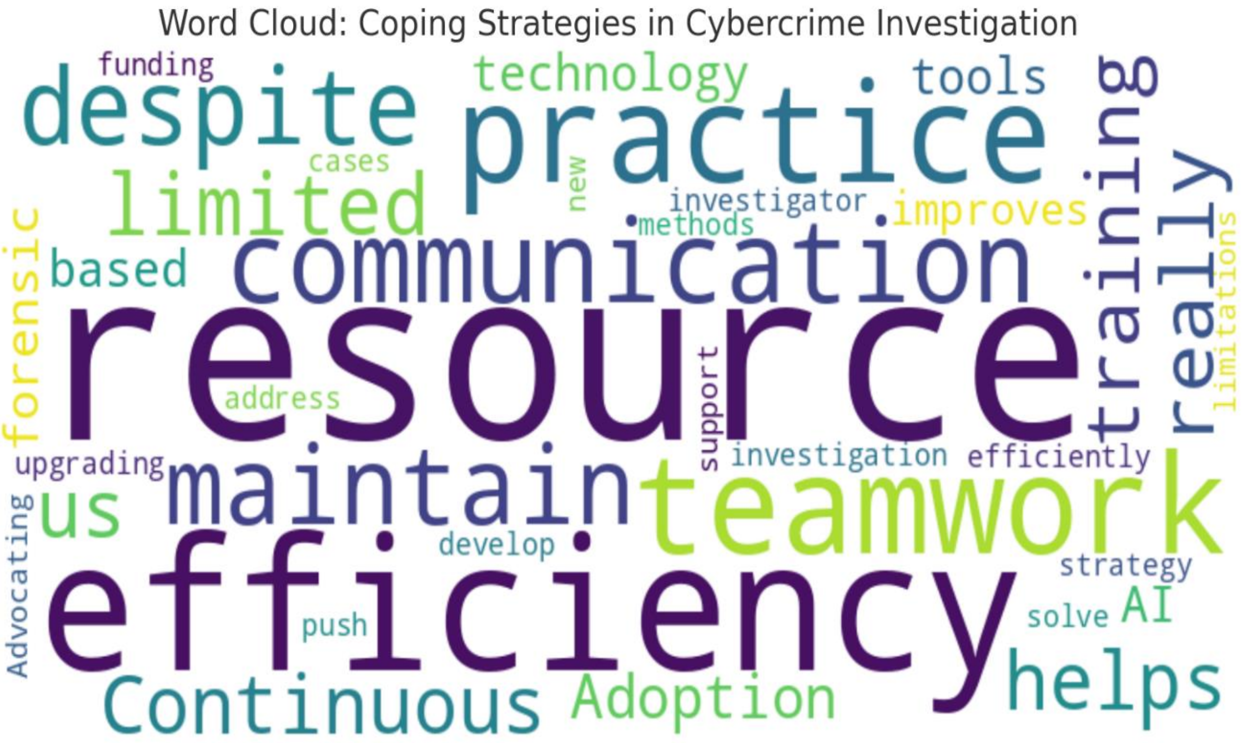


Figure 5. **Coping Strategies in Cybercrime Investigation**

The word cloud generated from participants' in vivo statements highlights key coping strategies used in cybercrime investigations. Prominent words such as *"resources"* and *"efficiency"* suggest that these are major concerns among investigators when handling complex cases. Terms like *"training," "communication," "technology,"* and *"teamwork"* also appear frequently, emphasizing the value placed on collaboration, continuous learning, and the integration of modern tools in improving investigative outcomes. These words reflect the participants' efforts to maintain effectiveness despite resource limitations and technological constraints.

The analysis further reveals that resource limitations are a recurring challenge, aligning with the participants' advocacy for more institutional support and funding. The repeated mention of *"efficiency,"* along with words like *"AI," "methods,"* and *"develop,"* illustrates a proactive approach in adopting innovative techniques and technologies. The overall thematic alignment with concepts like *Effective Investigation*, *Training*, *Technology Adaptation*, and *Advocacy* supports the study's findings. This also highlights the participants' focus on practical strategies and continuous improvement to strengthen cybercrime investigation under evolving digital threats.

Table 5. Coping Strategies in Cybercrime Investigation

Master Theme	**Themes**	**In Vivo Statements**	**Participants**
Effective Cybercrime Investigation.	Continuous Training and Skill Development	*"Nagpapractice kami teamwork at communication para mapanatili ang efficiency kahit limitado ang resources."*	P1
		"Continuous Training yan po yung makakatulong samin."	P2
	Adapting and Upgrading Technology	*"Adaption of technology AI-based forensic tools to improve investigation efficiency.*	P3
	Advocacy for Support and Resources	*"As investigator mag develop new methods to solves case Efficiently and resources upgrading funding ma'am."*	P4
		"Advocating support and resources is a strategy to address resource limitations."	P5

Effective Cybercrime Investigation

The master theme "Effective cybercrime investigation" highlights how cybercrime investigators in Cavite Provincial Police Office use proactive and adaptive approaches to overcome challenges like limited resources, technological gaps, and evolving cyber threats. These strategies are essential for maintaining effective operations and ensuring successful digital investigations.

The theme of **"Continuous Training and Skill Development"** is reflected in the in vivo statements from investigators. P1 mentions, *"Nagpapractice kami teamwork at communication para mapanatili ang efficiency kahit limitado ang resources,"* highlighting their focus on teamwork and communication to stay effective despite resource limitations. Similarly, P2 states, *"Continuous Training yan po yung makakatulong samin,"* emphasizing the importance of ongoing learning.

This demonstrates that investigators actively work to build their capabilities through regular practice and collaboration. Even when faced with outdated equipment or limited access to advanced tools, they prioritize developing their skills and working cohesively. This aligns with the idea that human capital—especially continuous training and teamwork—serves as a vital coping mechanism in resource-constrained environments, enabling them to adapt and remain effective in complex cybercrime investigations. It reflects a resilient approach where officers compensate for systemic deficiencies by enhancing their procedural and interpersonal skills.

From a theoretical perspective, SCOT highlights that human actors shape and adapt technology based on their social context. In resource-limited settings, investigators rely on their skills, teamwork, and ongoing training to cope with systemic constraints. Their commitment to these practices acts as a social construct that compensates for technological gaps, influencing how technology is utilized and improved.

This theme of **"Adapting and Upgrading Technology"** highlights the strategic focus of investigators on leveraging technological innovation to surmount investigative challenges in cybersecurity. The in vivo statements such as the adoption of AI-based forensic tools (P3) and the development of new methods alongside resource upgrades (P4) highlight a proactive, forward-looking approach driven by the evolving landscape of cyber threats and digital evidence complexity.

From the perspective of the Social Construction of Technology (SCOT) framework, this demonstrates how law enforcement officers actively shape and respond to technological advancements. Their efforts to integrate AI tools and develop novel investigative methods reflect an adaptive process wherein social actors influence technological trajectories to meet operational needs. Furthermore, their emphasis on resource upgrading signifies an understanding that technological agility and continuous innovation are essential for maintaining investigative efficacy in a rapidly changing digital environment.

This dynamic aligns with existing literature (Gomez et al., 2024; Klein & Kleinman, 2020), emphasizing that technology in law enforcement is not a static artifact but a socially constructed and evolving tool, shaped by the motivations, resource availability, and strategic responses of its users. Consequently, this underscores the importance of organizational flexibility and ongoing technological investment as critical components for effective cybercrime investigation in the digital age.

This theme of **"Advocacy for Support and Resources"** highlights the proactive role of law enforcement officers in addressing systemic resource limitations within cybersecurity investigations. The in vivo statement (P5) underscores how officers actively engage with higher authorities and stakeholders to secure necessary organizational and financial support.

From a theoretical perspective, this strategy reflects the application of organizational behavior principles, emphasizing that advocacy and proactive communication are vital in resource-constrained environments (Bossler et al., 2019). The officers' recognition of resource deficiencies such as outdated equipment and inadequate facilities demonstrates an awareness that sustainable improvements in cybercrime investigation depend on systemic change driven by internal advocacy and external support.

This approach aligns with the social construction of technology (SCOT) framework, illustrating how social actors law enforcement personnel actively influence resource allocation and organizational priorities through their advocacy efforts. Overall, it underscores the importance of institutional support and systemic change in enhancing investigative capacity amid resource constraints, emphasizing that technological and operational advancements are contingent upon effective resource mobilization and policy influence.

Enhancing operational effectiveness

To effectively capture and communicate the central ideas expressed by participants concerning the theme of Enhancing Operational Effectiveness, a word cloud was created based on their in vivo statements collected during interviews.

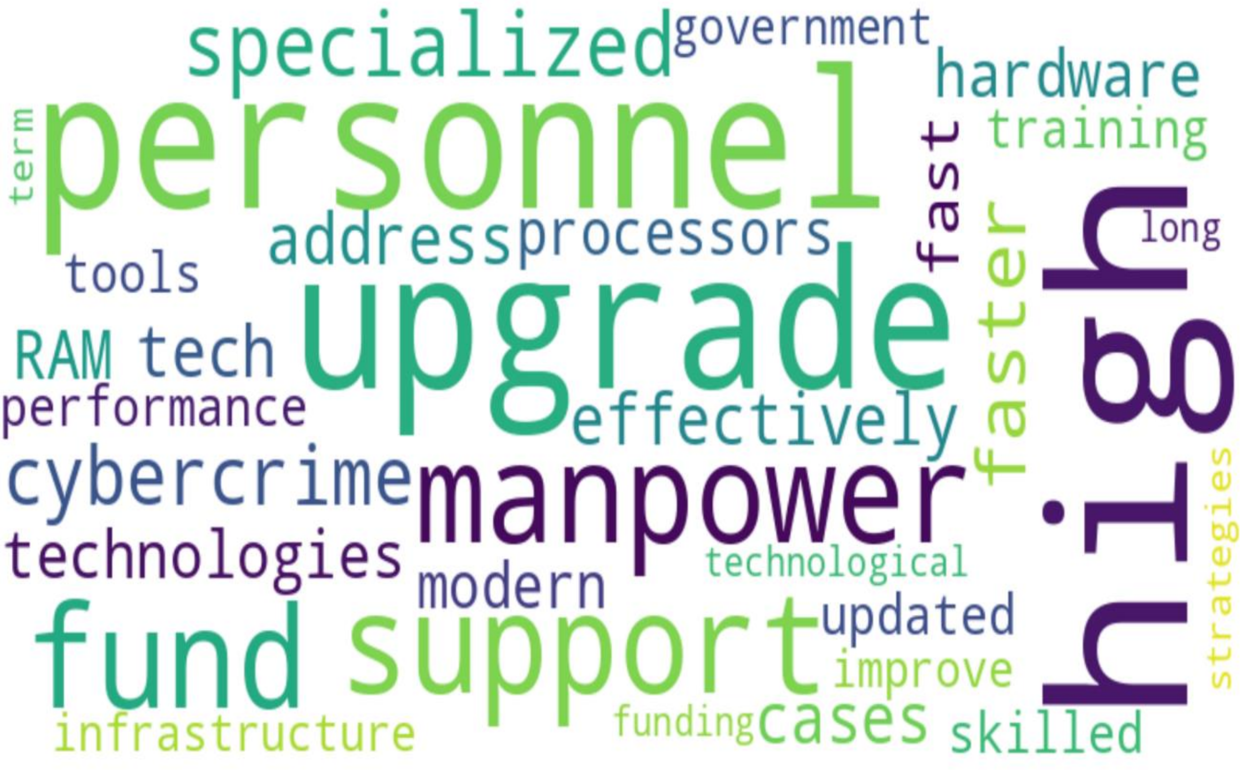


Figure 6. **Enhancing operational effectiveness**

To visualize the core ideas shared by participants regarding the master theme of *Enhancing Operational Effectiveness*, a word cloud was generated using the in vivo statements collected during the interview process. The word cloud serves as a qualitative tool that graphically presents the frequency and significance of words mentioned by the participants, offering an at-a-glance representation of their priorities and insights. The size of each word in the word cloud correlates with its prominence or repetition across the dataset.

Table 6. Enhancing operational effectiveness

Master Theme	Themes	In Vivo Statements	Participants
Capacity Building	Manpower and Funding Support	*"Una una ma'am yung manpower and fund support."*	P1
	Specialized Personnel and Advanced Technology	*"Additional specialized personnel na focus on cybercrime To make it faster and more effectively to address the cases And have higher tech technologies."*	P2
	Infrastructure and Technological Upgrades	*"Pag-upgrade ng Hardware yung high RAM at fast processors... more modern and high-performance hardware."*	P3
		"Pondo ma'am at training Kailangan din ng mas maraming Skilled personnel at updated na tools." *"Magdadag siguro ng pondo at support ng government Para ma improve yung infrastructure at technological Upgrades yung pang long term funding strategies."*	P4 P5

Capacity Building

The master theme of "Capacity Building" pertains to the strategies, initiatives, and resources dedicated to improving the cybercrime units' skills, knowledge, tools, and infrastructure within the Philippine National Police (PNP). It focuses on enhancing operational effectiveness through the development of personnel, technological improvements, and the establishment of sustainable funding sources.

Manpower and Funding Support

The theme "Manpower and Funding Support" was highlighted by Participant P1, who stated, *"Una una ma'am yung manpower and fund support."* This underscored the recognition that sufficient staffing and financial resources were essential for effective cybercrime investigations. The participant emphasized the urgent need for increased personnel and government funding to address the growing volume and complexity of cybercrimes. Without adequate manpower and funds, investigations were delayed, and the ability to respond quickly and thoroughly was constrained.

This observation is consistent with findings in cybersecurity literature, which assert that proper resource allocation is fundamental to strengthening investigative capabilities and ensuring timely responses to cyber threats (Johnson, 2020).

Specialized Personnel and Advanced Technology

The theme "Specialized Personnel and Advanced Technology" was reflected in Participant 2's statement, where they mentioned the need for *"additional specialized personnel na focus on cybercrime to make it faster and more effectively to address the cases and have higher tech technologies."* This highlights how important it is to train or hire experts with specific skills in cybercrime investigation. The participants understand that using advanced technological tools is essential for making investigations quicker and more effective. Building specialized expertise and embracing the latest technology are key steps in strengthening capacity, allowing investigators to better handle complex digital evidence and stay ahead of evolving cyber threats.

Participants acknowledged that leveraging advanced technological tools is essential to boost both the speed and efficiency of cases. Emphasizing the development of specialized skills and the integration of state of the art technology aligns with best practices in capacity building, as research shows that combining human expertise with technological innovation significantly improves digital evidence handling and cyber threat response (Choo, 2020).

Infrastructure and Technological Upgrades

The theme "Infrastructure and Technological Upgrades" reflected the participants' shared recognition of the need to enhance technological tools and physical systems to meet modern demands. Participant 3 emphasized the importance of upgrading equipment, stating the need for *"high RAM at fast processors... more modern and high-performance hardware,"* which indicated a call for better computing capability to support operations. This suggested that outdated or underperforming devices hindered productivity and effectiveness in their work.

In addition, Participant 4 highlighted the necessity of both financial resources and skills development, noting, *"Pondo ma'am at training Kailangan din ng mas maraming skilled personnel at updated na tools."* This statement demonstrated that infrastructure alone was insufficient without qualified individuals and up-to-date equipment, implying a connection between technological development and human resource readiness.

