Vol. 7, No. 11, November 2026. pp. 4197-4217
E-ISSN:2723 – 6692
P-ISSN:2723– 6595
https://doi.org/10.59141/jiss.v7i11.2605

Effectiveness Of Handling General Criminal Offenses By The Criminal Investigation Unit Of Jembrana Police Department, Bali Regional Police

Naufal Aqil Rizqulloh*, Mas Rahmah, Suparto Wijoyo, Prawitra Thalib
Universitas Airlangga Surabaya, Indonesia
Email : naqil6647@gmail.com*

Keywords:
Effectiveness, General Crime, Criminal Investigation Unit

This is an open access article under the CC BY-SA license.

Copyright © 2026 by Author. Published by Publikasi Indonesia

Abstract

This study evaluated the effectiveness of online fraud case handling by the Criminal Investigation Unit of the Jembrana Resort Police, Bali Regional Police, within its broader mandate to investigate general criminal offenses. An empirical socio-legal approach with a qualitative descriptive design was employed, incorporating interviews, observations, document analysis, and administrative records covering 2022–2025. The findings included statements from four police officers, although the total number of informants was not specified. The number of newly reported fraud cases declined from 24 in 2022 to 20 in 2023, seven in 2024, and three in 2025, while recorded case closures totaled 19, 24, eight, and three, respectively. The annual case closure-to-intake ratios exceeded 100% in 2023 and 2024, suggesting that some closures may have involved cases carried over from previous years. However, these aggregate figures did not establish cohort-specific resolution rates or demonstrate improvements in investigation speed without case-level data. Administrative records also indicated increased participation in cybercrime investigation training, while interviewed officers emphasized the importance of timely crime reporting, digital evidence preservation, and coordination with financial institutions and specialized police units. The principal challenges included inadequate digital forensic facilities, disparities in investigators' technical competencies, delayed reporting by victims, and perpetrators' use of fraudulent identities and anonymous online accounts. Public satisfaction summaries indicated generally favorable perceptions of police services, although the underlying sampling procedures and measurement methods remained unclear. The study contributed an integrated assessment of administrative performance indicators, investigative practices, and public service quality in handling online fraud cases. The findings highlighted the need to strengthen digital forensic investigation capabilities, standardize case monitoring and documentation procedures, improve communication with victims, and establish verifiable performance indicators to assess investigative effectiveness and case resolution outcomes.

INTRODUCTION

Digital communication has expanded opportunities for social and economic interaction while simultaneously transforming the methods used to commit fraud (Kolhe & Bhat, 2024; Shang et al., 2025; Yufriadi et al., 2024). Online transactions, social media platforms, and instant messaging applications enable perpetrators to approach victims remotely while concealing their identities. These developments require law enforcement agencies to adapt their

investigative procedures while upholding legal certainty, procedural fairness, and institutional accountability (Sumarna, 2025; Wathan, 2025). In Indonesia, online fraud has been examined as a form of cybercrime that exploits vulnerabilities in digital literacy and electronic transaction verification (Ardoni, 2022; Sahara & Kuswandi, 2025). Similarly, Lesmana et al. (2023) emphasized the importance of adapting law enforcement practices to technological developments. These challenges are particularly relevant to the Criminal Investigation Unit (Satuan Reserse Kriminal, Satreskrim) of the Jembrana Resort Police (Kepolisian Resor Jembrana), Bali Regional Police (Kepolisian Daerah Bali), which is responsible for investigating general criminal offenses. However, the empirical evidence examined in this study specifically concerned online fraud cases. Therefore, the assessment of investigative effectiveness was limited to this category rather than encompassing all general criminal offenses handled by the unit.

The urgency of addressing online fraud stems from the complexities of digital evidence and the circumstances surrounding victim reporting. Fraudulent transactions frequently involve accounts registered under false or third-party identities, electronic communications that can be deleted or manipulated, and financial transfers across institutions or jurisdictions. Delayed reporting may complicate digital evidence preservation, transaction tracing, and suspect identification, requiring investigators to coordinate with financial institutions, telecommunications service providers, and specialized cybercrime investigation units (Gusdiar et al., 2026; Haq et al., 2023). Kurniawan (2025) highlighted the importance of integrated digital policing, while previous studies identified institutional capacity limitations and technical challenges associated with cybercrime investigations (Hariyanto & Kusumah, 2026; Siregar et al., 2024; Wathan, 2025). These circumstances demonstrate that investigative effectiveness cannot be adequately assessed solely through the number of administratively closed cases. A comprehensive assessment must also consider the lawful acquisition and preservation of electronic evidence, procedural compliance, communication with complainants, and the identification of unresolved investigative obstacles. Furthermore, distinctions must be maintained among case registration, administrative closure, evidentiary completeness, referral for prosecution, and recovery of victims' financial losses, as these represent different dimensions of investigative outcomes.

Administrative records from the Jembrana Resort Police provided an empirical basis for examining online fraud investigation performance. The number of reported online fraud cases declined from 24 in 2022 to 20 in 2023, seven in 2024, and three in 2025, while recorded case closures totaled 19, 24, eight, and three, respectively. These figures demonstrated a declining trend in annual case registrations throughout the observation period. The corresponding annual case closure-to-intake ratios were approximately 79.17%, 120%, 114.29%, and 100%, respectively. Ratios exceeding 100% indicated that the number of cases closed during particular years surpassed the number of newly registered cases. However, without case-level records, these figures could not establish whether the closures involved cases carried over from previous years or determine the duration of individual investigations. Similarly, declining complaint registrations and relatively high annual closure ratios did not independently demonstrate improvements in investigative effectiveness. Therefore, these administrative indicators needed to be interpreted alongside evidence concerning investigators' professional competencies,

investigative procedures, technological resources, interagency cooperation, and the quality of services provided to complainants.

Previous research on technology-facilitated fraud investigations provided several relevant perspectives. Wahyudin et al. (2024) emphasized the importance of cross-institutional coordination in online fraud investigations, while Nurjanah and Masrukhin (2026) examined the evidentiary significance of electronic records in criminal proceedings. Aji (2024) investigated the performance of police criminal investigation units and highlighted the importance of operational capabilities, whereas Ananda (2020) discussed investigative difficulties associated with perpetrators using anonymous accounts and fraudulent identities. Collectively, these studies suggested that organizational capacity and digital investigative competence represented related but distinct dimensions of law enforcement effectiveness. The availability of investigative personnel did not necessarily guarantee adequate digital forensic expertise, while established coordination mechanisms did not automatically ensure timely access to relevant evidence. Building on these perspectives, the present study examined online fraud investigations at the district police level by integrating administrative case records, investigator training participation, investigative procedures, and reported public satisfaction. This multidimensional approach enabled a more comprehensive interpretation of available performance indicators while identifying limitations in the supporting evidence.

