

International Journal of Social Sciences and Humanities
Vol. 4 No. 3, October 2026, pages: 2020-2037
e-ISSN: 2985-6469
https://ejournal.45mataram.ac.id/index.php/ijssh

Reconstructing a Transnational Online Scam Network through Digital Forensics: A Case Study of a Freelance Online Job Scam

Irvan Reza [1]*, Suryadi MT [2], Muhammad Erza Aminanto [3]
Corresponding Author's e-mail : irvanreza2005@gmail.com

Article History

Manuscript submitted:
10 Agustus 2026
Manuscript revised:
20 September 2026
Accepted for publication:
19 October 2026

Keywords

Digital Forensics; Network Reconstruction; Freelance Job Scam;

Abstract

Freelance job scams have become a recurring form of online fraud targeting Indonesian citizens, with some operations conducted abroad by workers who were themselves recruited through deception. This article examines how investigators of the Directorate of Cyber Crime, Criminal Investigation Agency, Indonesian National Police, reconstructed a scam network operating from a Middle East country that, according to police statements, defrauded at least 823 Indonesian victims of approximately IDR 59 billion between 2022 and 2024. Using a qualitative single case study, the analysis draws on case documents, digital forensic records, financial tracing, and public statements, mapping digital artefacts onto crime script stages and three investigative paths: follow the technology, follow the money, and follow the people. The findings show that the scheme combined deceptive recruitment and coerced deployment of operators with a staged task scam involving escalating deposits, financial layering, and conversion into Tether. Digital forensics linked pseudonyms, accounts, wallets, locations, and roles, while integrating the three investigative paths enabled 26 police reports to be consolidated into one network case, resulting in seven convictions and international cooperation requests.

Copyright © 2025, The Author(s).
This is an open access article under the BY-NC-ND license

Contents

Abstract 2020
Introduction 2021
Methods 2022
Results and Discussions 2024
Conclusion 2034
Reference 2035

[1] Graduate School of Sustainable Development, Universitas Indonesia, Depok, Indonesia
[2] Department of Mathematics, Universitas Indonesia, Depok, Indonesia
[3] Cyber Security Monash University, Indonesia

Introduction

Indonesia's rapid adoption of digital payments and messaging applications has been accompanied by a substantial increase in online scams. Between 22 November 2024 and 14 January 2026, the Indonesia Anti-Scam Centre received 432,637 complaints, with reported financial losses reaching IDR 9.1 trillion. Job scams were among the frequently reported forms of fraud (Otoritas Jasa Keuangan, 2026). One increasingly concerning form is the freelance online job scam, commonly operated through task-based schemes. Perpetrators initially offer simple online tasks, such as liking social media posts, and provide small commissions to establish credibility. Victims are subsequently persuaded to deposit increasingly larger amounts in exchange for promised commissions that are ultimately withheld (Kipngetich, 2025). This mechanism illustrates how social engineering exploits employment expectations and financial incentives to facilitate fraud.

The problem becomes more complex when these operations cross national borders, involving perpetrators, victims, financial intermediaries, and digital evidence distributed across different jurisdictions. Such arrangements complicate investigations because criminal activities extend beyond the territorial authority of individual law enforcement agencies (Button et al., 2025; Cross, 2020). The United Nations Office on Drugs and Crime (2025) highlights the expansion of organised scam operations into regions beyond East and Southeast Asia and their increasing use of cryptocurrency and underground financial channels. Furthermore, some operations involve human trafficking for forced criminality, in which individuals recruited through fraudulent overseas employment offers are subsequently coerced into conducting online scams. These individuals may simultaneously be victims of exploitation and participants in criminal activities, complicating the assessment of individual responsibility (Office of the United Nations High Commissioner for Human Rights, 2023; Lazarus et al., 2025; Luong, 2025).

Addressing these challenges requires an investigative approach that connects digital evidence, financial transactions, and criminal actors. Digital forensics provides the foundation for identifying, preserving, analysing, and interpreting electronic evidence to support criminal investigations (Casey, 2011). However, increasing data volumes, encryption, anti-forensic techniques, and cross-border evidence distribution present considerable investigative challenges (Casino et al., 2022; Khan et al., 2025). Crime script analysis offers a complementary framework by examining criminal activities as interconnected stages involving actors, resources, and operational processes (Cornish, 1994). Previous studies have applied this approach to transnational computer fraud and phishing networks (Van Nguyen, 2022; Loggen & Leukfeldt, 2022). In cases involving forced criminality, however, examining victim exploitation alone is insufficient because operator recruitment, transportation, and coercive control also form part of the criminal process.