Furthermore, Participant 5 called for sustained investment, saying, *"Magdadag siguro ng pondo at support ng government Para ma-improve yung infrastructure at technological upgrades yung pang long term funding strategies."* This emphasized the importance of long-term planning and government support to ensure that improvements in infrastructure and technology were not temporary but part of a strategic, sustainable effort.

Summary of Findings

Following are the summary of findings obtained through the conduct of this study including the conclusions and recommendation formulated by the researcher. Using Interpretative Phenomenological Analysis (IPA) as the primary method and guided by the Social Construction of Technology (SCOT) theoretical framework, the study captured the real-world operational struggles faced by investigators handling increasingly complex cybercrime cases.

I. Demographic Profile

1. The participants were mostly male, aged 30 to 35, with one female officer, reflecting typical gender trends in specialized law enforcement units. While gender wasn't seen as a direct barrier, both male and female officers face the same systemic challenges. This aligns with Nouh et al. (2019), who observed that cybercrime investigation is still male dominated, though female involvement is gradually rising.

2. Respondents held ranks from Police Corporal to Police Chief Master Sergeant, showing that challenges affect both field and supervisory levels. Despite their authority, higher-ranking officers still face issues like outdated technology, limited personnel, and lack of legal support when dealing with online platforms.

3. Participants had between 3 to 6 years of experience in cybercrime investigation, offering a mix of fresh and experienced perspectives. This range helped highlight both initial training challenges and the evolving nature of cybercrime over time.

4. Participants handled 10 to 30 cybercrime cases weekly, including online fraud, cyber libel, identity theft, phishing, and online sexual exploitation. Many noted the challenge of managing cases with multiple overlapping offenses like identity theft and financial fraud.

II. Challenges Faced by the PNP in Cybercrime Investigations

1. The Cavite PNP faces multiple interconnected challenges that hinder effective cybercrime investigation. Key issues include a significant gap between their knowledge and the available tools, with officers possessing theoretical expertise but lacking access to modern, high-tech equipment. Outdated and insufficient hardware, such as secondhand computers and limited software access, impede digital forensic processes and slow down investigations.

2. Infrastructural deficiencies also pose critical barriers, with inadequate laboratory facilities, insecure storage, and unreliable internet connectivity affecting the secure handling and analysis of digital evidence. These infrastructural gaps limit operational efficiency and increase risks to evidence integrity.

3. Personnel shortages and a lack of specialized expertise further strain the investigative capacity. Overburdened investigators, due to insufficient staffing and training, struggle to manage the rising volume and complexity of cybercrime cases, leading to delays and reduced investigation quality.

4. Financial constraints are a pervasive issue, with inadequate funding restricting access to updated tools, software, and hardware necessary for modern investigations. Investigators often shoulder personal expenses, which affects morale and productivity.

5. Additionally, the rapidly evolving nature of cyber threats presents an ongoing challenge. Cybercriminals quickly adapt and develop new techniques, outpacing law enforcement's efforts to upgrade skills and technology. This dynamic arms race underscores the need for continuous training, adaptation, and investment in emerging technologies.

III. Assessment of Training Programs

1. Participants generally recognize that current training programs provide foundational knowledge in cybercrime, with some highlighting the helpfulness of technical

aspects and real-case simulations that prepare them for actual investigations. For instance, some participants appreciate the exposure to realistic scenarios, which they find valuable for their preparedness. Conversely, there is a notable concern regarding the limited scope of training, with one participant mentioning that the training only covers basic introduction to cybercrime, indicating a perceived gap in comprehensive coverage.

2. Furthermore, participants emphasize that training alone is insufficient if not accompanied by adequate resources. Several respondents point out that despite having undergone training, the lack of necessary tools hampers the practical application of their skills, rendering training less effective in real-world investigations. Overall, while current training programs are viewed as somewhat relevant and helpful, their effectiveness is hindered by resource limitations and the need for more comprehensive, practical, and advanced training modules.

IV. Additional training programs

1. Participants identify a critical need for ongoing and advanced digital forensic training to keep pace with evolving cyber threats. They emphasize the importance of foundational topics such as cybercrime, digital forensic methods, financial fraud, and intelligence communication, highlighting that continuous education in these areas enhances investigative effectiveness.

2. There is a strong call for expanding training programs to include more advanced digital forensic techniques, particularly in malware analysis and network security. Participants recognize that specialized training in malware detection, analysis, and understanding how malware spreads is essential for preventing and responding to cyber incidents effectively.

3. Furthermore, the utilization of advanced forensic tools is seen as vital in strengthening investigative capabilities. Training that incorporates the latest forensic software and tools will enable law enforcement officers to analyze complex cyber threats more efficiently, better protect networks, and prevent breaches.

V. Coping Strategies in Cybercrime Investigation

1. Participants emphasize that continuous training and skill development are essential for maintaining effective cybercrime investigations. Regular practice in teamwork and communication helps sustain efficiency despite resource limitations, and ongoing training is viewed as a vital factor in enhancing investigative capabilities.

2. Adapting and upgrading technology, including the integration of advanced tools like AI-based forensic solutions, is crucial for improving investigation efficiency. Participants recognize the need for developing new methods and continuously evolving technological approaches to keep pace with sophisticated cyber threats.

3. Advocacy for increased support and resources, including funding for technological upgrades and training, is identified as a strategic priority. Effective resource mobilization and institutional support are seen as necessary to address existing limitations and to strengthen cybercrime investigation efforts.

VI. Enhancing operational effectiveness

1. Participants highlight the importance of strengthening capacity through manpower, funding support, and technological upgrades. There is a clear consensus that increasing specialized personnel focused on cybercrime can improve case response times and overall effectiveness. Participants also emphasize the need for infrastructure and technological enhancements, such as upgrading hardware

with high RAM and fast processors, to support more efficient investigations.

2. Additionally, there is a recurring call for increased government funding and support to sustain long-term improvements in infrastructure, technology, and skilled personnel. Overall, the findings suggest that enhancing operational effectiveness relies heavily on investment in human resources, advanced technology, and infrastructure upgrades, supported by consistent funding strategies.

Conclusion:

Based on the findings of the study, the following conclusions are made:

1. The study showed that the organization is a male dominated agencies, and newly adopting to the challenge of cybercrime investigation. All investigators handle multiple complex cybercrime cases and tried their best to attend to all irrespective of the overloading cases.
2. The Cavite PNP faces a multifaceted set of challenges that significantly hinder their capability to effectively investigate cybercrimes. These include infrastructural deficiencies, personnel shortages, limited financial resources, and the rapidly evolving landscape of cyber threats. Addressing these interconnected issues requires comprehensive investments in modern technology, improved infrastructure, specialized training, and increased funding to enhance investigative capacity and ensure the integrity and efficiency of cybercrime investigations. Without these strategic improvements, the law enforcement effort to combat cybercrime will remain constrained, leaving gaps in national cybersecurity defenses.
3. Current training programs in cybercrime have very limited foundational knowledge and less on practical simulations, necessary training to augment the knowledge of investigators is not available thus this limits the effectiveness of the delivery of service.
4. There is a clear and pressing need for the development of ongoing and specialized training programs in digital forensics to keep pace with the rapidly evolving cyber threat landscape. Expanding training to include advanced techniques such as malware analysis, network security, and the use of cutting-edge forensic tools will significantly enhance the investigative capabilities of law enforcement officers. Implementing these specialized training initiatives is crucial for improving cyber incident response, strengthening digital defenses, and effectively combating sophisticated cybercrime threats.
5. Effective coping strategies for cybercrime investigation hinge on continuous training, technological advancement, and robust resource support. Regular skill development and teamwork are vital for maintaining investigation efficiency amid resource constraints, while adopting advanced tools such as AI-based solutions enhance investigative capabilities. Additionally, securing increased funding and institutional backing is essential to provide the necessary resources for technological upgrades and ongoing training, thereby strengthening the overall effectiveness of cybercrime investigation efforts.
6. Enhancing operational effectiveness in cybercrime investigations requires strategic investment in human resources, technological infrastructure, and funding support. Increasing specialized personnel and upgrading hardware with high-performance capabilities can significantly improve response times and investigative efficiency. Sustained long-term improvements depend on continuous government funding and support to ensure that infrastructure, technology, and skilled workforce development are adequately maintained and expanded, thereby strengthening the overall capacity to combat cyber threats effectively.

Recommendations

Based on the conclusions of this study, the researcher recommends the following:

1. To address the challenges faced by cybercrime investigators, this study recommends that the organization request an increase in government funding and institutional support for the Cybercrime Unit. Exploring private-public partnerships may also be explored for additional resources to address the needs to acquire modern forensic tools, upgrading outdated equipment, and improving infrastructure such as digital laboratories and secure storage facilities. Investment in high-performance software and hardware will not only enhance the accuracy and speed of digital evidence processing but also improve the overall quality of investigations. It is also recommended that the government establish dedicated cybercrime units equipped with advanced facilities to ensure operational efficiency and timely case resolution.
2. Based on the assessment of current training programs available to the Cybercrime Unit, it is recommended that the Philippine National Police (PNP) augment the knowledge of the investigator by designing a more comprehensive and specialized training framework tailored to the evolving nature of cybercrime focus on hands-on training with a real-case simulations, in-depth technical skill-building, and continuous updates.
3. The unit may consider exploring the coping strategies already being practiced and augment this with a more comprehensive technique to continuously develop themselves and respond to the needs of the changing world. Doing so would not only increase efficiency and preparedness but also promote a learning culture that helps investigators stay effective in the face of fast-changing cyber threats.
4. To improve the overall capacity of the Philippine National Police (PNP) in addressing cybercrime, it is recommended that the government prioritize sustained investments in manpower, funding, and technological resources. The participants strongly emphasized the need for additional specialized personnel and consistent financial support to enhance investigation speed and effectiveness. Hiring or training cybercrime-focused experts and providing sufficient operational budgets will allow units to handle complex digital cases with greater efficiency. This also includes the need for long-term funding strategies that can support evolving infrastructure and operations, rather than short-term or reactive solutions.

References:

1. lastal, A. I., & Shaqfa, A. H. (2023). Enhancing police officers' cybercrime investigation skills using a checklist tool. *Journal of Data Analysis and Information Processing*, *11*(02), 121–143. https://doi.org/10.4236/jdaip.2023.112008
2. Alghamdi, M. I. (2021). Digital Forensics in Cyber Security—Recent Trends, Threats, and opportunities. In *IntechOpen eBooks*. https://doi.org/10.5772/intechopen.94452

3. Amoo, N. O. O., Atadoga, N. A., Abrahams, N. T. O., Farayola, N. O. A., Osasona, N. F., & Ayinla, N. B. S. (2024). The legal landscape of cybercrime: A review of contemporary issues in the criminal justice system. *World Journal of Advanced Research and Reviews*, *21*(2), 205–217.https://doi.org/10.30574/wjarr.2024.21.2.0438
4. Annadurai, C., Nelson, I., Devi, K., Manikandan, R., Jhanjhi, N., Masud, M., & Sheikh, A. (2022). Biometric Authentication-Based Intrusion Detection using Artificial intelligence internet of things in smart city. *Energies*, *15*(19), 7430. https://doi.org/10.3390/en15197430
5. Argosino, F. (2024, July 1). Cybercrimes went up by 21% in the 1st quarter, says PNP. INQUIRER.net.
6. Arifi, D., & Arifi, B. (2020). Cybercrime: a challenge to law enforcement. *SEEU Review*, *15*(2), 42–55. https://doi.org/10.2478/seeur-2020-0016
7. Ashiq, M., Rehman, S. U., & Mujtaba, G. (2020). Future challenges and emerging role of academic libraries in Pakistan: A phenomenology approach. Information Development, 37(1), 158–173. https://doi.org/10.1177/0266666919897410
8. Azam, H., Dulloo, M. I., Majeed, M. H., Wan, J. P. H., Xin, L. T., & Sindiramutty, S. R. (2023). Cybercrime Unmasked: Investigating cases and digital evidence. *International Journal of Emerging Multidisciplinaries Computer Science & Artificial Intelligence2*(1). https://doi.org/10.54938/ijemdcsai.2023.02.1.255
9. Blancaflor, E., Arpilleda, J. A., Garcia, A. U., Monasterial, J. A., & Sulit, R. R. (2023). A literature review on the various trends of digital forensics usage in combating cybercrimes. A Literature Review on the Various Trends of Digital Forensics Usage in Combating Cybercrimes, 2019, 132–138. https://doi.org/10.1145/3592307.3592328
10. Bossler, A. M., & Berenblum, T. (2019). Introduction: new directions in cybercrime research. *Journal of Crime and Justice*, *42*(5), 495–499. https://doi.org/10.1080/0735648x.2019.1692426
11. Caliwan, C. L. C. (2024, February). PNP eyes cybersecurity desks to boost fight vs. online crimes. Philippine News Agency. https://www.pna.gov.ph/articles/1218444
12. Chigada, J., & Madzinga, R. (2021). Cyberattacks and threats during COVID-19: A systematic literature review. *South African Journal of Information Management*, *23*(1). https://doi.org/10.4102/sajim.v23i1.1277
13. Curtis, J., & Oxburgh, G. (2022). Understanding cybercrime in 'real world' policing and law enforcement. *The Police Journal Theory Practice and Principles*, *96*(4), 573–592. https://doi.org/10.1177/0032258x221107584

14. De Paoli, S., Johnstone, J., Coull, N., Ferguson, I., Sinclair, G., Tomkins, P., Brown, M., & Martin, R. (2020). A Qualitative Exploratory Study of the Knowledge, Forensic, and Legal Challenges from the Perspective of Police Cybercrime Specialists. *Policing a Journal of Policy and Practice*, *15*(2), 1429–1445. https://doi.org/10.1093/police/paaa027

15. Espiritu, P. G. G., & Jocson, J. C. (2023, November 11). *Navigating cybersecurity challenges in the era of Digital Transformation: Threats and mitigation strategies in the Philippines*. https://journal.ijprse.com/index.php/ijprse/article/view/994

16. Fajardo, M. B., Abragon, M. N., Abuan, L. L., Hinlayagan, J. M., Marmol, D. J., Contreras, A. B., Basbas, R., Jr, & Villa, E. B. (2025). Challenges faced by PNP in resolving cybercrime cases.*ijmaberjournal.org*. https://doi.org/10.11594/ijmaber.06.03.23

17. Horan, C., & Saiedian, H. (2021). Cyber Crime Investigation: landscape, challenges, and future research directions. *Journal of Cybersecurity and Privacy*, *1*(4), 580–596. https://doi.org/10.3390/jcp1040029

18. https://newsinfo.inquirer.net/1956595/cybercrimes-up-by-21in-1st-quarter-says-pnp

19. Jerry. (2024, June 30). *Top 10 cyber security threats in the Philippines*. Olern AI for Business. https://www.olern.com/top-10-cyber-security-threats-in-the-philippines/

20. Johnson, D., Faulkner, E., Meredith, G., & Wilson, T. J. (2020). Police Functional Adaptation to the Digital or Post Digital Age: Discussions with Cybercrime Experts. *The Journal of Criminal Law*, *84*(5), 427–450. https://doi.org/10.1177/0022018320952559