The research gap addressed in this study extended beyond the limited availability of empirical investigations within a particular police jurisdiction. Previous studies had generally examined legal frameworks, online fraud characteristics, investigative procedures, or organizational performance as separate research dimensions. However, limited attention had been given to integrating operational case records with investigators' experiences of institutional coordination, technological constraints, professional competencies, and public service delivery within the same local police institution. Annual case closure ratios could indicate substantial administrative throughput without necessarily demonstrating timely investigations or satisfactory outcomes for victims. Similarly, increased participation in professional training did not automatically establish improvements in investigative competence or case processing efficiency. To address these limitations, the present study combined descriptive administrative indicators with qualitative evidence concerning investigative practices, institutional coordination, and operational challenges. Rather than assuming consistency across all performance measures, the analysis acknowledged discrepancies and limitations in the available records. The study's contribution therefore lay in developing an integrated, evidence-based interpretation of investigative effectiveness in handling online fraud cases at the local law enforcement level.

The study adopted organizational performance and law enforcement effectiveness perspectives to examine the institutional and procedural dimensions of online fraud investigations. Organizational performance was assessed in relation to the ability of the Criminal Investigation Unit to fulfill its investigative responsibilities through available personnel, technological resources, operational procedures, and interagency coordination. Meanwhile, law enforcement effectiveness was examined through considerations of evidentiary adequacy, procedural compliance, investigative accountability, and the protection of

complainants' rights (Sintasari et al., 2025). These perspectives emphasized that investigative effectiveness could not be inferred exclusively from administrative case statistics. Increased participation in cybercrime investigation training, for example, could indicate institutional efforts to strengthen professional capacity but did not independently verify improvements in investigative competence. Similarly, an increase in the number of respondents reporting satisfaction with police services did not necessarily represent an improvement in satisfaction rates, particularly when survey sample sizes and measurement procedures varied. Accordingly, case handling outcomes, professional training records, and public satisfaction data were interpreted descriptively, with attention to the methodological limitations affecting comparisons across years. This approach was particularly important because the available records did not provide comprehensive investigation duration data, case-level backlog information, or consistently standardized public satisfaction measurements.

Against this background, the study aimed to evaluate the effectiveness of online fraud case handling by the Criminal Investigation Unit of the Jembrana Resort Police, examine the roles of investigator professionalism and interagency coordination, and identify procedural, technological, and public service challenges affecting investigative performance. Specifically, the research sought to interpret annual case registration and closure statistics while distinguishing administrative case processing from the resolution of specific case cohorts, assess the evidentiary value of professional training and public satisfaction records, and formulate practical recommendations for improving digital evidence preservation, investigator competency development, administrative recordkeeping, victim communication, and case monitoring. Academically, the study was expected to contribute a more comprehensive framework for evaluating cybercrime investigation performance within local law enforcement institutions. Practically, the findings were intended to support institutional decision-making by identifying operational improvements and data requirements necessary for transparent and accountable performance evaluation. Nevertheless, the study's conclusions were restricted to the available administrative records and interview evidence concerning online fraud investigations and could not be generalized to all categories of general criminal offenses.

METHOD

This study employed an empirical socio-legal approach (Soekanto, 2019) with a qualitative descriptive design (Creswell, 2014; Sugiyono, 2020) to examine criminal investigation practices at the Jembrana Resort Police, Bali. The research focused specifically on online fraud cases handled by the Criminal Investigation Unit (Satuan Reserse Kriminal, Satreskrim), although the unit's broader jurisdiction encompassed general criminal offenses. The units of analysis included investigative procedures, organizational practices, services provided to complainants, and administrative case records covering 2022–2025. The research location was purposively selected based on the unit's responsibilities for preliminary inquiries and criminal investigations, as well as its access to relevant case handling records. Because the dates and duration of field interviews and observations were not fully documented, the findings were interpreted within the available study period rather than as evidence of continuous operational monitoring.

Informants were purposively selected based on their involvement in criminal investigation activities, including the Head of the Criminal Investigation Unit, operational and investigative officers, case administration personnel, and complainants where available. The findings included statements from four identified police officers, although the total number of informants was not documented. Data were collected through interviews, observations, and document reviews involving relevant legislation, administrative case records, investigator training records, and public satisfaction summaries. These sources provided complementary information on investigative procedures, digital evidence management, interagency coordination, and operational challenges. However, the available documentation did not fully describe the interview instruments, observation procedures, consent processes, or methods used to validate the public satisfaction data.

Data were analyzed using qualitative descriptive analysis through data selection, thematic categorization (Miles et al., 2014), comparison of interview findings with administrative records, and interpretation of relevant investigative practices. The analysis focused on case resolution, investigator competence, timeliness and accuracy of investigations, public satisfaction, and technological and institutional constraints. Administrative performance was examined using annual case closure-to-intake ratios, calculated by dividing the number of cases closed by the number of newly reported cases in the corresponding year. These ratios were interpreted as descriptive indicators of case processing rather than cohort-specific resolution rates. Investigator training records were assessed as indicators of participation rather than verified professional competence, while public satisfaction data were interpreted proportionally when the relevant denominators were available. The absence of case-level processing times, comprehensive backlog records, and standardized validation procedures limited the assessment of investigative effectiveness and prevented stronger causal conclusions regarding institutional performance.

RESULTS AND DISCUSSIONS

The Effectiveness of Online Fraud Case Disclosure

The effectiveness of disclosing online fraud cases is a measure of the success of the Jembrana Police Criminal Investigation Unit in uncovering the perpetrators, finding evidence, and resolving cases to the filing stage. Based on the results of the study, the effectiveness of disclosing cases is influenced by the speed of receiving reports, the ability to analyze digital evidence, interagency coordination, and the response of the community in providing supporting information to investigators.

Annual administrative reports recorded 24 new online-fraud complaints in 2022, 20 in 2023, seven in 2024, and three in 2025. Thus, the recorded volume declined over the period rather than increased. The available figures distinguish new registrations (CT) from closures recorded during each calendar year (CC). These two quantities need not refer to the same cohort of cases, so a closure-to-intake ratio cannot alone establish the rate of resolution of cases registered in that year.

There were 19 closures and 24 new reports in 2022 (19/24 = 79.17%); 24 closures and 20 new reports in 2023 (120%); eight closures and seven new reports in 2024 (114.29%); and three

closures and three new reports in 2025 (100%). Ratios exceeding 100% are arithmetically possible when closures include cases registered before the current year, but the original case-level data are not provided to confirm the age or origin of the closed cases. The 100% ratio in 2025 likewise cannot establish that every case newly registered in that year was closed. These indicators describe annual case-handling throughput, not cohort-specific clearance rates or investigation times.