21. JOVILAND RITA,GMA Integrated News & JOVILAND RITA, GMA Integrated News. (2024, February 29). PH gov't acquiring tools vs financial cybercrimes —CICC. GMA News Online. https://www.gmanetwork.com/news/topstories/nation/899034/ph-gov-t-acquiring-tools-vs-financial-cybercrimes-cicc/story/

22. Li, J. (2021, May). View of Cybercrime in the Philippines: A case study of National security. https://www.turcomat.org/index.php/turkbilmat/article/view/6550/5407

23. Li, Y., & Liu, Q. (2021). A comprehensive review study of cyber-attacks and cyber security; Emerging trends and recent developments. *Energy Reports*, *7*, 8176–8186. https://doi.org/10.1016/j.egyr.2021.08.126

24. McKoy, C. (2021). Law enforcement officers' reaction on traditional crimes to fight cybercrime locally. ABC Journal of Advanced Research, 10(2), 159–174. https://doi.org/10.18034/abcjar.v10i2.601

25. Mishra, A., Alzoubi, Y. I., Anwar, M. J., & Gill, A. Q. (2022). Attributes impacting cybersecurity policy development: An evidence from seven nations. *Computers & Security*, *120*, 102820. https://doi.org/10.1016/j.cose.2022.102820

26. Mpa, P. J. C. L. A., & Diaz, R. (2019). INVESTIGATION AND DETECTIVE COMPETENCIES OF THE PHILIPPINE NATIONAL POLICE IN THE PROVINCE OF BATAAN:. . . *ResearchGate*. https://www.researchgate.net/publication/333784234_INVESTIGATION_AND_DETECTIVE_COMPETENCIES_OF_THE_PHILIPPINE_NATIONAL_POLICE_IN_THE_PROVINCE_OF_BATAAN_BASIS_FOR_PROFESSIONAL_DEVELOPMENT_PLAN

27. Nelufule, N., Masango, M., & Singano, T. (2024). The Future of Digital Forensic Investigations: Keeping Pace with Technological Advancements. 1843–1848. https://doi.org/10.1109/mipro60963.2024.10569461

28. Nishnianidze, A. (2023). Some new challenges of cybercrime and the reason for its outdated regulations. *European Scientific Journal ESJ*, *19*(39), 92. https://doi.org/10.19044/esj.2023.v19n39p92

29. Nouh, M., Nurse, J. R. C., Webb, H., & Goldsmith, M. (2019). Cybercrime Investigators are Users Too! Understanding the Socio−Technical Challenges Faced by Law Enforcement. *(Cornell University)*. https://arxiv.org/abs/1902.06961

30. O, N. B. D. G. G., Jr. (2024). CHALLENGES ENCOUNTERED BY THE POLICE OFFICERS IN CRIME PREVENTION IN TABUK CITY, KALINGA. *EPRA International Journal of Multidisciplinary Research (IJMR)*, 49–63. https://doi.org/10.36713/epra16729

31. Paek, S., Nalla, M. K., Chun, Y., & Lee, J. (2021). The Perceived Importance of Cybercrime Control among Police Officers: Implications for Combatting Industrial Espionage. *Sustainability*, *13*(8), 4351. https://doi.org/10.3390/su13084351

32. Pasinhon, L. G., & Donato, L. M. (2024). Capability of the Regional Anti-Cybercrime Unit-Cordillera (Racu-CoR) in handling cybercrime cases. *APJAET - Journal Ay Asia Pacific Journal of Advanced Education and Technology*, *2*(3). https://doi.org/10.54476/apjaet/06740

33. Prakash, V., Williams, A., Garg, L., Savaglio, C., & Bawa, S. (2021). Cloud and Edge Computing-Based Computer Forensics: Challenges and Open Problems. *Electronics*, *10*(11), 1229. https://doi.org/10.3390/electronics10111229

34. Rakha, N. A. (2024). Cybercrime and the Law: Addressing the challenges of digital forensics in criminal investigations. *Mexican Law Review*, 23–54. https://doi.org/10.22201/iij.24485306e.2024.2.18892

35. RecordedFuture, & Borges, E. (2024, February). What is a Cyber

Crime Investigation? Essentials of Cyber Crime Investigation. https://www.recordedfuture.com/threat-intelligence-101/incident-response-management/cyber-crime-investigation

36. Sarkar, G., & Shukla, S. K. (2024). Reconceptualizing Online Offenses: A framework for distinguishing cybercrime, cyberattacks, and cyberterrorism in the Indian legal context. *Journal of Economic Criminology*, 100063. https://doi.org/10.1016/j.jeconc.2024.100063

37. Siddiqua, D. (2024). Challenges Faced by Police Officers in Investigating Cyber Crime: An Exploratory Study in Bangladesh. *International Journal of Humanities Social Sciences and Education*, *11*(7), 150–161. https://doi.org/10.20431/2349-0381.1107014

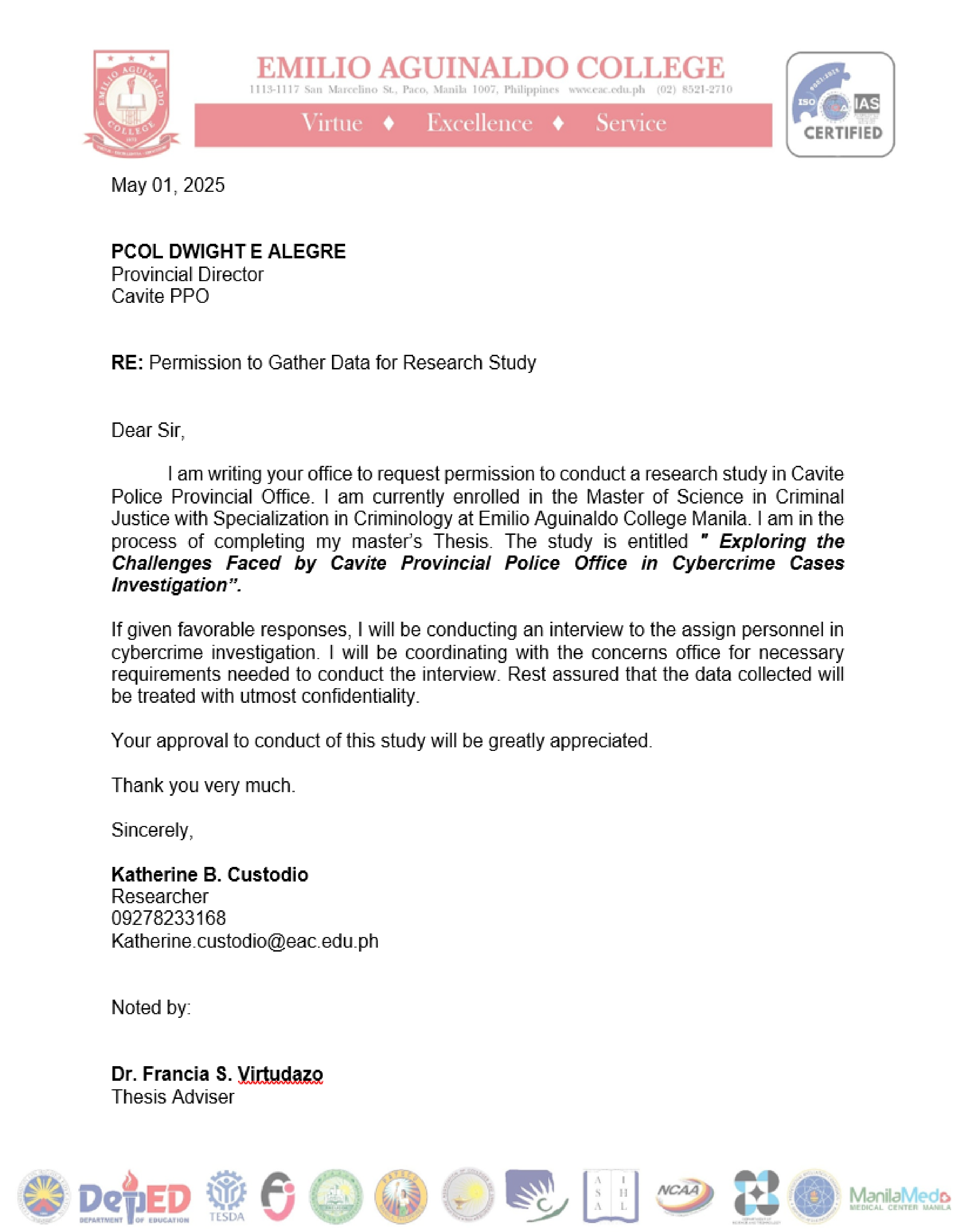
38. Tithi, S. T., Aziz, N. M. B., & Shadhukha, N. K. R. (2024). Police officers experience facing challenges in combating crime in urban and rural areas: A study on District Police Faridpur. International Journal of Scientific Research and Management (IJSRM), 12(03), 1742–1747. https://doi.org/10.18535/ijsrm/v12i03.sh04

39. Viraja, V. K., & Purandare, P. (2021). A qualitative research on the impact and challenges of cybercrimes. *Journal of Physics Conference Series*, *1964*(4), 042004. https://doi.org/10.1088/1742-6596/1964/4/042004

40. Vitus, E. N. (2023). Cybercrime and Online Safety: Addressing the challenges and solutions related to cybercrime, online fraud, and ensuring a safe digital environment for all users— A Case of African States. *Zenodo (CERN European Organization for Nuclear Research)*. https://doi.org/10.6084/m9.figshare.24155610.v1

APPENDIX A

LETTER ASKING FOR PERMISSION



EMILIO AGUINALDO COLLEGE

1113-1117 San Marcelino St., Paco, Manila 1007, Philippines www.eac.edu.ph (02) 8521-2710

Virtue ♦ Excellence ♦ Service

May 01, 2025

PCOL DWIGHT E ALEGRE
Provincial Director
Cavite PPO

RE: Permission to Gather Data for Research Study

Dear Sir,

I am writing your office to request permission to conduct a research study in Cavite Police Provincial Office. I am currently enrolled in the Master of Science in Criminal Justice with Specialization in Criminology at Emilio Aguinaldo College Manila. I am in the process of completing my master's Thesis. The study is entitled ***" Exploring the Challenges Faced by Cavite Provincial Police Office in Cybercrime Cases Investigation".***

If given favorable responses, I will be conducting an interview to the assign personnel in cybercrime investigation. I will be coordinating with the concerns office for necessary requirements needed to conduct the interview. Rest assured that the data collected will be treated with utmost confidentiality.

Your approval to conduct of this study will be greatly appreciated.

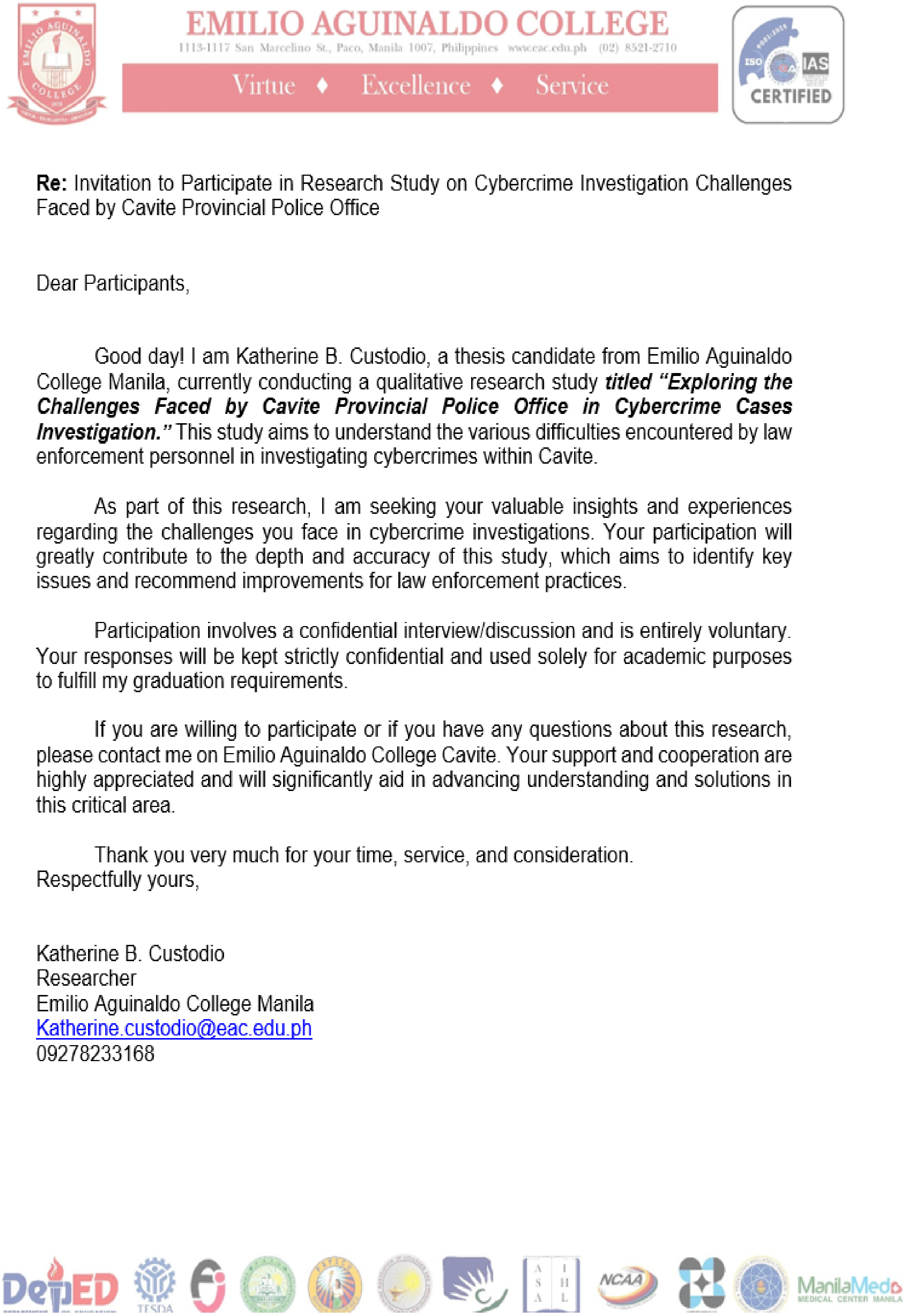
Thank you very much.

Sincerely,

Katherine B. Custodio
Researcher
09278233168
Katherine.custodio@eac.edu.ph

Noted by:

Dr. Francia S. Virtudazo
Thesis Adviser



EMILIO AGUINALDO COLLEGE
1113-1117 San Marcelino St., Paco, Manila 1007, Philippines www.eac.edu.ph (02) 8521-2710
Virtue ♦ Excellence ♦ Service

Re: Invitation to Participate in Research Study on Cybercrime Investigation Challenges Faced by Cavite Provincial Police Office

Dear Participants,

Good day! I am Katherine B. Custodio, a thesis candidate from Emilio Aguinaldo College Manila, currently conducting a qualitative research study ***titled "Exploring the Challenges Faced by Cavite Provincial Police Office in Cybercrime Cases Investigation."*** This study aims to understand the various difficulties encountered by law enforcement personnel in investigating cybercrimes within Cavite.

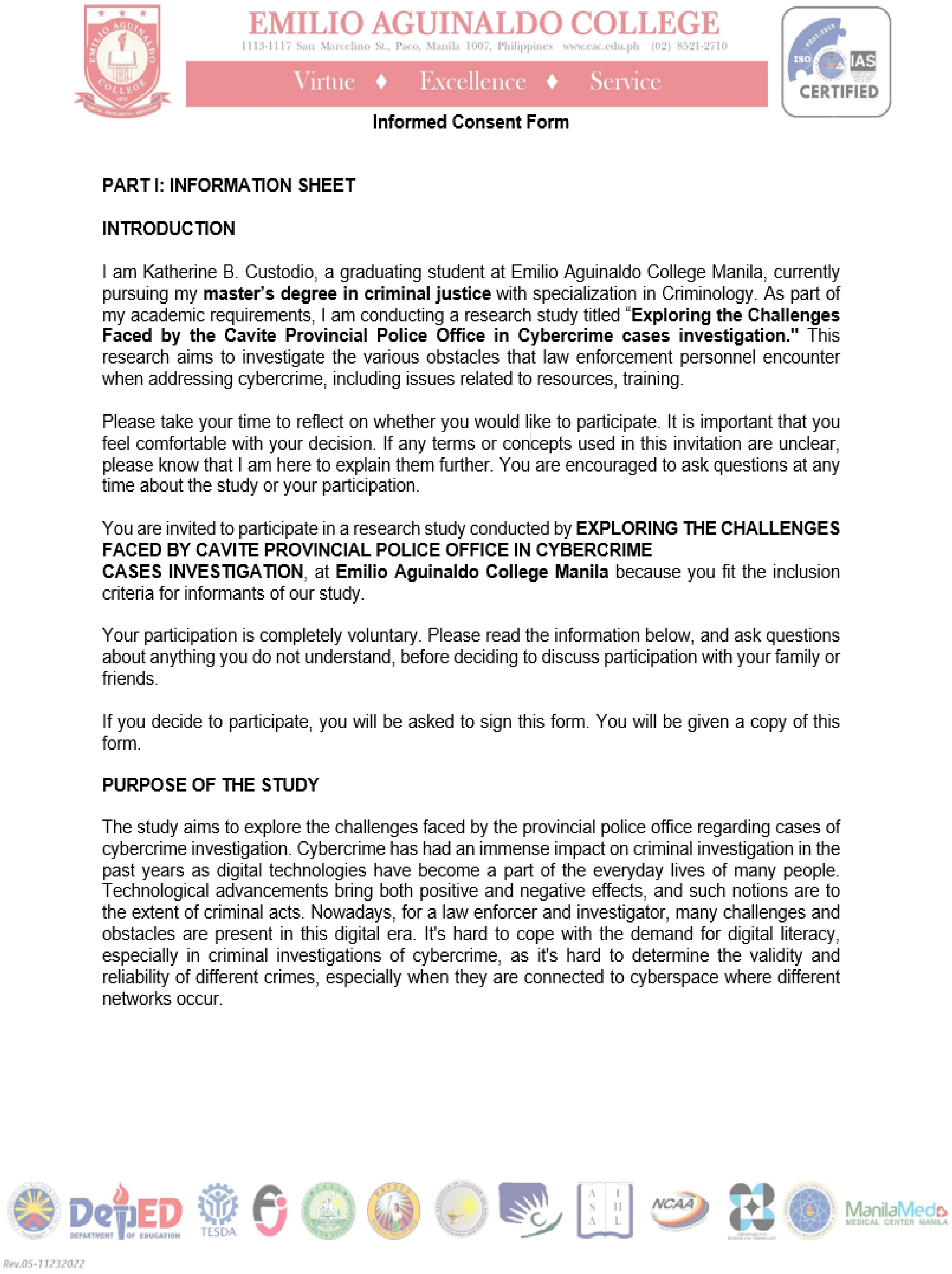
As part of this research, I am seeking your valuable insights and experiences regarding the challenges you face in cybercrime investigations. Your participation will greatly contribute to the depth and accuracy of this study, which aims to identify key issues and recommend improvements for law enforcement practices.

Participation involves a confidential interview/discussion and is entirely voluntary. Your responses will be kept strictly confidential and used solely for academic purposes to fulfill my graduation requirements.

If you are willing to participate or if you have any questions about this research, please contact me on Emilio Aguinaldo College Cavite. Your support and cooperation are highly appreciated and will significantly aid in advancing understanding and solutions in this critical area.

Thank you very much for your time, service, and consideration.
Respectfully yours,

Katherine B. Custodio
Researcher
Emilio Aguinaldo College Manila
Katherine.custodio@eac.edu.ph
09278233168



EMILIO AGUINALDO COLLEGE

1113-1117 San Marcelino St., Paco, Manila 1007, Philippines www.eac.edu.ph (02) 8521-2710

Virtue ♦ Excellence ♦ Service

Informed Consent Form

PART I: INFORMATION SHEET

INTRODUCTION

I am Katherine B. Custodio, a graduating student at Emilio Aguinaldo College Manila, currently pursuing my **master's degree in criminal justice** with specialization in Criminology. As part of my academic requirements, I am conducting a research study titled "**Exploring the Challenges Faced by the Cavite Provincial Police Office in Cybercrime cases investigation."** This research aims to investigate the various obstacles that law enforcement personnel encounter when addressing cybercrime, including issues related to resources, training.

Please take your time to reflect on whether you would like to participate. It is important that you feel comfortable with your decision. If any terms or concepts used in this invitation are unclear, please know that I am here to explain them further. You are encouraged to ask questions at any time about the study or your participation.

You are invited to participate in a research study conducted by **EXPLORING THE CHALLENGES FACED BY CAVITE PROVINCIAL POLICE OFFICE IN CYBERCRIME CASES INVESTIGATION**, at **Emilio Aguinaldo College Manila** because you fit the inclusion criteria for informants of our study.

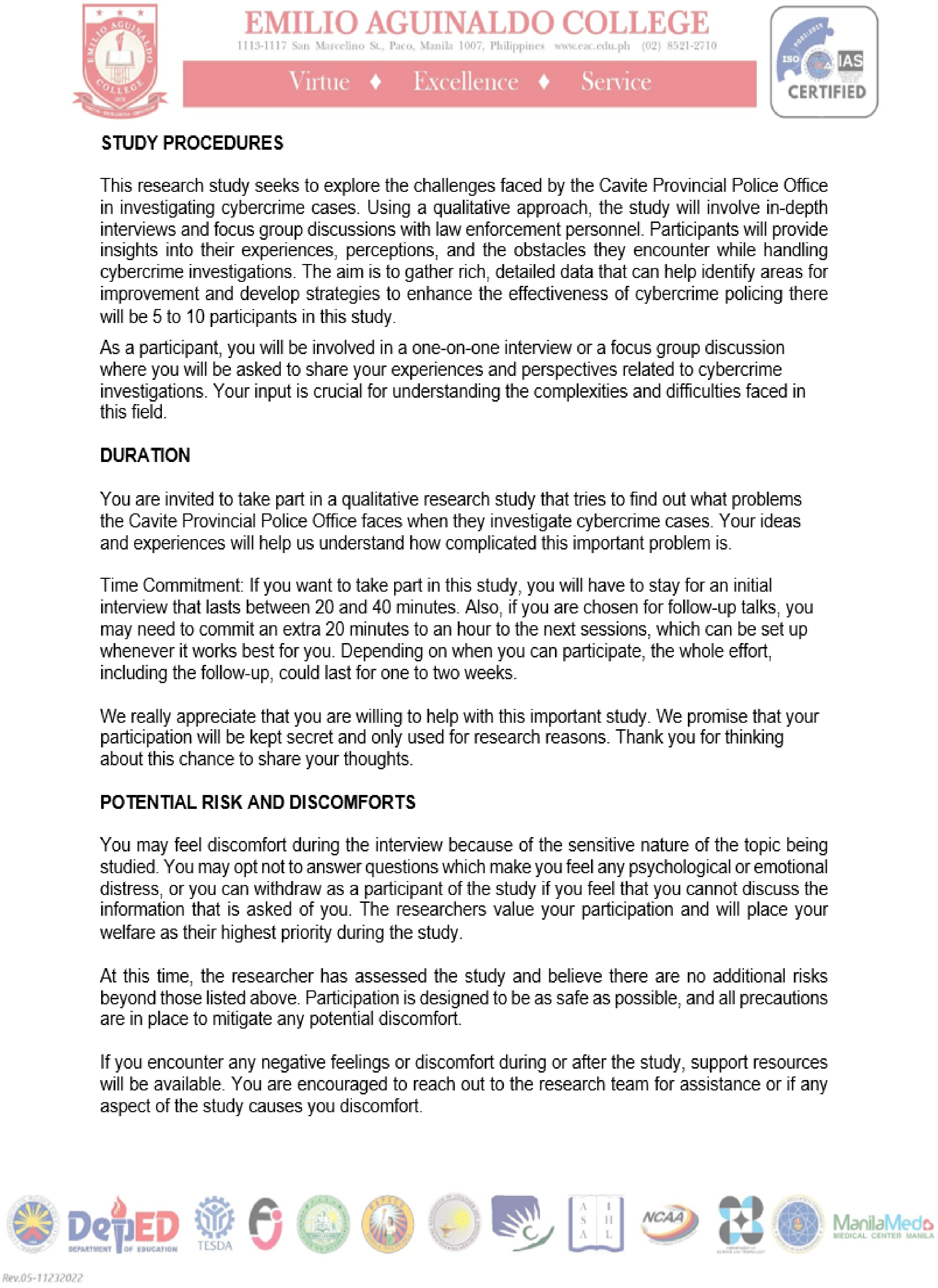
Your participation is completely voluntary. Please read the information below, and ask questions about anything you do not understand, before deciding to discuss participation with your family or friends.

If you decide to participate, you will be asked to sign this form. You will be given a copy of this form.

PURPOSE OF THE STUDY

The study aims to explore the challenges faced by the provincial police office regarding cases of cybercrime investigation. Cybercrime has had an immense impact on criminal investigation in the past years as digital technologies have become a part of the everyday lives of many people. Technological advancements bring both positive and negative effects, and such notions are to the extent of criminal acts. Nowadays, for a law enforcer and investigator, many challenges and obstacles are present in this digital era. It's hard to cope with the demand for digital literacy, especially in criminal investigations of cybercrime, as it's hard to determine the validity and reliability of different crimes, especially when they are connected to cyberspace where different networks occur.

Rev.05-11232022



EMILIO AGUINALDO COLLEGE

1113-1117 San Marcelino St., Paco, Manila 1007, Philippines www.eac.edu.ph (02) 8521-2710

Virtue ♦ Excellence ♦ Service

STUDY PROCEDURES

This research study seeks to explore the challenges faced by the Cavite Provincial Police Office in investigating cybercrime cases. Using a qualitative approach, the study will involve in-depth interviews and focus group discussions with law enforcement personnel. Participants will provide insights into their experiences, perceptions, and the obstacles they encounter while handling cybercrime investigations. The aim is to gather rich, detailed data that can help identify areas for improvement and develop strategies to enhance the effectiveness of cybercrime policing there will be 5 to 10 participants in this study.

As a participant, you will be involved in a one-on-one interview or a focus group discussion where you will be asked to share your experiences and perspectives related to cybercrime investigations. Your input is crucial for understanding the complexities and difficulties faced in this field.

DURATION

You are invited to take part in a qualitative research study that tries to find out what problems the Cavite Provincial Police Office faces when they investigate cybercrime cases. Your ideas and experiences will help us understand how complicated this important problem is.

Time Commitment: If you want to take part in this study, you will have to stay for an initial interview that lasts between 20 and 40 minutes. Also, if you are chosen for follow-up talks, you may need to commit an extra 20 minutes to an hour to the next sessions, which can be set up whenever it works best for you. Depending on when you can participate, the whole effort, including the follow-up, could last for one to two weeks.

We really appreciate that you are willing to help with this important study. We promise that your participation will be kept secret and only used for research reasons. Thank you for thinking about this chance to share your thoughts.

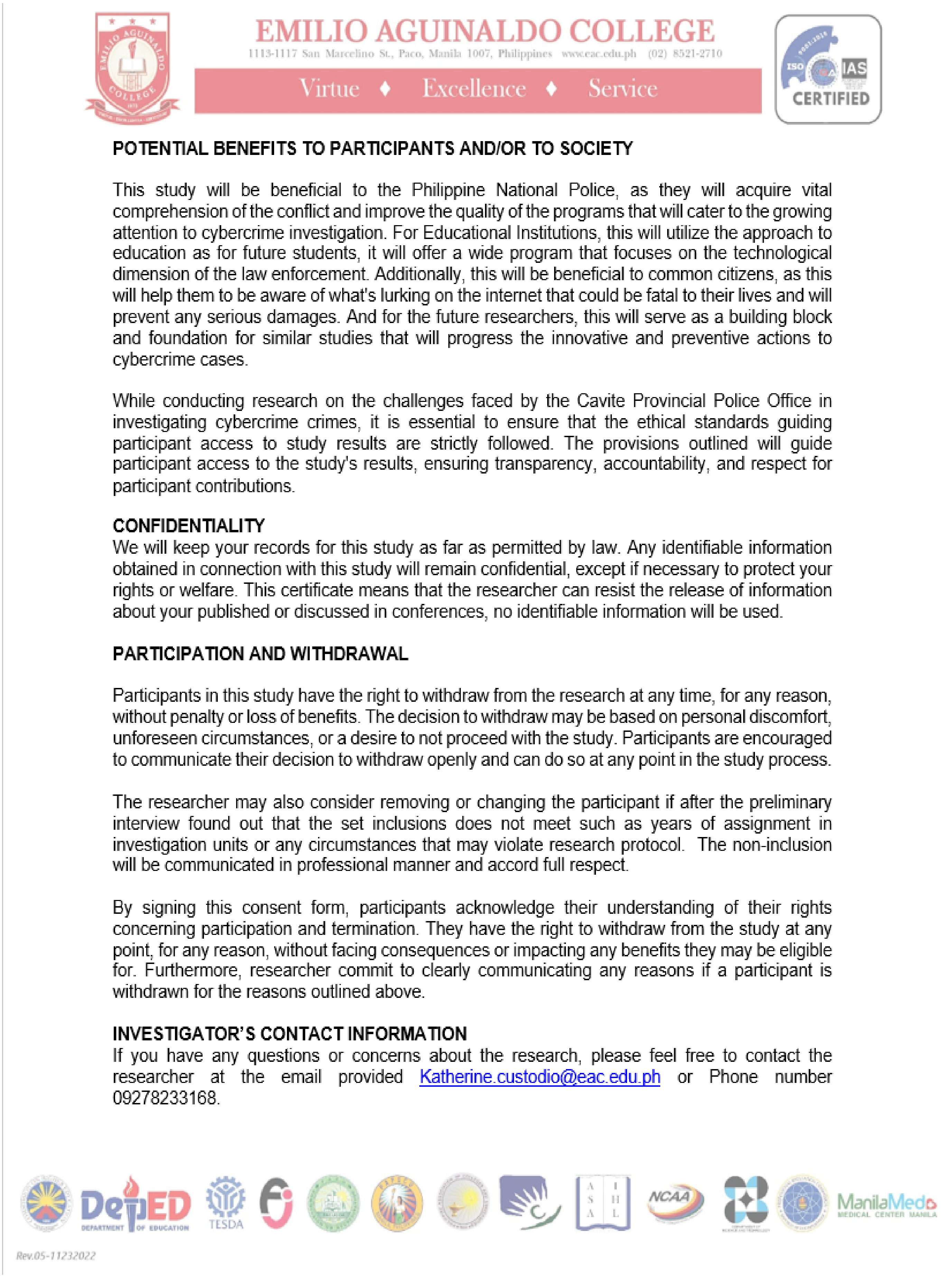
POTENTIAL RISK AND DISCOMFORTS

You may feel discomfort during the interview because of the sensitive nature of the topic being studied. You may opt not to answer questions which make you feel any psychological or emotional distress, or you can withdraw as a participant of the study if you feel that you cannot discuss the information that is asked of you. The researchers value your participation and will place your welfare as their highest priority during the study.