The figures indicate that Jembrana Police recorded closures in each of the four observed years, including years in which closures exceeded new reports. They are not sufficient, on their own, to conclude that effectiveness increased from year to year. A stronger assessment would require opening and closing dates for individual cases, the status of remaining cases, reasons for closure, evidentiary completeness, and prosecution outcomes. Interviews and descriptions of cooperation with banks and specialist cybercrime units provide relevant qualitative context but do not replace those records.

The substantial decline in the number of newly reported cases, from 24 to three, also requires cautious interpretation. The data do not establish whether the decline reflects fewer incidents, changes in reporting behavior, different recording practices, or other factors. Public communication about online-fraud risks and accessible reporting arrangements remain relevant, but their impact was not directly evaluated in this study. Future monitoring should separate prevention indicators from performance measures for cases already reported.

Interviewed investigators described coordination with banking institutions and the Bali Police cybercrime unit as useful for locating transaction trails and identifying perpetrators. Such accounts support an explanation of operational practices but should not be treated as proof of improved annual disclosure rates without longitudinal investigation records.

Based on the results of an interview with AKP I Gede Alit Darmana, S.H., M.H as the Head of Criminal Investigation of the Jembrana Police, it was explained that:

"Online fraud cases have different characteristics from ordinary criminal acts because perpetrators often use fake identities and other people's accounts. However, the Jembrana Police Criminal Investigation Unit continues to improve the ability of investigators in digital tracing so that the level of case disclosure increases every year."

The statement illustrates an investigator's perspective on adapting to technological changes in online fraud. Investigators reportedly examine witnesses, analyze digital conversations, trace bank accounts, and coordinate with relevant institutions. These practices may support case handling, but the interview does not independently establish an increase in disclosure effectiveness from one year to the next.

Furthermore, IPDA Gusti Putu Boy Pusuara M., S.H as Kaur Bin Ops stated that:

"The speed of handling reports greatly determines the success of disclosing online fraud cases. The sooner the report is received, the greater the chance of tracking the perpetrator's account and identity."

The results of the interviews show that the time factor is an important aspect in handling cybercrime cases. Many cases experience obstacles because victims report late, making it difficult to trace the traces of transactions and digital communications.

Then, IPDA Alonso Robby Gray Litaay, S.Tr.K as the Head of Idik I explained that:

"In the investigation process, digital evidence is the main factor. Investigators must be able to ensure the authenticity of evidence in the form of screenshots, transfer history, and electronic communications so that they can be used in evidence at trial."

The statement shows that the effectiveness of disclosure of cases does not only depend on the arrest of the perpetrators, but also on the ability of investigators to build a construction of proof based on electronic evidence as stipulated in the Law on Information and Electronic Transactions.

Meanwhile, AIPDA I Dewa Gede Alit Darmika, S.H as a member of the Idik IV Unit said that:

"The obstacles that are often faced are that perpetrators use anonymous accounts and move locations. Therefore, cross-regional cooperation and technological support are needed to speed up the process of identifying perpetrators."

Based on the results of the study, it can be understood that the effectiveness of disclosing online fraud cases at the Jembrana Police has shown quite good development, but it still requires continuous improvement of digital forensic facilities and investigator training.The results of this study are similar to research conducted by Anisa Sahara and Kuswandi (2025) which stated that the development of online fraud is influenced by the increasing use of digital technology and low public cybersecurity literacy. In research at the Jembrana Police Station, it was found that most victims easily trust online transactions without verifying the identity of the perpetrator.

This research is also in line with the research of Gagas Dewanta Aji (2024) regarding the optimization of the performance of the Kudus Police Satreskrim in handling online fraud. The similarity between the two lies in the importance of improving the ability of investigators and coordination with external institutions in increasing crime clearance. The difference is that research at the Jembrana Police focuses more on the effectiveness of the use of digital evidence in the investigation process.Furthermore, research by Adji Rizky Ananda (2020) explained that the main obstacle in handling online fraud is the limitation of cross-regional identification of perpetrators. This was also found in this study, where perpetrators often use fake accounts and identities, making it difficult to track the tracking process.

Research by Diana Berlian Nurjanah and Masrukhin (2026) emphasizes the importance of digital evidence in proving online fraud crimes. The results of the research at the Jembrana Police show suitability because investigators rely heavily on electronic evidence such as transfer history, digital conversations, and social media account data in uncovering cases.Research by Wahyudin et al. (2024) stated that the success of handling online fraud requires cross-institutional coordination. In this study, it was found that the Jembrana Police Criminal Investigation Unit actively coordinates with the Bali Police cyber unit and the banking sector to accelerate the tracking of perpetrators.In addition, research by Yusri Ardiyah Pramesti and Emy Rosnawati (2023) explains that online fraud crimes can be charged using the Criminal Code and the ITE Law. This is relevant to the practice of investigation at the Jembrana Police which uses the provisions of Article 378 of the Criminal Code and the provisions in the ITE Law as the legal basis for handling cases.

Research by Fayza Hafiz Rahmadani et al. (2025) shows that online fraud modes continue to develop through digital communication applications such as WhatsApp. These findings were also found in this study, where most of the public's reports are related to fraud through social media and instant messaging applications.

According to organizational performance theory, the effectiveness of an organization can be measured through the achievement of goals, the efficiency of task implementation, and the organization's ability to adapt to changes in the environment. Based on this theory, the Jembrana Police Criminal Investigation Unit has shown an improvement in performance through an increase in the percentage of online fraud case settlements every year.This increase shows the organization's ability to adapt to the development of cybercrime. In addition, the division of tasks between units and internal coordination that runs well also shows the effectiveness of organizational management in supporting the investigation processHowever, organizational performance theory also emphasizes the importance of supporting human resources and infrastructure. In this study, it was still found that there are limitations in digital forensic facilities and the number of personnel who understand the handling of cybercrime in depth, so that it is a factor that hinders performance optimization.

Law enforcement theory explains that the success of law enforcement is influenced by legal factors, law enforcement officials, facilities and facilities, society, and legal culture. Based on this theory, the effectiveness of the disclosure of online fraud cases at the Jembrana Police is influenced by the professionalism of investigators and adequate legal regulatory support.

The existence of the Electronic Information and Transaction Law provides a legal basis for investigators to use electronic evidence as legitimate evidence. In addition, coordination with external institutions shows the support of an integrated law enforcement system.However, low public awareness in maintaining the security of personal data and delays in reporting are still obstacles in the law enforcement process. This shows that the success of handling cases does not only depend on the police, but is also influenced by public participation.

Cyber crime theory explains that cybercrime is a form of criminality that utilizes information technology as the main means of committing crimes. Online fraud is one of the forms of cybercrime that is growing rapidly due to the ease of internet access and weak digital security of the community.Based on this theory, the characteristics of online fraud in the jurisdiction of the Jembrana Police show a pattern that is in accordance with the concept of modern cybercrime, namely the use of fake identities, anonymous accounts, holding accounts, and digital communications to deceive victims.