At this time, the researcher has assessed the study and believe there are no additional risks beyond those listed above. Participation is designed to be as safe as possible, and all precautions are in place to mitigate any potential discomfort.

If you encounter any negative feelings or discomfort during or after the study, support resources will be available. You are encouraged to reach out to the research team for assistance or if any aspect of the study causes you discomfort.

Rev.05-11232022



EMILIO AGUINALDO COLLEGE

1113-1117 San Marcelino St., Paco, Manila 1007, Philippines www.eac.edu.ph (02) 8521-2710

Virtue ♦ Excellence ♦ Service

ISO IAS CERTIFIED

POTENTIAL BENEFITS TO PARTICIPANTS AND/OR TO SOCIETY

This study will be beneficial to the Philippine National Police, as they will acquire vital comprehension of the conflict and improve the quality of the programs that will cater to the growing attention to cybercrime investigation. For Educational Institutions, this will utilize the approach to education as for future students, it will offer a wide program that focuses on the technological dimension of the law enforcement. Additionally, this will be beneficial to common citizens, as this will help them to be aware of what's lurking on the internet that could be fatal to their lives and will prevent any serious damages. And for the future researchers, this will serve as a building block and foundation for similar studies that will progress the innovative and preventive actions to cybercrime cases.

While conducting research on the challenges faced by the Cavite Provincial Police Office in investigating cybercrime crimes, it is essential to ensure that the ethical standards guiding participant access to study results are strictly followed. The provisions outlined will guide participant access to the study's results, ensuring transparency, accountability, and respect for participant contributions.

CONFIDENTIALITY

We will keep your records for this study as far as permitted by law. Any identifiable information obtained in connection with this study will remain confidential, except if necessary to protect your rights or welfare. This certificate means that the researcher can resist the release of information about your published or discussed in conferences, no identifiable information will be used.

PARTICIPATION AND WITHDRAWAL

Participants in this study have the right to withdraw from the research at any time, for any reason, without penalty or loss of benefits. The decision to withdraw may be based on personal discomfort, unforeseen circumstances, or a desire to not proceed with the study. Participants are encouraged to communicate their decision to withdraw openly and can do so at any point in the study process.

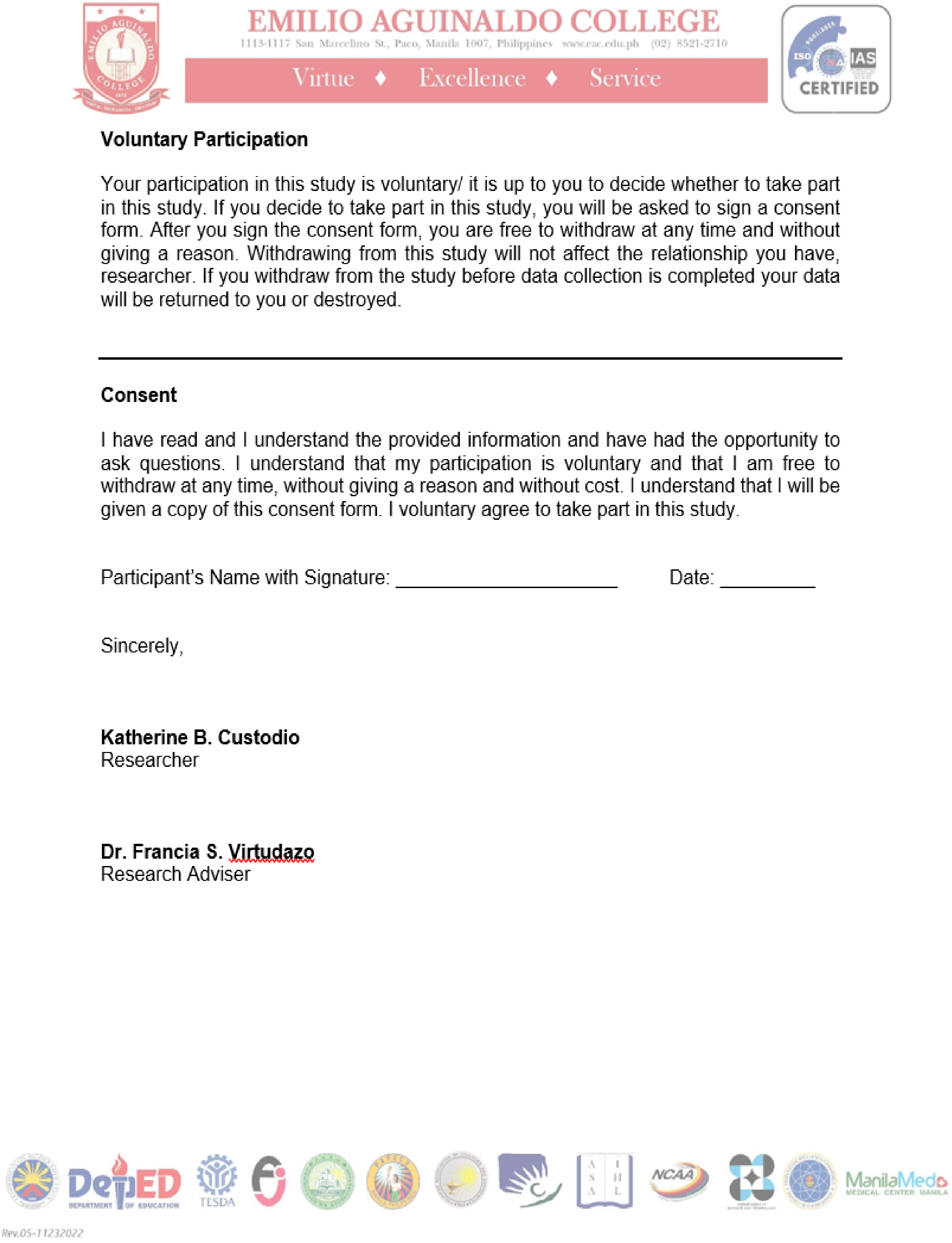
The researcher may also consider removing or changing the participant if after the preliminary interview found out that the set inclusions does not meet such as years of assignment in investigation units or any circumstances that may violate research protocol. The non-inclusion will be communicated in professional manner and accord full respect.

By signing this consent form, participants acknowledge their understanding of their rights concerning participation and termination. They have the right to withdraw from the study at any point, for any reason, without facing consequences or impacting any benefits they may be eligible for. Furthermore, researcher commit to clearly communicating any reasons if a participant is withdrawn for the reasons outlined above.

INVESTIGATOR'S CONTACT INFORMATION

If you have any questions or concerns about the research, please feel free to contact the researcher at the email provided Katherine.custodio@eac.edu.ph or Phone number 09278233168.

Rev.05-11232022



EMILIO AGUINALDO COLLEGE

1113-1117 San Marcelino St., Paco, Manila 1007, Philippines www.eac.edu.ph (02) 8521-2710

Virtue ♦ Excellence ♦ Service

IAS CERTIFIED

Voluntary Participation

Your participation in this study is voluntary/ it is up to you to decide whether to take part in this study. If you decide to take part in this study, you will be asked to sign a consent form. After you sign the consent form, you are free to withdraw at any time and without giving a reason. Withdrawing from this study will not affect the relationship you have, researcher. If you withdraw from the study before data collection is completed your data will be returned to you or destroyed.

Consent

I have read and I understand the provided information and have had the opportunity to ask questions. I understand that my participation is voluntary and that I am free to withdraw at any time, without giving a reason and without cost. I understand that I will be given a copy of this consent form. I voluntary agree to take part in this study.

Participant's Name with Signature: ______________________ Date: _________

Sincerely,

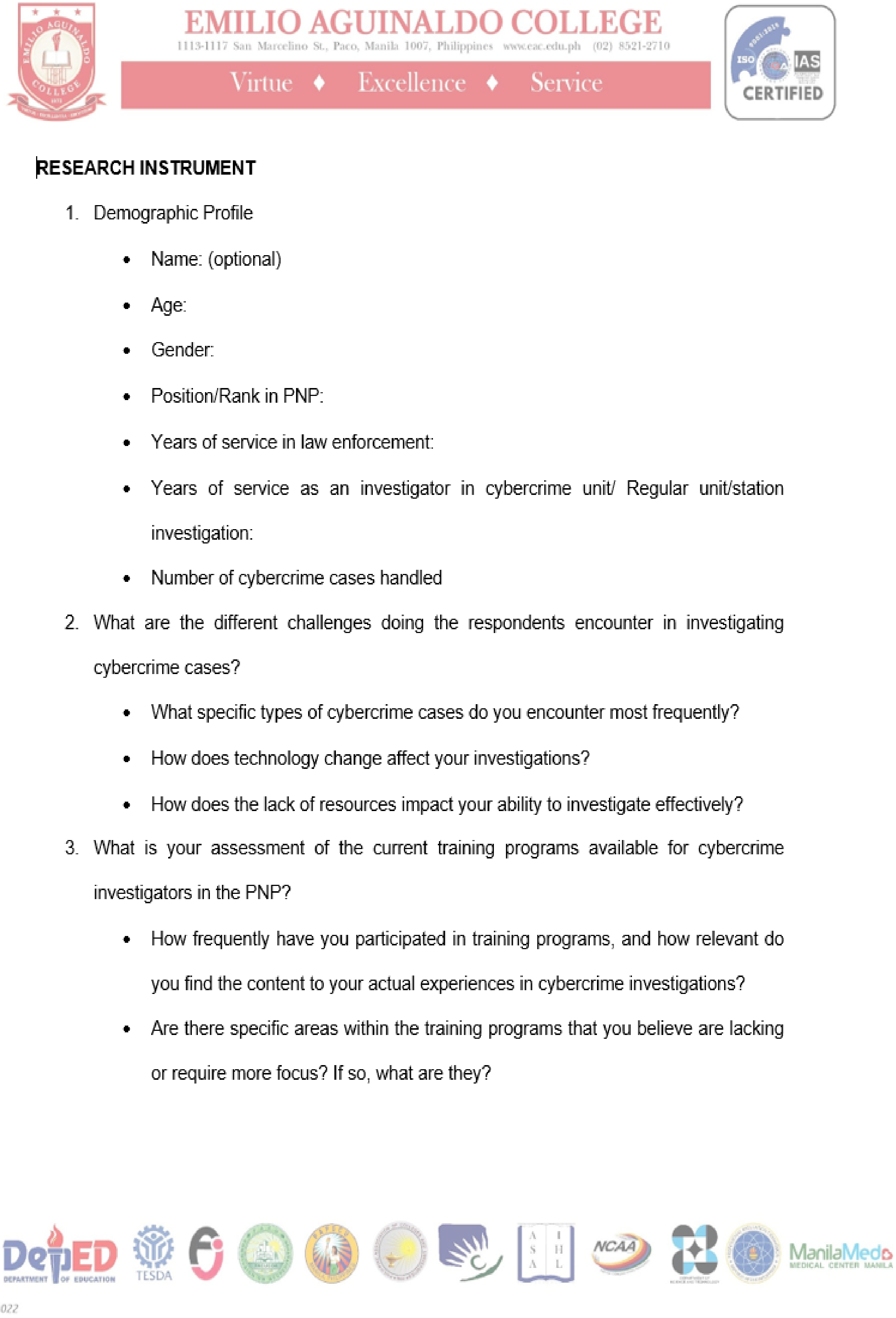
Katherine B. Custodio
Researcher

Dr. Francia S. Virtudazo
Research Adviser

DepED DEPARTMENT OF EDUCATION TESDA NCAA ManilaMed MEDICAL CENTER MANILA

Rev.05-11232022

APPENDIX C
RESEARCH INSTRUMENT

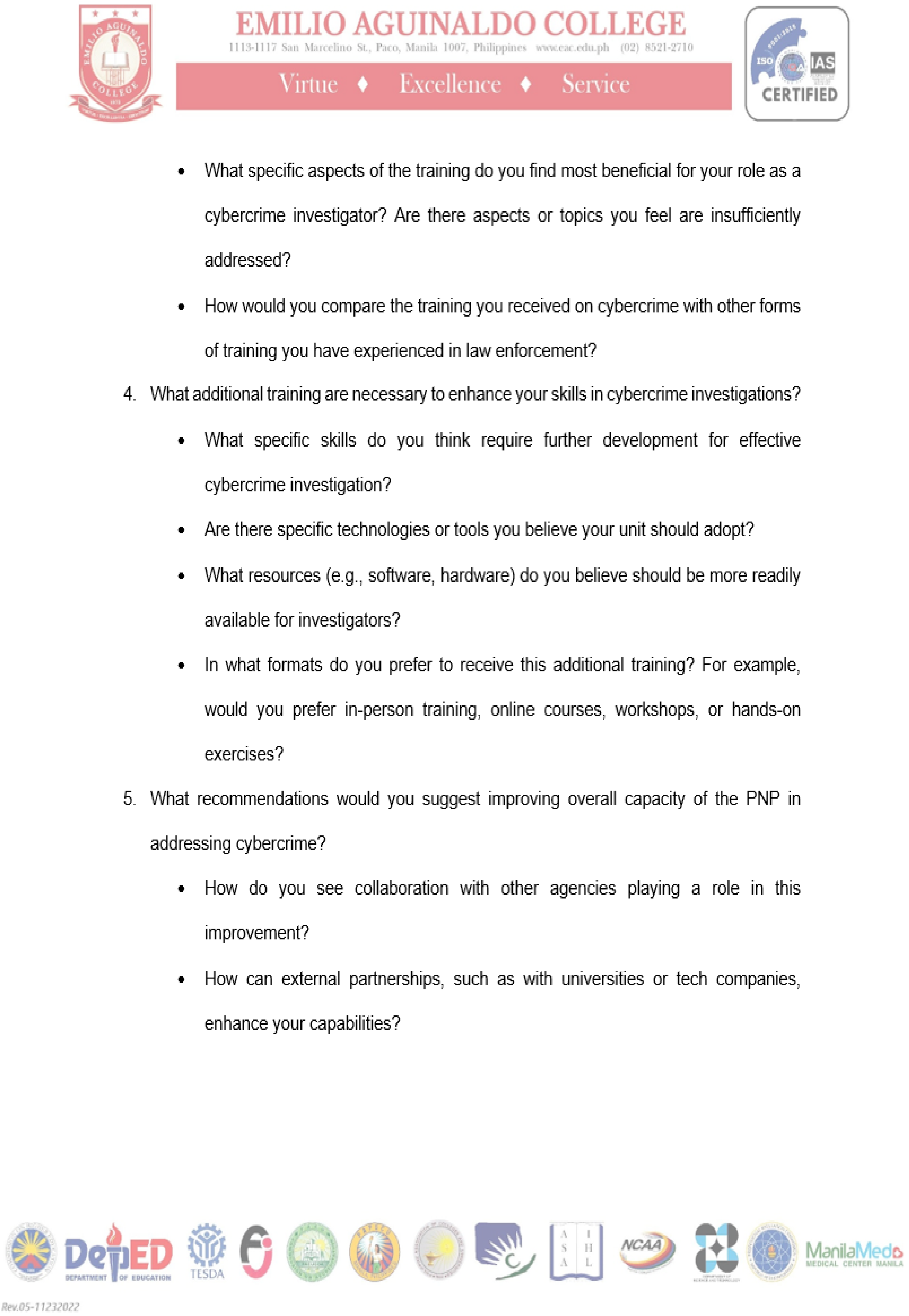


EMILIO AGUINALDO COLLEGE
1113-1117 San Marcelino St., Paco, Manila 1007, Philippines www.eac.edu.ph (02) 8521-2710
Virtue ♦ Excellence ♦ Service

RESEARCH INSTRUMENT

1. Demographic Profile
   - Name: (optional)
   - Age:
   - Gender:
   - Position/Rank in PNP:
   - Years of service in law enforcement:
   - Years of service as an investigator in cybercrime unit/ Regular unit/station investigation:
   - Number of cybercrime cases handled
2. What are the different challenges doing the respondents encounter in investigating cybercrime cases?
   - What specific types of cybercrime cases do you encounter most frequently?
   - How does technology change affect your investigations?
   - How does the lack of resources impact your ability to investigate effectively?
3. What is your assessment of the current training programs available for cybercrime investigators in the PNP?
   - How frequently have you participated in training programs, and how relevant do you find the content to your actual experiences in cybercrime investigations?
   - Are there specific areas within the training programs that you believe are lacking or require more focus? If so, what are they?