In this context, the ability of investigators to understand information technology is an important factor in the effectiveness of case disclosure. Handling cybercrime cannot be done by conventional methods alone, but requires a digital investigation approach and adequate forensic technology support. Therefore, increasing the capacity of investigators in the field of information technology is an important need to support the success of law enforcement against online fraud crimes.

Investigator Professionalism in Case Handling

The professionalism of investigators is one of the important factors in determining the success of handling online fraud crimes. In the context of law enforcement, professionalism is not only related to the technical ability of investigators to conduct investigations, but also

includes integrity, discipline, communication skills, legal understanding, and the ability to follow information technology developments. Handling online fraud cases requires special competence because this crime is carried out through electronic media with a mode that continues to develop and involves the use of digital technology.

Based on the results of research at the Jembrana Police Criminal Investigation Unit, the professionalism of investigators in handling online fraud cases can be seen from the investigator's ability to receive public reports, analyze digital evidence, coordinate across agencies, and systematically compile case files. Investigators are also required to be able to understand the patterns of cybercrime that develop so that the investigation and investigation process can run effectively.In practice, the Jembrana Police Criminal Investigation Unit has made various efforts to improve the professionalism of investigators, including through cybercrime investigation training, internal coaching, and coordination with the Bali Police cyber unit. These efforts are carried out because online fraud crimes have different characteristics from conventional criminal acts so they require information technology-based investigative skills.

Internal records describe cybercrime-related training and technical guidance participation by Criminal Investigation Unit personnel. The figures provide a descriptive measure of recorded participation, not a direct assessment of investigators' professional competence.

Table 1. Investigator Participation in Cybercrime Training, 2022–2024

Year	Number of Investigators at the Criminal Investigation Unit	Investigators Participate in Cybercrime Training	Percentage
2022	24 staff	8 staff	33%
2023	25 staff	13 staff	52%
2024	26 staff	18 staff	69%

Source: Jembrana Police

The personnel records show that cybercrime training participation was reported for 8 of 24 investigators in 2022, 13 of 25 in 2023, and 18 of 26 in 2024. The respective proportions are approximately 33%, 52%, and 69%. The source does not clarify whether the reported totals are unique trained individuals or annual participation events, and it does not report competency-assessment results. These figures therefore demonstrate increased recorded training participation, not independently verified improvement in investigative competence.

Based on the results of an interview with AKP I Gede Alit Darmana, S.H., M.H as the Head of Criminal Investigation of the Jembrana Police, it was explained that:

"The professionalism of investigators is the main factor in handling online fraud cases because this crime develops following technological developments. Therefore, members must continue to improve their digital investigation capabilities and understand the new modes used by perpetrators."

The statement shows that improving the competence of investigators is a necessity that cannot be separated from handling cybercrime. The professionalism of law enforcement officials is an important indicator in maintaining the effectiveness of law enforcement against online fraud crimes.

Furthermore, IPDA Gusti Putu Boy Pusuara M., S.H as Kaur Bin Ops said that:

"In handling online fraud cases, investigators must work quickly, thoroughly, and professionally because digital evidence can change or be lost at any time. Therefore, members are required to have good analytical skills."

From the results of the interview, it can be understood that the professionalism of investigators is not only related to legal knowledge, but also technical ability in maintaining the validity of digital evidence. The accuracy of investigators is an important factor to ensure that electronic evidence can be used in the evidentiary process at trial.

Then, IPDA Alonso Robby Gray Litaay, S.Tr.K as the Head of Idik I explained that:

"Investigators must be able to keep up with technological developments and understand the digital communication patterns of perpetrators. Many cases of online fraud use fake accounts and anonymous identities, requiring more complex investigative capabilities."

The statement shows that the professionalism of investigators in cybercrime cases requires the ability to adapt to information technology developments. Investigators are required to understand digital investigation methods in order to identify perpetrators appropriately.

Meanwhile, AIPDA I Dewa Gede Alit Darmika, S.H as a member of the Idik IV Unit said that:

"In addition to technical skills, investigators must also be able to provide good service to the community. Victims of online fraud often suffer great losses so investigators must provide a humane and professional explanation."

Based on the results of the interview, it can be understood that the professionalism of investigators is also reflected in the quality of service to the community. A humanist approach in the investigation process is an important part of building public trust in the police institution.

In general, the results of the study show that the professionalism of the investigators of the Jembrana Police Criminal Investigation Unit in handling online fraud cases has gone quite well. However, there are still several obstacles such as the limitation of personnel who have special abilities in the field of digital forensics and the limited technological facilities to support cybercrime investigations.The results of this study have similarities with the research of Gagas Dewanta Aji (2024) which explains that the optimization of Satreskrim's performance in handling online fraud is greatly influenced by the quality of human resources and the ability of investigators to conduct digital investigations. In research at the Jembrana Police, it was found that professional improvement is carried out through regular training and technical coaching.

This research is also relevant to the research of Adji Rizky Ananda (2020) who states that the ability of investigators to understand information technology is the main factor in the success of handling online fraud cases. This similarity can be seen from the importance of digital analysis skills in revealing the identity of perpetrators and electronic transaction flows.Furthermore, research by Diana Berlian Nurjanah and Masrukhin (2026) emphasizes that the use of digital evidence requires investigators who have technical competence and a good understanding of the law. This is in accordance with the findings of research at the Jembrana Police where investigators must ensure the validity of electronic evidence so that it can be used in the evidentiary process in court.

Research by Wahyudin et al. (2024) stated that handling online fraud crimes requires more complex coordination and investigative skills than conventional crimes. In this study, it

was also found that Jembrana Police investigators actively coordinate with the Bali Police cyber unit to increase the effectiveness of investigations.In addition, research by Yusri Ardiyah Pramesti and Emy Rosnawati (2023) explains that law enforcement against online fraud requires an understanding of criminal law and information technology law at the same time. This is relevant to the conditions at the Jembrana Police where investigators must understand the application of the Criminal Code and the ITE Law in handling cases.

The research of Fayza Hafiz Rahmadani et al. (2025) also shows that the development of cybercrime modes requires law enforcement officials to continue to improve information technology capabilities. These findings are in accordance with this study where the professionalism of investigators is greatly influenced by the ability to follow the development of increasingly complex digital fraud modes.Meanwhile, research by Anisa Sahara and Kuswandi (2025) explains that cybercrime is growing due to the high use of digital technology and weak public cybersecurity supervision. In research at the Jembrana Police Station, it was found that investigators not only play a role in taking action, but also educate the public as a preventive measure.

From an organizational-performance perspective, greater participation in training suggests that Jembrana Police has allocated attention to cybercrime-related capability development. However, attendance figures alone cannot show improved competence; evaluation would require tests of knowledge, quality of case files, compliance with evidence procedures, and subsequent investigative outcomes. The observed participation data therefore support a cautious claim about training activity rather than verified individual skill gains.

However, organizational performance theory also emphasizes the importance of supporting facilities and infrastructure. In this study, it was still found that the limitations of digital forensic facilities were found that affected the optimization of investigators' performance in uncovering online fraud cases.Law enforcement theory states that the success of law enforcement is influenced by law enforcement officials, legal substance, facilities and facilities, society, and legal culture. In this study, the professionalism of investigators is the main factor in supporting the effectiveness of law enforcement against online fraud crimes.

The ability of investigators to understand electronic evidence and conduct digital investigations shows the quality of law enforcement officials who support the law enforcement process professionally. In addition, the existence of the Electronic Information and Transaction Law provides a clear legal basis for investigators in handling cybercrime cases.However, limited technological facilities and low public awareness of digital security are still obstacles in the law enforcement process. Therefore, increased cooperation between police officers and the public is needed to prevent and uncover online fraud crimes.

Cyber crime theory explains that the development of information technology creates a new form of crime that utilizes electronic media as the main means of committing criminal acts. In the context of this research, the professionalism of investigators is very important because the characteristics of cybercrime are different from conventional crimes.

Online fraud is carried out through digital media using anonymous accounts, fake identities, and electronic communication systems that are difficult to track. Therefore, investigators must have digital investigation skills and an adequate understanding of

information technology.Based on cyber crime theory, improving the competence of investigators is an important step in dealing with the development of increasingly complex cybercrime modes. Handling cybercrime cases requires law enforcement officials who are adaptive to technological developments so that the case disclosure process can run effectively and professionally.

Speed and Accuracy of the Investigation Process

The case-registration and closure figures describe administrative throughput, not the duration of individual investigations. Recorded annual ratios exceeding 100% can arise when earlier cases are closed; they do not justify a claim that every current-year report was resolved or that investigation speed necessarily improved. The source does not provide complete opening-to-closing timestamps, so average case-handling times cannot be calculated reliably. A time-based evaluation should use verified case-level dates and separate inquiry, investigation, file completion, referral, and closure stages.

The administrative records indicate that annual case closures and newly received cases were not identical for every year. In 2022, 19 closures were recorded against 24 new reports (79.17%); in 2023, 24 closures against 20 new reports (120%); in 2024, eight closures against seven new reports (114.29%); and in 2025, three closures against three new reports (100%). A ratio greater than 100% may occur when earlier cases are closed in the reporting year, but the available summary does not identify the source year of each closed case. These figures are consequently not measures of the probability that a new report was resolved within the same year. Likewise, the study does not provide reliable elapsed-time records for calculating average investigation speed. Interview evidence emphasizes timely reporting, lawful collection of electronic evidence, and coordination with banks and the Bali Police cybercrime unit, while also noting delays associated with late victim reports. Evaluating the effectiveness and accuracy of investigation requires case-level records and a clear definition of each stage and outcome.

Interviews with four police officers support these findings. The Head of Criminal Investigation stressed immediate action after a report to prevent perpetrators from erasing traces or moving funds. The Kaur Bin Ops emphasized that electronic evidence must be obtained according to procedure so it is admissible in court. The Head of Idik I highlighted the need for fast coordination with banks, mobile operators, and the Bali Police cyber unit, and a member of Idik IV pointed to late reporting by victims, which often leaves accounts empty or inactive, as a major obstacle.

The author links these results to prior studies (Aji, 2024; Ananda, 2020; Nurjanah & Masrukhin, 2026; Pramesti & Rosnawati, 2023; Rahmadani et al., 2025; Sahara & Kuswandi, 2025; Wahyudin et al., 2024), which similarly find that response speed, inter-agency coordination, proper handling of digital evidence, accurate application of legal articles, and technology-based methods determine success, and that late public reporting hinders it. Under organizational performance theory, the unit shows greater effectiveness through better coordination and responsiveness, though limited digital forensic facilities and slow cross-agency bureaucracy remain constraints. Under law enforcement theory, the investigators' professionalism and inter-agency integration are positive factors, while low public legal awareness is a weakness. Under cybercrime theory, the anonymous and technology-driven

nature of the offense demands faster, more accurate, and more technology-based investigation than conventional crime.

Level of Community Satisfaction with Police Services

The level of public satisfaction with police services is one of the important indicators in assessing the performance of the Jembrana Police Criminal Investigation Unit in handling online fraud crimes. Public satisfaction can be seen from the quality of investigator services, the speed of response to reports, the disclosure of information on case handling, the professional attitude of the apparatus, and the effectiveness of case resolution reported by the public.

In online fraud cases, the public as victims generally suffer material and psychological losses so that fast, clear, and humane police services are an important factor in building public trust in police institutions. Therefore, the Jembrana Police Criminal Investigation Unit seeks to provide responsive services through open receipt of reports, the provision of Notification of Investigation Results Development Letters (SP2HP), and active communication between investigators and victims.Based on the results of the study, most of the people who reported were quite satisfied with the services of the Jembrana Police Criminal Investigation Unit, especially in the aspect of receiving reports and communicating with investigators to victims. However, there are still several complaints related to the length of the perpetrator tracking process and the limited return of victim losses due to the difficulty of tracking the proceeds of crime.

Based on internal survey data, public satisfaction with the services of the Jembrana Police Criminal Investigation Unit in handling online fraud cases obtained the following results:

Table 2. Internal Public Satisfaction Survey for Jembrana Police, 2022–2024

Year	Number of Respondents	Satisfied	Quite satisfied	Dissatisfied
2022	50 respond	29 people	15 people	6 people
2023	65 respond	42 people	17 people	6 people
2024	80 respond	58 people	18 people	4 people

Source: Jembrana Police Criminal Investigation Unit

The internal satisfaction summaries show 29 of 50 respondents satisfied in 2022 (58.0%), 42 of 65 in 2023 (64.6%), and 58 of 80 in 2024 (72.5%). The percentage satisfied increased alongside the number of respondents; however, comparability across years depends on a consistent questionnaire, sampling procedure, and respondent population, none of which are fully documented in the supplied manuscript. The figures should consequently be treated as descriptive, rather than conclusive evidence that service quality improved.

Based on the results of an interview with AKP I Gede Alit Darmana, S.H., M.H as the Head of Criminal Investigation of the Jembrana Police, it was explained that:

"We strive to provide professional and transparent services to the public, especially victims of online fraud. The public must get clear information about the progress of handling the cases they report."

The statement shows that service transparency is an important part in increasing public trust and satisfaction with police institutions.

Furthermore, IPDA Gusti Putu Boy Pusuara M., S.H as Kaur Bin Ops said that:

"Good service is not only related to the settlement of cases, but also how members provide explanations and assistance to victims during the investigation process."

The results of the interviews show that the quality of humanist communication and service is an important factor in building public satisfaction with law enforcement officials.