Rev.05-11232022



EMILIO AGUINALDO COLLEGE

1113-1117 San Marcelino St., Paco, Manila 1007, Philippines www.eac.edu.ph (02) 8521-2710

Virtue ♦ Excellence ♦ Service

- What specific aspects of the training do you find most beneficial for your role as a cybercrime investigator? Are there aspects or topics you feel are insufficiently addressed?
- How would you compare the training you received on cybercrime with other forms of training you have experienced in law enforcement?

4. What additional training are necessary to enhance your skills in cybercrime investigations?
   - What specific skills do you think require further development for effective cybercrime investigation?
   - Are there specific technologies or tools you believe your unit should adopt?
   - What resources (e.g., software, hardware) do you believe should be more readily available for investigators?
   - In what formats do you prefer to receive this additional training? For example, would you prefer in-person training, online courses, workshops, or hands-on exercises?
5. What recommendations would you suggest improving overall capacity of the PNP in addressing cybercrime?
   - How do you see collaboration with other agencies playing a role in this improvement?
   - How can external partnerships, such as with universities or tech companies, enhance your capabilities?

Rev.05-11232022

APPENDIX D

Line		In Vivo Statements
	Researcher	Good morning po.
		Thank you for taking the time to speak with me
		Today sir.
		My name is Katherine Custodio
		As discussed, this interview is about the
		Challenges faced cybercrime cases
		Investigation your insights will be
		Invaluable for my study.
		With your permission I would like to record our
.		Our conversation that I capture your insight
.		Accurately ensure confidentiality.
.		Is that okay with you sir?
.	Participant 1	Yes, ma'am.
.		Good morning po.
.	Researcher	How many numbers of cybercrime cases do
.		You handle Per week po?
.	Participant 1	Around 30 different cybercrimes.
.	Researcher	Sir, what are the different cybercrime cases
.		that you have handled?
.	Participant 1	Online fraud and scam po romances scam
.		And R. A10175
.	Researcher	Among the different types of cybercrime
.		What is the highest?
.	Participant 1	Online scam ma'am
.	Researcher	Online scams ano po yung sa facebook po?
.	Participant 1	Ma'am yung mga naloloko sa marketplace
.		Then nabubudol na fake pagkapadala ng pera
.		Iblock sila mga ganun ma'am.
.		pag bumibili sila ng item.
.	Researcher	Paano po yun mga ginagawa nyo dun ano
.		nangyayare?
.	Participant 1	Ah pag po ganyan kami cases ang advise
.		Namin Is ireport muna kung saan financially
.		Bumagsak yung pera.
.		Halimbawa ma'am nagpadala sya sa gcash
.		Para ma aware siya mag conduct
.		Si gcash ng initially investigation.
.	Researcher	May timeline po ba yun?
.	Participant 1	Wala naman ma'am.
.		Actually, si gcash kasi pag nag imbestigate
.		Siya at kaylangan police report minsan
.		nagbibigay sila Ng 3 days dapat makapag

.		Report sila sa police.
.		Pag meron naman insurances na cover
.		Yung gcash account dapat within 24 hours
.		May police report ka na.
.	Researcher	Ahhh ok po.
.		So normally talaga is scamming
.	Participant 1	Yes ma'am.
.	Researcher	Yung sa mga romance scam po yung online
.		Virtual space Eengayuhin ka tapos s*x
.		Ayun pala vinideo Screen record na or
.		yung buong katawan mo tapos block mail ka na
.		ikakalat keme kapag hindi ka
.		Nakapagbigay ng pera ganun po.
.	Participant 1	Yes, ma'am.
.		Madami kami ganyan mostly mga lalaki po.
.	Researcher	Kaya nga po sir e.
.	Participant 1	May oras din yan e.
.		Nangyayari po jan mostly ma'am
.		Gabi hanggang madaling araw kasi yan yung
.		Time nasa bahay yung mga lalaki
.		Active mostly mga Kabataan mapupusok
.		Tumatawag yan alanganin oras.
.	Researcher	Sino po yung tumatawag yun babae po?
.	Participant 1	Hindi ma'am
.		Profile picture e Maganda akala nila tunay
.		Babae makikipagkaibigan magaaya ng
.		Sexual online di nila alam AI lang pala.
.	Researcher	AI nga po eh.
.	Participant 1	Yes ma'am.
.		yung ginagawa iniscreen record po tapos ayun
.		Gagamitin para pang blackmail sa kanila.
.	Researcher	Pero meron po ba jan somewhere
.		jan sa cavite po?
.	Participant 1	Mostly ma'am everyday ganyan dito ma'am
.		Ang tawag po namin jan vidiakol ganun.
.	Researcher	Lalaki po ba madalas yung victim?
.		Pero po pagka ganun matrace niyo po ba yun?
.	Participant 1	Actually, ma'am sa tracing ayun nga ma'am.
.		Sakop tayo ng data privacy pwede tayo
.		Makitulong sa tracing pag and case ay
.		Involve national security, terrorism
.		Pwede kasi po saklaw ng national
.		Yan pati mga sexual exportation
.		Mostly ma'am minor pwede po

.		Tumulong ma'am pero pag dating sa ibang
.		Cases Hindi na ma'am.
.	Researcher	Ah okay po.
.	Participant 1	Bawal po tayo magtrace at isa pa
.		Wala tayo tools dito.
.	Researcher	Ayun po yung isa sa challenges na wala kayo?
.	Participant 1	Yes ma'am.
.	Researcher	Dito po wala naman po ako nakikita laboratory
.		Na pang digital forensic.
.	Participant 1	Wala po kami digital forensic actually ma'am
.		Ang digital forensic bibihira lang po sa PNP
.		Pero meron naman kami knowledge dun
.		Pero and problema wala naman kami tools.
0.	Researcher	Ang challenges niyo po Talaga is tools?
1.	Participant 1	Yes ma'am.
2.	Researcher	Pag may mga cases po kayo na ganyan
3.		kalangan talaga digital forensic
4.		Saan po sila pupunta?
5.	Participant 1	Pag ganyan ma'am,
6.		nirerefer po namin sa regional headquarters.
7.	Researcher	Ah okay po
8.		Regional Headquarters na po.
9.	Participant 1	Opo sa region meron na po niyan.
0.	Researcher	Kumpleto na po sila dun?
1.	Participant 1	Meron na po gamit kahit papaano.
2.	Researcher	Papano pagka halimbawa crime scene hindi na
3.		Nila nalalaman kung may mga evidence
4.		Nag processing Crime scene may camera
5.		Computer hindi na nila kinoconsider yan.
6.	Participant 1	Depende po yun ma'am.
7.		Kung ano matatagpuan sa crime scene
8.		hindi siya pwede galawin ang gagalaw
9.		lang Talaga Niyan is digital forensic expert.
0.	Researcher	Pero kinukuha niyo po yan?
1.	Participant 1	Yes, ma'am.
2.		After na ma secure at marking ng digital
3.		Forensic natin sila lang po kasi yung allow
4.		Gumawa niya.
5.	Researcher	How many digital forensic do we have?
6.		Halimbawa ang Cavite we have many
7.		Municipalities and provinces kung may cases
8.		Isa lang?
9.	Participant 1	Ayun nga ma'am pinapatawag po siya ma'am
0.	Researcher	Challenges talaga you have to wait

1.		Kulang ng skilled personnel.
2.	Participant 1	Yes, ma'am kasi siya yung may dala tools.
3.	Researcher	Ang Calabarzon gano kalaki yan staka
4.		2nd highest Industrialize or urbanize places
5.		2nd national capital region.
6.	Participant 1	Yes ma'am.
7.	Researcher	Meron ba kayo records or ideal as
8.		How many cybercrimes attended or handle?
9.	Participant 1	Ever sinces nag bukas po kami almost
0.		4 years na ma'am na handled ko po or ranges
1.		30 siguro ma'am kada week po.
2.	Researcher	Sayo palang po yung?
3.	Participant 1	Saakin palang ma'am iba pa yun kanila.
4.		Meron po kami regular filling nagsasampa
5.		din po kasi kami Ng kaso pag ang mga cases
6.		Ay cyber libel adjust vicsation,
7.		Mga estafa yun na cater po namin.
8.	Researcher	In history, dati kasi sinasabi ang pinaka
9.		Marami ay cyber libel ngayn ay scamming na.
0.		Yes ma'am.
1.	Researcher	Ano po undergradate mo po?
2.	Participant 1	Bachelor of Science in criminology ma'am
3.		NCST po.
4.	Researcher	Ayaw mo po mag explore sa digital forensic
5.		Po?
6.	Participant 1	Actually, ma'am
7.		Pag available yung schooling ma'am
8.		Ano po yan e pinipila pila pa e ma'am e.
9.	Researcher	Pero ngayon nakakapag digital forensic
0.		instruction of evidence?
1.	Participant 1	Yes ma'am.
2.		Nag extract naman po kami kukuhanan lang
3.		Naming ng Sample example po nvit code
4.		Irrl link po.
5.	Researcher	Ilang taon na po kayo sa service po?
6.	Participant 1	10 years na po.
7.	Researcher	Sa cybercrime unit po?
8.	Participant 1	4 years na po.
9.	Researcher	So talaga ang crime ngayon papunta na sa
0.		Cybercrime.
1.	Participant 1	Yes ma'am
2.		Rampant po talaga pag dating sa cybercrime
3.	Researcher	Ano yun pinaka hirap na nahandle
4.		niyo sa cybercrime?

5.	Participant 1	Paghahabol ng mga bank account po.
6.	Researcher	Bank account.
7.	Participant 1	Yes ma'am.
8.		kasi kagaya nga po nun scam ako kaylangan
9.		Ko pa kasi apply yung sa court para ma
0.		Disclosed particular account.
1.	Researcher	Sa training po sir ano po yung training na
2.		Na available sa inyo?
3.	Participant 1	Nag training ako ng criminal investigative
4.		Lecture course sa camp vicente laguna.
5.	Researcher	Pero po sa cybercrime po?
6.	Participant 1	More on criminal investigation,
7.		Meron din po ako introduction to cybercrime po
8.	Researcher	Ilang ang percentages of resolve?
9.	Participant 1	Sa online scam crime ma'am.
0.	Researcher	Yes po.
1.	Participant	Sa online scam ma'am siguro ma'am lima lang.
2.		Kasi actually yung iba ma'am nawithdraw na
3.		Yung pera pag Nawala na yung pera dun.
4.		Ang mangyayare po sa proseso is yung
5.		Sinasabi kong application warrant .
6.	Researcher	Paano yung expenses in all of this halimbawa
7.		pupunta kayo sa court sa Ganun?
8.	Participant 1	Sagot po lahat namin lahat ng pamasahe
9.		Namin samin lahat yun.
0.	Researcher	Ayun din yung challenges.
1.	Participant 1	Yes ma'am.
2.	Researcher	Wala kayo service po?
3.	Participant 1	May mobile naming kami dalawa
4.		Pero pag sa court kasi ma'am e.
5.		Kami kami nalang lumalakad
6.	Researcher	Ah ok po.
7.		E ano pa po yun ginagastusan nyo ng
8.		Personal?
9.	Participant 1	Pag personal po halibawa unang una yun,
0.		Travel expenses namin sarili na po yun
1.		Yun pagkain saamin rin po.
2.		Di kasi pwede magksabay sabay yun e may
3.		Kanya kanya kami pupuntahan or kanya kanya
4.		Lakad pero pag entrapment operation
5.		Magkakasam naman kami niya.
6.	Researcher	Pag entrapment may kasama kayo?
7.	Participant 1	Opo, kami kami lang ma'am.
8.		Kami na rin ma'am muti tasking kami ma'am e.

9.	Researcher	Yung gamit na meron kayo yung mga
0.		available, nyo?
1.	Participant 1	Itong mga computer tatlo po yan actually
2.		Galing pa to sa 2nd hand sa crame bigay lang.
3.		Isang lang po brand new jan
4.		Computer ko lang po ma'am.
5.	Researcher	Ano specs nyan mataas po ba?
6.	Participant 1	Mataas rin naman ma'am.
7.	Researcher	And then the rest challenge niyo yun gamit?
8.	Participant 1	Yes, ma'am.
9.		Actually, ma'am may mga request po kami
0.		Kami until now wala pa printer palang
1.		Dumating galing imus and then the rest wala p
2.	Researcher	Sa local government
3.	Participant 1	Yes, ma'am sa imus city.
4.	Researcher	Di kayo nag approach kay government?
5.	Participant 1	Meron ma'am kaso until now wala pa din.
6.		Ito palang printer ma'am
7.	Researcher	If you were to assess the training available
8.		In cybercrime investigation
9.		Do you think it is sufficient?
0.	Participant 1	Actually, ma'am
1.		Meron kasi apat na training para
2.		Ayun nga introduction digital forensic,
3.		And financial fraud Intelligence communication
4.		Apat po yan e.
5.	Researcher	Pero ano po yun nakuha mo?
6.	Participant 1	Isa palang ma'am
7.		kaya di ko makuha yun tatlo kasi ma'am
8.		DS lang po ako dito hindi po talaga ako assign
9.		Ng cybercrime hineram lang ako ang
0.		Inuuna nila yung mga kapwa cybercrime
1.		Mostly sa crame mga ganun.
2.	Researcher	So dito sa inyo sino ang nakatraining
3.		Nito lahat?
4.	Participant 1	Wala pa ma'am lahat kami introduction lang.
5.	Researcher	Ah introduction palang.
6.	Participant 1	Opo ma'am.
7.	Researcher	Yung mga mabibigat na kaso
8.		Ibabato nyo pa region?
9.	Participant 1	Kami na rin ma'am
0.		base sa experience naming.
1.	Researcher	Ano ano pa yung kailangan nyo trainings?
2.	Participant 1	Yan apat ma'am.