Then, IPDA Alonso Robby Gray Litaay, S.Tr.K as the Head of Idik I explained that:

"Victims of online fraud generally hope that the lost funds can be returned. But in practice, not all cases can be resolved with a refund of losses because perpetrators often use fake accounts and identities."

The statement shows that the level of community satisfaction is also influenced by the victim's expectations for the final outcome of the case handling. In some cases, the community still feels dissatisfied if the losses experienced cannot be fully recovered.

Meanwhile, AIPDA I Dewa Gede Alit Darmika, S.H as a member of the Idik IV Unit said that:

"We try to provide fast and friendly services to the community so that victims feel cared for. In addition, investigators also provide education so that the public is more careful about online fraud modes."

Based on the results of the interview, it can be understood that police services are not only oriented towards law enforcement, but also on preventive and educational approaches to the community.

In general, the results of the study show that the level of public satisfaction with the services of the Jembrana Police Criminal Investigation Unit in handling online fraud is in the fairly good category. However, there are still several factors that affect public satisfaction, such as the length of the process of tracking perpetrators across regions, the limitation of returning victim losses, and the complexity of the process of proving cybercrime cases.The results of this study have similarities with the research of Gagas Dewanta Aji (2024) which explains that the quality of police services in handling online fraud greatly affects the level of public trust in police institutions. In research at the Jembrana Police, it was found that increased communication and transparency of investigations have an impact on increasing public satisfaction.This research is also relevant to the research of Adji Rizky Ananda (2020) who stated that the public expects the handling of online fraud cases to be carried out quickly and professionally. This similarity can be seen in this study where the victim is very attentive to the initial response of the investigator to the report submitted.

Furthermore, the research of Wahyudin et al. (2024) explained that the effectiveness of police services in cybercrime cases is influenced by the ability of investigators to provide legal certainty to the public. In this study, it was found that the provision of SP2HP and active communication by investigators are factors that increase victim satisfaction.Research by Diana Berlian Nurjanah and Masrukhin (2026) states that the use of appropriate digital evidence can improve the quality of case evidence so that the public has more confidence in the law enforcement process. This is in accordance with the conditions at the Jembrana Police where

the use of electronic evidence helps clarify the investigation process for victims.In addition, the research of Yusri Ardiyah Pramesti and Emy Rosnawati (2023) explains that the handling of online fraud must provide legal protection to victims through professional and transparent services. These findings are relevant to this study where investigators seek to provide an open explanation of the development of the case.

Research by Fayza Hafiz Rahmadani et al. (2025) shows that the increasing mode of cybercrime causes people to need fast and adaptive police services to technological developments. This is in accordance with this study where victims expect a quick response to digital fraud reports.Meanwhile, research by Anisa Sahara and Kuswandi (2025) explains that the low digital literacy of the community causes many victims of online fraud to suffer large losses. In research at the Jembrana Police Station, it was found that investigators not only carry out law enforcement, but also provide education to the public as a form of preventive service.According to the theory of organizational performance, the success of the organization can be measured through the effectiveness of services, the achievement of organizational goals, and the level of community satisfaction with the services provided. Based on this theory, the increasing level of public satisfaction with the services of the Jembrana Police Criminal Investigation Unit shows an improvement in the quality of organizational performance.Responsive services, good communication, and regular provision of information on case developments show that the organization has tried to carry out its public service functions effectively. In addition, the increase in the number of people who are satisfied shows an improvement in the quality of investigation services.However, organizational performance theory also emphasizes the importance of efficiency and service results. In this study, there are still people who are dissatisfied due to the length of the investigation process and the difficulty of recovering losses to victims in online fraud cases.

Law enforcement theory explains that the success of law enforcement is not only determined by the success of punishing the perpetrator, but also by the quality of legal services to the community. In this study, the level of public satisfaction is influenced by the professionalism of investigators, the transparency of the investigation process, and the ability of the authorities to provide legal certainty.The provision of SP2HP, active communication with victims, and humane services show that the law enforcement process has been carried out by paying attention to the rights of the community as victims of criminal acts. In addition, the use of electronic evidence in accordance with procedures also increases public trust in the legal process.However, limitations in tracking crime proceeds and the complexity of cybercrime are still obstacles in providing maximum satisfaction to the community. This shows that the effectiveness of law enforcement is also influenced by technological factors and adequate legal system support.

Cyber crime theory explains that cybercrime has complex characteristics because it is carried out through electronic media and often involves anonymous identities and cross-regional networks. This condition causes the process of disclosing cases to require more complex time and technology than conventional crimes.In this study, it was found that the level of public satisfaction is influenced by the ability of investigators to explain technical obstacles in handling cybercrime to victims. People who understand the complexity of handling online

fraud tend to be more receptive to the investigation process that takes longer.In addition, cyber crime theory also explains that the development of digital fraud modes requires law enforcement officials to continue to improve the quality of information technology-based services. Therefore, improving digital investigation capabilities and public communication services is an important step in increasing public trust in handling online fraud crimes at the Jembrana Police.

his section examines how the Jembrana Police Criminal Investigation Unit (Satreskrim) applies the law to online fraud and what role it plays in cyber law enforcement. In the first part, investigators combine Article 378 of the Criminal Code (fraud) with the Electronic Information and Transaction (ITE) Law (including Articles 28(1), 29, and 45), and rely on Article 5 of the ITE Law, which recognizes electronic information and documents as valid evidence. They also follow the Criminal Procedure Code, for example on detention under Article 21, and National Police Chief regulations and circular letters on cyber cases. The process runs from receiving reports and initial investigation through collecting electronic evidence, examining witnesses and victims, naming suspects, and handing the case to the prosecutor. The case examples, from a Rp 798,999,999 phone fraud to Facebook marketplace fraud involving a car, tiles, and Rp 450,000,000, up to a January 2025 case in Pekutatan worth Rp 149,932,275, all use this same combined legal basis, with stronger digital forensic evidence in the latest case. The text describes the process as structured and transparent, grounded in valid electronic evidence, procedurally correct in detention, and protective of victims.

In the second part, the police are described as having both repressive and preventive roles. They receive reports, investigate, trace digital evidence, coordinate with the Bali Police cyber unit, banks, and telecommunication operators, and educate the public about online fraud modes. Four officers interviewed, namely the Head of Criminal Investigation, the Kaur Bin Ops, the Head of Idik I, and a member of Idik IV, consistently stress the combined use of the Criminal Code and ITE Law, the need for accurate articles and properly obtained evidence, the importance of digital investigation skills against anonymous perpetrators, and the value of public education.

The obstacles identified are the complexity of digital proof, limited digital forensic facilities and uneven technical capability among investigators, perpetrators' use of fake identities and cross-regional networks, fast-changing fraud modes, and low digital literacy among the public. The findings are linked to seven earlier studies (Aji, 2024; Ananda, 2020; Nurjanah & Masrukhin, 2026; Pramesti & Rosnawati, 2023; Rahmadani et al., 2025; Sahara & Kuswandi, 2025; Wahyudin et al., 2024), which support the combined legal basis, the central place of electronic evidence, inter-agency coordination, and public education.