3.		Yung introduction to cybercrime,
4.		digital forensic and financial fraud
5.		intelligence communication.
6.	Researcher	Ano ano pa yung kailangan nyo trainings
7.	Participant 1	Yan apat ma'am.
8.		Yung introduction to cybercrime,
9.		Digital forensic and financial fraud
0.		Intelligence communication
1.		Kasi ma'am yung training naming sa criminal
2.		Investigation in apply din naman naming e
3.	Researcher	Ano po kaya yung mga coping strategies
4.		ginagamit niyo para harapin yung mga
5.		Challenges niyo po?
6.	Participant 1	Nagpapractice kami teamwork at
7.		communication para mapanatili ang efficiency
8.		kahit limitado ang resources.
9.	Researcher	Ano naman po yung inyo suggestion
0.		Para maimprove?
1.	Participant 1	Una una ma'am.
2.		Yung manpower and fund support.
3.		Yun lang ma'am
4.	Researcher	Maraming salamat po sa kooperasyon
5.		At oras na inilaan po asahan po ninyo na ang
6.		Inyo pong pagkakakilanlan at mga sinabi
7.		Ay para lamang po sa aking pagaaral at
8.		hindi ko po ipagsasabi kahit kanino.
9.	Researcher	Good morning po.
0.		Thank you for taking the time to speak with me
1.		Today sir.
2.		My name is Katherine Custodio
3.		As discussed, this interview is about the
4.		Challenges faced cybercrime cases
5.		Investigation your insights will be
6.		Invaluable for my study.
7.		With your permission I would like to record our
8.		Our conversation that I capture your insight
9.		Accurately ensure confidentiality.
0.		Is that okay with you sir?
1.	Participant 2	Good morning, ma'am
2.		No problem, ma'am.
3.	Researcher	Could you please tell me your age?
4.	Participant 2	34-year-old
5.	Researcher	Thank you. And your gender?
6.	Participant 2	Male

7.	Researcher	What is your current position sir and rank in
8.		law enforcement?
9.	Participant 2	Police Staff Sergeant
0.	Researcher	Ok po.
1.		Years of service as an investigator in the
2.		cybercrime unit?
3.	Participant 2	4 years ma'am
4.	Researcher	Number of cybercrime cases na handled niyo?
5.	Participant 2	Nag range approximately 20 plus per week
6.	Researcher	Madami dami rin po pala sir.
7.	Participant 2	Oo ma'am.
8.		Ayan cybercrime ang nag increase ng crime
9.		ngayon.
0.	Researcher	I see
1.		Sir, what types of cybercrime cases na
2.		handled niyo po?
3.	Participant 2	Estafa, Phishing online shopping fraud,
4.		Swindling Photo video voyeurism
5.		Cyber libel and Violation of R.A 10175 ma'am.
6.	Researcher	What do you think is the highest?
7.	Participant 2	Online shopping fraud rampant po Talaga
8.		Nag uses sila fake online stores or products
9.		to deceive yun mamimili and these
0.		Scammers use the popular platforms
1.		Facebook especially marketplace.
2.		lang po jan is maari sila magpadala
3.		Mga peke price and notifications ganyan po.
4.	Researcher	Ah ok po mas mataas po
5.		Pala ito online shopping fraud sir.
6.	Participant 2	Yes ma'am
7.	Researcher	Out of the 20 plus cases you handled,
8.		Are all of them resolved?
9.	Participant 2	No ma'am
0.	Researcher	What percentage of cases have you resolved
1.		if the cases you handled
2.		range from 20-plus cases?
3.	Participant 2	Depende po e.
4.		But out of 20 plus cases, ma'am,
5.		Maybe only about five.
6.	Researcher	Why are there so few resolved cases?
7.	Participant 2	Minsan po kasi kaya ganyan lang
8.		Narereresolved minsan na withdraw na sa gcash
9.		Isa pa hindi narereport agad dun sa third party.
0.	Researcher	Sir, on to the challenges you encounter in

1.		Investigating cybercrime cases?
2.	Participant 2	Marami challenges e,
3.		first rapidly ng technology Malaki kasi
4.		Yung effect sa investigation naming kasi every
5.		Time na nag adopt kami ng technology,
6.		Ito naman cybercriminals mabilis din
7.		Sila nakakahanap ng paraan.
8.		Isa pa wala naman kami sapat na tools
9.		Na gagamitin.
0.		Tapos limited number of experts kasi ma'am
1.		Sa pag taas ng cybercrime mas nangangailang
2.		Pa kami ng marami expert personnel.
3.	Researcher	Manpower po or limited number of experts
4.		And tools ang challenges po?
5.	Participant 2	Opo ma'am
6.	Researcher	Sir, what about po sa facilities na meron po
7.		Cybercrime unit?
8.	Participant 2	Sa totoo lang kulang sa facilities kulang talaga
9.		Inventory Labs natin example po yung mga
0.		Server room so nagkakaroon talaga sa pag
1.		analyze sa digital evidence.
2.	Researcher	Kaya po nagkakaroon ng delays sa
3.		investigation?
4.	Participant 2	Oo
5.	Researcher	What about your resources and equipment?
6.	Participant 2	We have the equipment pero hindi pa naman
7.		Sapat.
8.		Kulang paring resourse namin tulad ng
9.		high-tech tools.
0.		Nag requested po kami kaso di pa rin
1.		dumadating.
2.		And marami sa mga devices is outdated
3.		Or second hand na kaya deficiencies in
4.		digital forensics.
5.		Isa pa sa challenge is yung fund support,
6.		Para makabili ng kagamitan at mabigay yung
7.		Tamang training sa mga cybercrime personnel.
8.		May mga training naman kami.
9.		Kaso kulang sa resourses ayun po.
0.	Researcher	So ito po yung mga challenges na encounter
1.		During investigation.
2.		limited number of experts and fund support
3.		And resources?
4.	Participant 2	Yes, ma'am.

5.		Ayan yung mga challenges po para saakin.
6.	Researcher	Paano nakakaapekto ang pagbabago
7.		Sa technology sa inyo investigation?
8.	Participant 2	Mas gumagaling yung mga cybercriminal
9.		Kesa samin.
0.	Researcher	How does the lack of resources impact your
1.		Ability to investigate effectively?
2.	Participant 2	Malaki.
3.		Kulang kami sa high tech tools
4.		outdated pa karamihan sa devices
5.		Wala sapat na funds.
6.	Researcher	Okay sir,
7.		How can you assess the training you have?
8.	Participant 2	Ok naman yung sa training or schooling namin
9.		Provided naman ni PNP helpful naman.
0.		Especially Technical aspects meron kami
1.		Introduction to cybercrime ok naman.
2.	Researcher	Nakakatulong naman po kahit papaano.
3.	Participant 2	Opo.
4.	Researcher	Gaano kadalas ka sumasali sa mga
5.		training programs?
6.	Participant 2	Minsan po.
7.		Once or 6 months or kaya quarterly
8.	Researcher	What is their specific area within the
9.		training programs that you believe are lacking
0.		or require more focus?
1.	Participant 2	Mas maganda sana kung mas maraming
2.		Focus sa mga advanced digital
3.		forensic tools.
4.	Researcher	What are the Most Beneficial Aspects of the
5.		Training and areas for improvement
6.	Participant 2	Dabest Talaga yung actual case studies po.
7.	Researcher	Sir, what additional training and resources are
8.	Participant 2	Necessary to enhance your skills in cybercrime
9.		Continuous education or additional training
0.		Workshop On the latest technology machine
1.		Learning Digital forensic software is more
2.		effectively.
3.	Researcher	Are there specific applications or tools
4.		You believe Are their specific applications or
5.		Purchase subscription?
6.	Participant 2	Yes ma'am
7.		Updating forensic software and subscribing
8.		To cybercrime databases para matulungan

9.		Yung pag identifying tracking.
0.	Researcher	Those sound-like important resources.
1.	Participant 2	Yes ma'am
2.	Researcher	What coping mechanisms or strategies
3.		Do investigators manage the challenges
4.	Participant 2	Continuous Training yan po yung
5.		makakatulong samin.
6.	Researcher	Moving on to recommendations,
7.		What suggestions do you have to improve
8.		The overall Capacity of the PNP in
9.		Addressing cybercrime?
0.	Participant 2	Additional specialized personnel na focus on
1.		Cybercrime To make it faster and more
2.		Effectively to address the case and have a
3.		Higher technologies.
4.	Researcher	Sir How do you see collaboration with other
5.		Agencies Playing a role in this improvement?
6.	Participant 2	Yes ma'am
7.		Enhance information sharing and inter-agency
8.		Support To allow us to tackle cybercrime more
9.		Effectively.
0.	Researcher	How can external partnerships, such as with
1.		University Tech companies, enhance your
2.		Capabilities?
3.	Participant 2	Collaborating with the universities that focus
4.		On cybercrime can provide training and
5.		Research opportunities tailored to our needs.
6.	Researcher	Maraming salamat po sa kooperasyon
7.		At oras na inilaan po asahan po ninyo na ang
8.		Inyo pong pagkakakilanlan at mga sinabi
9.		Ay para lamang po sa aking pagaaral at
0.		hindi ko po ipagsasabi kahit kanino.
1.	Participant 2	Thank you, good luck, with your study.
2.	Researcher	Good morning po.
3.		Thank you for taking the time to speak with me
4.		Today sir.
5.		My name is Katherine Custodio
6.		As discussed, this interview is about the
7.		Challenges faced cybercrime cases
8.		Investigation your insights will be
9.		Invaluable for my study.
0.		With your permission I would like to record our
1.		Our conversation that I capture your insight
2.		Accurately ensure confidentiality.

3.		Is that okay with you sir?
4.	Participant 3	Morning ma'am
5.		Ok po.
6.	Researcher	Ready na po kayo?
7.	Participant 3	Opo ma'am
8.	Researcher	Could you please tell me your age?
9.	Participant 3	31-year-old
0.	Researcher	How many years have you been in the service?
1.	Participant 3	6 years
2.	Researcher	In cybercrime unit po?
3.	Participant 3	2-year na rin mahigit
4.	Researcher	Okay po.
5.		What course did you complete? undergrad
6.	Participant 3	BS Criminology
7.	Researcher	How many cases do you handle? Range week
8.	Participant 3	Range 15 cases.
9.	Researcher	What are the types of cybercrime cases
0.		handled?
1.	Participant 3	More on swindling, Violation of 10175
2.		And then Cyber libel phishing.
3.	Researcher	What specific types of cybercrime cases
4.		Encounter most frequently?
5.	Participant 3	Phishing ma'am
6.		Hacking phishing mga nagpapadala ng fake
7.		Email Or nag aalok ng mga fake websites
8.		Tapos para kunin yun mga personal
9.		Informations username mo password credit
0.		Cards details mo yan po yung madalas.
1.	Researcher	Phishing talaga.
2.	Participant 3	Oo ma'am.
3.	Researcher	Do you think all 15 cases
4.		How many of your cases have you resolved?
5.	Participant 3	4 to 6 lang yung nareresolved
6.	Researcher	Why are there so few resolved cases?
7.	Participant 3	Minsan po.
8.		Kaya di po nareresolved agad lahat
9.		Yung complainant po Di complete yung
0.		Documents
1.	Researcher	Which is kaya tumatagal din yun pag process
2.		What other challenges have you encountered?
3.	Participant 3	Sa totoo lang, kakaunti lang expert sa
4.		Cybercrime sa atin po.
5.		Challenges rin yung resources sa digital
6.		Forensics tools.

7.	Researcher	Need niyo po talaga need skilled personnel
8.		and tools?
9.	Participant 3	Opo.
0.		Need talaga ng fund support ng makapag
1.		Update ng mga tools na kailangan ng mga
2.		Investigator.
3.	Researcher	Dami po pala mga challenges na encounter
4.		Ng cybercrime investigator.
5.	Participant 3	Oo ma'am.
6.		Dahil Talaga sa digital word po.
7.	Researcher	How does technology change affect
8.		Your investigations?
9.	Participant 3	We constantly need to update
0.		Our knowledge and tools.
1.	Researcher	How does the lack of resources impact your
2.		Ability to investigate effectively?
3.	Participant 3	Malaki impact lack of resources kaya minsan
4.		Matagal yung pag process ng investigation.
5.	Researcher	What is your assessment of the current training
6.		Programs available for cybercrime investigators
7.		In the PNP
8.	Participant 3	Effective naman training na available samin.
9.		Sa cybercrime investigations.
0.	Researcher	Are there specific areas within the training
1.		Programs that You believe are lacking or
2.		Require focusing?
3.	Participant 3	More focus on advanced digital forensic and
4.		Soft skills.
5.	Researcher	What specific aspects of the training do you find
6.		Most Beneficial for your role as a cybercrime
7.		Investigator?
8.	Participant 3	Actually ma'am
9.		Yung real-case simulations during training
0.		Yung pinaka-nakatulong kasi na-expose kami
1.		Sa actual investigations.
2.	Researcher	Are there aspects or topics you feel are
3.		Insufficiently addressed?
4.	Participant 3	Oo ma'am
5.		More topic pa sa deepfakes and AI powered
6.		Need pa iupdate training materials na meron
7.		Jan.
8.	Researcher	How would you compare the training you
9.		Received on Cybercrime with other forms of

0.		Training you have Experienced in law
1.		Enforcement?
2.	Participant 3	In my personal experience challenging yung
3.		Cybercrime mas Mas focus niya kasi technology
4.		So, need mo pa continuous training or
5.		Updating.
6.	Researcher	What additional training and resources are
7.		Necessary to enhance your skills in cybercrime
8.		investigations?
9.	Participant 3	More on advanced digital forensic training
0.		I expand pa.
1.	Researcher	What specific skills do you think require further
2.		development for effective cybercrime
3.		Investigation?
4.	Participant 3	Yung soft skills forensic tools at AI-based
5.		Analysis.
6.	Researcher	Are there specific technologies or tools you
7.	Participant 3	Oo naman.
8.		Mag-adopt tayo ng AI-driven forensic software.
9.	Researcher	What resources do you believe should be more
0.		readily available for investigators?
1.	Participant 3	Update forensic software's and high specs
2.		Computers and Secure storage servers and
3.		Reliable din ng internet Connection
4.		Para mapabilis po yung pag transfer.
5.	Researcher	In what formats do you prefer to receive this
6.		Additional training?
7.	Participant 3	Mas ok sakin ma'am.
8.		Combined approach may hand on Training na
9.		May online courses parang flexible learning
0.		Ganun po.
1.	Researcher	Okay po.
2.		What coping mechanisms or strategies do
3.		Investigator to manage the challenges?
4.	Participant 3	Adaption of technology, AI-based forensic tools
5.		Improve investigation efficiency.
6.	Researcher	What recommendations would you suggest
7.		Improving the overall capacity of the PNP in
8.		Addressing cybercrime?
9.	Participant 3	Pondo ma'am at training Kailangan din ng mas
0.		Maraming skilled personnel at updated na tools.
1.	Researcher	How do you see collaboration with other
2.		Agencies playing a role in this improvement?
3.	Participant 3	Strong collaboration and joint operations.

4.	Researcher	How can external partnerships, such as
5.		With universities or tech companies,
6.		Enhance your capabilities?
7.	Participant 3	Actually ma'am
8.		Pwede tayo makipag collaborate with other
9.		Partnerships na makakatulong sapag develop
0.		Methods and techniques against cybercrime.
1.		And also, mapapalawak pa natin yung network
2.		Natin.
3.	Researcher	Maraming salamat po sa kooperasyon
4.		At oras na inilaan po asahan po ninyo na ang
5.		Inyo pong pagkakakilanlan at mga sinabi
6.		Ay para lamang po sa aking pagaaral at
7.		hindi ko po ipagsasabi kahit kanino.
8.	Participant 3	Walang anuman ma'am.
9.	Researcher	Good morning po.
0.		Thank you for taking the time to speak with me
1.		Today sir.
2.		My name is Katherine Custodio
3.		As discussed, this interview is about the
4.		Challenges faced cybercrime cases
5.		Investigation your insights will be
6.		Invaluable for my study.
7.		With your permission I would like to record our
8.		Our conversation that I capture your insight
9.		Accurately ensure confidentiality.
0.		Is that okay with you sir?
1.	Participant 4	Morning, po.
2.	Researcher	Ok po.
3.		Start na po tayo
4.	Participant 4	Yes ma'am
5.	Researcher	Sir, how many years have you been in the
6.		Service?
7.	Participant 4	6 years po
8.	Researcher	Sir, how many years have you been in the
9.		Cybercrime investigation unit?
0.	Participant 4	Mga 2 years na mahigit
1.	Researcher	Sir, what types of cybercrimes do you deal with
2.		As an investigator?
3.	Participant 4	Online shopping scam ma'am.
4.	Researcher	Bakit po kaya?
5.	Participant 4	Kasi ganito po yan sila kasi yung mga
6.		Nagtatayo Ng mga fake na online shopping site
7.		Ito yung mga nagaalok ng popular na products

8.		Sa murang halaga then kapag nagbayad na
9.		Tong victim e hindi na nil mahigilap yung
0.		Kanila order.
1.	Researcher	Ah para pong sa marketplace sa facebook?
2.	Participant 4	Oo ma'am.
3.		Dami talaga ganun nangyayare
4.		lalo na sa panahon ngayon na mas maraming
5.		tao ang nag-online shopping.
6.	Researcher	Kaya nga sir e.
7.		Sir, in your 3 years in the cybercrime unit,
8.		How many cases have you handled? Per week
9.	Participant 4	In 3 years, cybercrime umaabot 15 cases
0.	Researcher	Out of the 15 cases you handle, how many
1.		How many have been resolved?
2.	Participant 4	Not all. Sometimes,
3.		Only 3 to 5 cases ang nare-resolve namin
4.		Bawat buwan.
5.	Researcher	Why, sir, are only a few of them being
6.		resolved?
7.	Participant 4	Bukod sa mga hamon sa ebidensya,
8.		Malaking factor din ang kakulangan sa mga
9.		Modern tools at software na kailangan sa
0.		Digital forensics.
1.	Researcher	Things you use now, like computers,
2.		Are all brand new?
3.	Participant 4	Yung computer po, yung iba jan 2nd hand na.
4.		Isa palang yung bago jan.
5.	Researcher	Sir, is there a shortage of manpower?
6.	Participant 4	Kulang na kulang po Dahil sa dami ng trabaho,
7.		At kami Cybercrime investigators madalas
8.		Nahihirapan na tapusin understaffed na kami.
9.		Yung lahat ng mga kaso. Kung kulang sa tao
0.		Nagiging understaffed na kami.
1.		Magkaroon ng sapat ng funds para mabili yung
2.		Mga high performance system."
3.	Researcher	Challenge niyo po outdated or secondhand
4.		Tools and limited personnel with expertise
5.		And funds?
6.	Participant 4	Yes ma'am
7.	Researcher	Nag request po ba kayo sa local government?
8.	Participant 4	Meron ma'am.
9.		Kaso wala pa rin yung request namin.
0.	Researcher	Paano naaapektuhan ng pagbabago sa
1.		Technology in your investigation?

2.	Participant 4	Kailangan namin ng mas advanced na tools
3.		At software para mapadali ang digital forensics
4.		At maiwasan ang network breaches
5.	Researcher	Paano naaapektuhan ng kakulangan sa
6.		Resources capacity in investigation?
7.	Participant 4	Nagkakaroon kami ng lack sa modern tools
8.		Manpower, at pondo na nagreresulta sa mas,
9.		mahirap na pagresolba ng kaso at mas mabagal
0.		Na process.
1.	Researcher	How would you assess the current training
2.		Programs that you have?
3.	Participant 4	May basic cybercrime course ako na tinuruto
4.		Nila yung mga fundamentals ng cybercrime
5.		Schooling kaya ok naman training.
6.	Researcher	How frequently have you participated in training
7.		Programs?
8.	Participant 4	Frequently sumali sa training programs,
9.		At very relevant Content sa trabaho ko
0.		As cybercrime investigator.
1.	Researcher	Are there specific areas within the training
2.		Program that you believe are lacking
3.		Or require more focus?
4.	Participant 4	Sa tingin ko, kulang pa ang focus sa advanced
5.		Digital forensics at cybercrime law sa mga
6.		Trainings.
7.	Researcher	What specific aspects of the training do you
8.		find the most beneficial for your role?
9.	Participant 4	Ang pinaka-nakapag-benefit sa akin ay yung
0.		Mga updated na techniques sa digital
1.		Investigation.
2.	Researcher	Are there aspects or topics you feel are
3.		insufficient?
4.	Participant 4	Sa tingin ko, kulang pa ang practical hands-on
5.		sessions.
6.	Researcher	How would you compare the training you
7.		Received Cybercrime with other forms of
8.		training you have on experienced in
9.		law enforcement?
0.		Mas comprehensive ang training sa cybercrime
1.	Participant 4	Compare sa iba pang law enforcement training.
2.	Researcher	In your opinion, what additional training and
3.		Are resources needed to enhance your skills?
4.	Participant 4	Para ma enchance siguro yung training sa

5.		Malware analysis kasi matutunan ng mga
6.		Kapulisan.
7.		Paano suriin ang malware programs at paano
8.		Kumakalat yan mga yan at kung paano
9.		Maiiwasan ang mga network breaches.
0.	Researcher	What specific skills do you think require further
1.		Development for effective cybercrime
2.		investigation?
3.	Participant 4	We still need advanced skills in digital
4.		forensics.
5.	Researcher	Are there specific technologies or tools you
6.		Believe your unit should adopt.
7.	Participant 4	Yes, more modern and high-performance
8.		Hardware and updated forensic software.
9.	Researcher	What resources (software, hardware) do you
0.		Believe should be more readily available for
1.		Investigator?
2.		In what formats do you prefer to receive this
3.		Additional example online courses etc?
4.	Participant 4	I prefer hands-on workshops and online
5.		courses.
6.		Para mas madali matutunan at ma-apply.
7.	Researcher	What coping mechanisms or strategies
8.		manage the challenges?
9.	Participant 4	As investigator mag develop new methods
0.		To solve cases efficiently and resources
1.		Upgrading funding ma'am.
2.		Ok po.
3.	Researcher	What would you recommend improving
4.		the overall capacity of the PNP?
5.	Participant 4	Pag-upgrade ng Hardware yung high RAM at
6.		Fast processors yung Pag-upgrade ng
7.		Makakatulong para mabilis nap ag process
8.		Ng mga large data files backup storage
9.		Para sa mga malalaking data sets.
0.		Syempre para mabili natin yan yung
1.		fund support ayusin or Lakihan
2.		Tapos mag-invest sa mga mas advanced na
3.		Cybercrime tools Kung may continuously
4.		Training program.
5.	Researcher	How about sir sa collaboration or partnership
6.		po other agencies for improvement?
7.	Participant 4	Actually, Mahalaga naman yung collaboration,
8.		Pero minsan mahirap ang coordination at

9.		Communication Sa ibang agencies.
0.		Kung may share platforms
1.		At regular training, magiging mas mabilis at
2.		Mas effective ang pagtutulungan namin
3.	Researcher	University or private sector po for
4.		partnership improvement po?
5.	Participant 4	Mahalaga ang partnership namin sa universities
6.		At private sector, lalo na sa training at
7.		Research.
8.		Nakakatulong sila sa long term ng knowledge
9.		Namin sa mga new technology at cybercrime
0.		Trends Kung magtutulungan kami makakakuha
1.		Kami ng mga resources at expertise na
2.		Kailangan namin.
3.	Researcher	Tama po sir.
4.		Maraming salamat po sa kooperasyon
5.		At oras na inilaan po asahan po ninyo na ang
6.		Inyo pong pagkakakilanlan at mga sinabi
7.		Ay para lamang po sa aking pagaaral at
8.		hindi ko po ipagsasabi kahit kanino.
9.	Participant 4	Ok po.
0.	Researcher	Good morning po.
1.		Thank you for taking the time to speak with me
2.		Today sir.
3.		My name is Katherine Custodio
4.		As discussed, this interview is about the
5.		Challenges faced cybercrime cases
6.		Investigation your insights will be
7.		Invaluable for my study.
8.		With your permission I would like to record our
9.		Our conversation that I capture your insight
0.		Accurately ensure confidentiality.
1.		Is that okay with you ma'am?
2.	Participant 5	Morning, po. Madam
3.	Researcher	Start na po tayo?
4.	Participant 5	Go madam.
5.	Researcher	How many years have you been in service?
6.	Participant 5	8 years madam.
7.	Researcher	To the cybercrime unit?
8.	Participant 5	3 years
9.	Researcher	In your 3 years in cybercrime investigation,
0.		How many cases did you handle per week?
1.	Participant 5	Around 5 to 10 cases
2.	Researcher	Out of the 5 to 10 cases you catered to have

3.		You resoled all of them?
4.	Participant 5	Not all Madam.
5.	Researcher	What Types of cybercrime cases handled?
6.	Participant 5	Estafa, Online Fraud Fake Investment,
7.		Cyber harassment mg ana handle ko.
8.	Researcher	What other challenges do you encounter during,
9.		Cybercrime investigations?
0.	Participant 5	Mag tatagalog na ko madam ah HAHA
1.	Researcher	Sigi ma'am
2.	Participant 5	Ano madam ahm.
3.		Yung policies yung nagpapahirap sa amin
4.		Pagkuha ng, Mula sa mga third-party online
5.		Platforms or online Payment system ay
6.		nakikipagtulugan sa mga investigation.
7.	Researcher	Mga policies po.
8.	Participant 5	Oo madam di lang policies e pati.
9.		Yung limited manpower kasi Sa dami ng mga
0.		Kaso na dumarating hindi kami palaging
1.		makakapag focus sa bawat isa kaya tumatagal
2.		Ang inestigation.
3.		Isa pa ma'am modern tools or technology
4.		May mga Computer kami at iilang ma software
5.		Hindi palagi sapat mga tools namin lalo na sa
6.		Digital forensic ma'am.
7.	Researcher	Ok po.
8.		Challenges Policies Limits manpower and tools
9.	Participant 5	Yes
0.	Researcher	What specific types of cybercrime cases do
1.		Encounter most frequently?
2.	Participant 5	Most common online fraud fake investment.
3.	Researcher	How does technology change affect your
4.		investigations?
5.	Participant 5	Effect.
6.		Kailangan natin mag update ng strategies and
7.		Tools para maging effient
8.	Researcher	How would you assess the current training
9.		Programs you have?
0.	Participant 5	Marami nga mga training pero,
1.		Wala naman kaming mga tools na pwede
2.		Sana Magamit namin sa investigation.
3.		Ang nagiging hadla lang limited yung resourses
4.		Marami nga mgatraining pero
5.		Wala naman kaming mga tools na pwede sana
6.		Magamit namin sa investigation.

7.	Researcher	How frequently have you participated in training
8.		Programs?
9.	Participant 5	I think helpful naman yung training na meron
0.		kami.
1.	Researcher	Are there specific areas within the training
2.		Programs that you believe are lacking
3.		or require more focus?
4.	Participant 5	Focus more on advanced digital forensic tools.
5.	Researcher	What specific aspects of the training do you
6.		Find most beneficial for your role as a
7.		cybercrime investigator?
8.	Participant 5	Ang pinaka magbenefit kami rin naman po.
9.		Lalo na sa tools na makakatulong sa
0.		Investigation namin.
1.	Researcher	How would you compare the training you
2.		Received on cybercrime with other forms of
3.		Training you have experienced in law
4.		enforcement?
5.	Participant 5	Mas technical sa cybercrime mabilis mag
6.		Evolve kumpara other training sa PNP mas
7.		Challenging kasi need namin
8.		Malawak na knowledges sa mga digital tools.
9.	Researcher	What specific skills do you think require further
0.		Development for effective cybercrime
1.		investigation?
2.	Participant 5	Training talaga sa digital forensics and
3.		Advanced software
4.	Researcher	Are there specific technologies or tools you
5.		believe your unit should adopt?
6.	Participant 5	AIs digital forensic at software's
7.		Na mas makakatulong mapabilis sa pag
8.		Retrieve madam.
9.	Researcher	What resources do you believe should be more
0.		readily available for investigators?
1.	Participant 5	Sapat na pondo for infrastructure at training.
2.		Yung workshop na onsite at mas maganda
3.		Kung may record modules.
4.	Researcher	What coping mechanisms or strategies do
5.		Investigators manage the challenges?
6.	Participant 5	Advocating support and resources is a strategy
7.		To address resource limitations.
8.	Researcher	What recommendations would you suggest
9.		Improving overall capacity of the PNP in

0.		addressing cybercrime?
1.	Participant 5	Magdadag siguro ng pondo at support
2.		Ng government.
3.		Para mas improve yung infrastructure at
4.		Technological upgrades yung pang long term
5.		Funding strategies.
6.	Researcher	Okay po noted po.
7.		How about collaboration with other agencies
8.		Role in this improvement?
9.	Participant 5	Solid dapat yung coordination namin lalo na sa
0.		International level.
1.	Researcher	In external partnership like universities or
2.		Technology companies to enhance
3.		your capabilities?
4.	Participant 5	Definitely madam.
5.		Makakatulong yung external partnership
6.		Para makakuha pa kami ng new knowledge
7.		Sa bago technology.
8.	Researcher	Maraming salamat po sa kooperasyon
9.		At oras na inilaan po asahan po ninyo na ang
0.		Inyo pong pagkakakilanlan at mga sinabi
1.		Ay para lamang po sa aking pagaaral at
2.		hindi ko po ipagsasabi kahit kanino.
3.	Participant 5	Salamat madam.