The analysis through three theories reaches a consistent conclusion. Organizational performance theory shows the unit adapting to cybercrime, though facilities and human resources remain limited. Law enforcement theory shows professional conduct by officers and supportive legal substance, while public digital literacy and technological change remain challenges. Cybercrime theory holds that digital, anonymous, and cross-regional crime requires an adaptive legal approach, technology-based investigation, and public awareness efforts. Overall, the section concludes that legal implementation and the police role have gone quite well, but need stronger apparatus capacity, forensic technology, and cross-sector cooperation.

The effectiveness of law enforcement against online fraud perpetrators is a measure of the success of police officers in uncovering, processing, and providing legal certainty for information technology-based crimes. In the context of cybercrime, the effectiveness of law enforcement is not only measured by the number of cases successfully resolved, but also includes the ability of the authorities to identify perpetrators, collect electronic evidence, track digital transactions, and provide a deterrent effect against criminals.

Based on the results of the research, the Jembrana Police Criminal Investigation Unit has sought to increase the effectiveness of law enforcement through strengthening coordination with the Bali Police cyber unit, improving the ability of investigators in digital investigations, and applying a combination of the provisions of the Criminal Code and the Information and Electronic Transactions Law in the investigation process of online fraud cases.In practice, the effectiveness of law enforcement against online fraud perpetrators faces quite complex challenges. Perpetrators often use fake identities, loan accounts, anonymous accounts, and cross-regional digital communication networks to evade legal proceedings. In addition, delays in public reports also affect the success of the authorities in tracking and securing electronic evidence.

Interviews attribute operational improvements to developing digital-investigation skills and interagency coordination. Without case-level comparison records, however, the contribution of these factors to the observed annual closure figures cannot be quantified.

Based on the results of an interview with AKP I Gede Alit Darmana, S.H., M.H as the Head of Criminal Investigation of the Jembrana Police, it was explained that:

"The effectiveness of law enforcement against online fraud is greatly influenced by the speed of handling reports and the ability of investigators to conduct digital tracking. The faster the process is carried out, the greater the chance of disclosure of the perpetrators."

The statement shows that the success of law enforcement in cybercrime cases is greatly influenced by the time factor and information technology capabilities of law enforcement officials.

Furthermore, IPDA Gusti Putu Boy Pusuara M., S.H as Kaur Bin Ops said that:

"In the law enforcement process, investigators must ensure that all electronic evidence is obtained in accordance with procedures so that the case can continue to the trial stage without legal obstacles."

The results of the interviews show that the effectiveness of law enforcement is not only related to the arrest of perpetrators, but also related to the quality of the legal proof process in online fraud cases.

Then, IPDA Alonso Robby Gray Litaay, S.Tr.K as the Head of Idik I explained that:

"The main obstacle in handling online fraud is that perpetrators are often outside the region and use anonymous accounts. Therefore, cross-regional coordination and digital technology support are needed to accelerate the disclosure of cases."

The statement shows that the effectiveness of law enforcement against cybercrime is greatly influenced by the ability to coordinate and use digital investigative technology.

Meanwhile, AIPDA I Dewa Gede Alit Darmika, S.H as a member of the Idik IV Unit said that:

"In addition to law enforcement, we also carry out prevention efforts through socialization to the public so that the number of victims of online fraud can be reduced."

This passage closes the discussion of how effective law enforcement is against online fraud perpetrators at the Jembrana Police. It begins by noting that effectiveness is also shaped by the preventive measures officers take to reduce the chance of crimes occurring. Overall, enforcement has developed quite well, although it is still hampered by limited forensic technology, the complexity of digital proof, and the anonymous, cross-regional nature of cybercrime.

The author ties these findings to seven earlier studies. Aji (2024) found that effectiveness depends on digital investigation skills and inter-agency coordination, and at Jembrana, closer coordination with the Bali Police cyber unit raised the case resolution rate. Ananda (2020) identified fake identities and anonymous accounts as the main obstacle, which matches the difficulty investigators have in tracking perpetrators who often change locations. Nurjanah and Masrukhin (2026) stressed that legally obtained and well-managed electronic evidence determines success. Wahyudin et al. (2024) emphasized cross-institutional cooperation and technological support, seen in the work with banks and cyber units to trace transactions. Pramesti and Rosnawati (2023) argued that applying the Criminal Code and the ITE Law together gives a stronger legal basis, as investigators do with Article 378. Rahmadani et al. (2025) showed that evolving cybercrime modes force officers to keep upgrading their methods, and Sahara and Kuswandi (2025) linked rising cybercrime to technological growth and low public literacy, which is why the police also educate the public.

The analysis then applies three theories. Under organizational performance theory, the higher resolution rate, the success in identifying suspects and reaching the P21 stage (the prosecutor's declaration that the case file is complete), and better coordination show greater effectiveness, though limited forensic facilities and the difficulty of tracking perpetrators across regions still hold it back. Under law enforcement theory, effectiveness rests on investigator professionalism, electronic evidence, and adequate legal rules, with the Criminal Code and ITE Law giving sufficient legal substance, while public factors such as low digital security awareness and late reporting remain obstacles. Under cybercrime theory, the digital, anonymous, and cross-regional character of the offense demands more complex investigation methods than conventional crime, and the unit's digital tracking of identities, transactions, and communications shows the adaptiveness required. The theory also highlights prevention through public awareness, so the police's education and socialization activities are an important part of making enforcement effective.

CONCLUSION

The findings indicated that the Criminal Investigation Unit (Satuan Reserse Kriminal, Satreskrim) of the Jembrana Resort Police handled online fraud cases through complaint registration, preliminary inquiries, criminal investigations, witness examinations, electronic evidence collection, and coordination with relevant institutions. Administrative records covering 2022–2025 revealed that annual case closures occasionally exceeded newly registered reports. However, these figures did not establish cohort-specific case resolution rates or demonstrate improvements in investigative efficiency without supporting case-level records. Interviews highlighted investigators' efforts to preserve digital evidence, trace financial

transactions, coordinate with the cybercrime investigation unit of the Bali Regional Police and financial institutions, and communicate case progress to complainants. Although these practices reflected efforts to strengthen investigative accountability and institutional coordination, their effectiveness could not be conclusively established solely through interview findings and aggregate administrative statistics.

The study identified several challenges affecting online fraud investigations, including inadequate digital forensic facilities, disparities in investigators' specialized competencies, difficulties identifying perpetrators using fraudulent identities or operating across jurisdictions, delayed victim reporting, and obstacles to recovering financial losses. Accordingly, improvements should prioritize competency-based investigator training, standardized documentation of case status and investigation duration, strengthened digital evidence management and interagency coordination procedures, and transparent communication with complainants. Future research should distinguish administrative case closure from evidentiary completeness, prosecution outcomes, and victim restitution while validating public satisfaction findings through transparent and standardized survey procedures. These recommendations provided a foundation for strengthening investigative practices and developing more reliable performance evaluation mechanisms. Nevertheless, the findings were limited to online fraud investigations and could not be generalized to all categories of general criminal offenses handled by the Jembrana Resort Police.

FUNDING

The authors declare that no financial support was received for the conduct of this research and/or the publication of this article.

CONFLICT OF INTEREST

The authors declare that this research was conducted in the absence of any commercial or financial relationships that could be construed as a potential conflict of interest.

AUTHOR CONTRIBUTION

All authors contributed to the preparation and writing of this article.

GENERATIVE ARTIFICIAL INTELLIGENCE USAGE STATEMENT

In the preparation of this manuscript, the authors utilized Artificial Intelligence (AI) solely for the purposes of improving grammar and checking language usage.

REFERENCES

Aji, G. D. (2024). Optimizing the performance of the Kudus Police Satreskrim in handling online fraud to increase crime clearance. *Advances in Police Science Research Journal, 6*(1). https://doi.org/10.70526/apsrj.v6i1.1238

Ananda, A. R. (2020). Upaya penanganan tindak pidana penipuan online oleh Satreskrim Polres Ciamis [Efforts to handle online fraud crimes by the Criminal Investigation Unit of Ciamis Police]. *Advances in Police Science Research Journal, 4*(10).

Ardoni. (2022). Information items used by online fraudsters and their relationship to Indonesian digital literacy. *Berkala Ilmu Perpustakaan dan Informasi, 18*(2), 326–337. https://doi.org/10.22146/bip.v18i2.5866

Creswell, J. W. (2014). *Research design: Qualitative, quantitative, and mixed methods approaches* (4th ed.). SAGE Publications.

Gusdiar, A., Ekawati, & Aminanto, K. (2026). Reconstruction of the integrated online investigation legal policy for online fraud with victims located outside the police jurisdiction area. *Customary Law Journal*, 1–16. https://doi.org/10.47134/jcl.v3i3.2.6312

Haq, M. A., Barthos, M., & Fakrulloh, Z. A. (2023). Digital forensics in online fraud crimes investigation. In *Proceedings of the 3rd International Conference on Law, Social Science, Economics, and Education (ICLSSEE 2023)*. EAI. https://doi.org/10.4108/eai.6-5-2023.2333408

Hariyanto, Y., & Kusumah, H. A. (2026). Kepastian hukum dan efektivitas pembuktian digital dalam penyidikan online fraud: Analisis normatif Pasal 235 KUHAP baru dan implementasinya di Polres Cimahi. *Mahkamah: Jurnal Riset Ilmu Hukum.*

Kolhe, D., & Bhat, A. H. (2024). Crime and fraud at the community level: social networking understanding into economic crimes and psychology motivations. *Journal of Social Sciences and Economics, 3*(2), 109–128.

Kurniawan, R. C. (2025). Enhancing cybercrime response capabilities through integrated digital policing systems. *Jurnal Scientia Indonesia, 9*(2). https://doi.org/10.15294/scientia.v9i2.37964

Lesmana, S. J., Sofia, I., & Felina, F. (2023). Law enforcement in efforts to combat cyber crime in Indonesia building future digital security. *The International Journal of Law Review and State Administration, 2*(6), 120–128. https://doi.org/10.58818/ijlrsa.v1i3.90

Miles, M. B., Huberman, A. M., & Saldaña, J. (2014). *Qualitative data analysis: A methods sourcebook* (3rd ed.). SAGE Publications.

Nurjanah, D. B., & Masrukhin. (2026). Handling online fraud crimes through digital evidence in the Surakarta Police: A positive legal perspective and Islamic law. *Legalite, 11*(1), 36–52. https://doi.org/10.32505/legalite.v11i1.13733

Pramesti, Y. A., & Rosnawati, E. (2023). Fraud crimes in online buying and selling media. *Web of Scientist: International Scientific Research Journal, 4*(2). https://doi.org/10.47134/webofscientist.v2i4.8

Rahmadani, F. H., Sutany, H. C., Aditya, M. R., Fajar, M. A., Dari, Y. U., & Fauziyah. (2025). Cybercrime: Analisis dan mitigasi resiko penipuan tilang online melalui aplikasi WhatsApp (WA). *Jurnal Sistem Informasi Galuh, 3*(1), 23–38. https://doi.org/10.25157/jsig.v3i1.4124

Sahara, A., & Kuswandi, K. (2025). Online fraud as a form of cybercrime in a criminological perspective. *Parlementer: Journal of Legal and Public Administration Studies, 2*(4), 92–105. https://doi.org/10.62383/parlementer.v2i4.1425

Shang, D., Yuan, D., Wu, X., & Li, D. (2025). Can digital transformation alleviate corporate fraud? Evidence from China. *Internet Research, 35*(4), 1554–1583.

Sintasari, D. A., Juita, S. R., & Triwati, A. (2025). Perlindungan hukum bagi korban tindak pidana penipuan (bisnis online) berdasarkan perspektif viktimologi: Studi kasus di Polres Kudus. *Semarang Law Review, 6*(2). https://doi.org/10.26623/slr.v6i2.12524

Siregar, Z. A., Rafiqi, & Sitorus, N. T. (2024). Tinjauan yuridis pembuktian elektronik dalam perkara tindak pidana penipuan online. *Arbiter, 6*(2), 219–231.

Soekanto, S. (2019). *Pengantar penelitian hukum* [Introduction to legal research]. UI Press.

Sugiyono. (2020). *Metode penelitian kuantitatif, kualitatif, dan R&D* [Quantitative, qualitative, and R&D research methods]. Alfabeta.

Sumarna. (2025). The influence of legal literacy and law enforcement effectiveness on cybercrime prevention. *Jurnal Pembaharuan Hukum, 12*(3). https://doi.org/10.26532/jph.v12i3.49118

Wahyudin, J., Renggong, R., & Hamid, A. H. (2024). Analisis tindak pidana penipuan secara online di wilayah Kepolisian Daerah Sulawesi Selatan. *Indonesian Journal of Legality of Law, 6*(2), 273–280. https://doi.org/10.35965/ijlf.v6i2.4474

Wathan, H. (2025). The criminology of cybercrime: A study of online financial fraud and the challenges for Indonesian law enforcement. *Cognitionis Civitatis et Politicae, 2*(3).

Yufriadi, F., Syahriani, F., & Afifi, A. A. (2024). Trade transformation in the digital era: Agency role, opportunities and challenges. *AL-IMAM: Journal on Islamic Studies, Civilization and Learning Societies, 5*(1), 13–23.