The reconstruction of criminal networks therefore requires the integration of three investigative pathways: following the technology, following the money, and following the people. These approaches examine digital infrastructure, financial transactions, and relationships among individuals to establish connections between otherwise fragmented evidence. Their integration is consistent with research highlighting the significance of social relationships and digital connections in understanding cybercriminal networks (Leukfeldt et al., 2017; Morselli, 2009). Nevertheless, previous research has generally examined digital forensics, crime scripts, forced criminality, and cross-border investigations separately (Casino et al., 2022; Khan et al., 2025; Van Nguyen, 2022; Lazarus et al., 2025; Luong, 2025; Button et al., 2025; Cross, 2020). Limited empirical research has demonstrated how these approaches can be integrated to reconstruct the interconnected processes of operator recruitment,

e-ISSN : 2985-6469

victim exploitation, financial movements, and criminal relationships within an actual transnational scam investigation. This constitutes a research gap, particularly in the Indonesian context.

To address this gap, this study examines a transnational freelance online job scam investigated by the Directorate of Cyber Crime, Criminal Investigation Agency, Indonesian National Police (Dittipidsiber Bareskrim Polri). The criminal network operated from a Middle Eastern country (Country X) and targeted victims in Indonesia, India, Thailand, and China. Police statements indicated that at least 823 Indonesian victims suffered estimated losses of IDR 59 billion between 2022 and 2024, while the reported losses across the four countries reached approximately IDR 1.5 trillion (Modus Sindikat Penipuan Online, 2024; Sindikat Scam Online Tipu 823 WNI, 2024). A significant investigative development was the consolidation of 26 police reports submitted to different police units into a single network case (Direktorat Tindak Pidana Siber, 2025a).

Accordingly, this study addresses three research questions: (1) How was the freelance online job scam structured and operationalised, from the recruitment of Indonesian operators to the extraction and laundering of victims' funds? (2) How did investigators use digital forensic evidence to trace the technological infrastructure, financial flows, and individuals involved? and (3) How did the integration of following the technology, following the money, and following the people support the consolidation of separate police reports into a single network case?

This study aims to reconstruct the operator and victim crime scripts, analyse the application of digital forensic evidence, and explain how the integration of the three investigative pathways supports criminal network reconstruction. Its novelty lies in combining two interconnected crime scripts with three investigative pathways in an empirical investigation of a transnational freelance online job scam. By connecting operator recruitment, coercive deployment, victim exploitation, and financial transactions through digital forensic evidence, this research contributes a more integrated approach to understanding transnational cybercrime. Its findings are expected to support more effective investigations, the identification of criminal network structures, the tracing of illicit proceeds, and international law enforcement cooperation, while recognising the potential victimisation of individuals subjected to forced criminality.

Methods

This study uses a qualitative single case study design (Yin, 2018) to examine a transnational freelance online job scam investigated by the Directorate of Cyber Crime, Criminal Investigation Agency, Indonesian National Police, between June 2023 and January 2025. A single case design is appropriate because the case is revelatory: it provides access to investigative records that are rarely available to researchers, and it allows the investigative process to be examined in full sequence, from the first information to prosecution. The unit of analysis is the investigation, and the embedded units of analysis are the crime script stages and the three investigative paths. The case was selected purposively on four criteria. First, it consolidated 26 police reports filed with different police units into a single network case. Second, it combined online fraud with the trafficking of Indonesian nationals as scam operators. Third, the offenders were based abroad, in Country X, while the Indonesian victims were in Indonesia. Fourth, the proceedings against the seven defendants had been completed and the defendants had been sentenced, so that the analysis does not interfere with a pending trial, although inquiries into network members abroad continue (Direktorat Tindak Pidana Siber, 2025a, 2025b). The study draws on five types of data, summarised in Table 1.

Table 1. Data Source

Source	Content	Use in analysis
Case documents	Police reports, information report, investigation orders, examination records of witnesses and suspects, case chronology, and case file completion letters of the Attorney General's Office; the Directorate's academic manuscript and presentations on the case	Crime script, actor roles, chronology
Digital forensic examination reports	Reports of seven digital evidence examinations (September 2023 to October 2024), including extractions from the devices of four repatriated operators and of the principal organiser; the investigators' link analysis chart	Follow the technology, attribution
Financial tracing records	Lists of 1,121 bank accounts and 748 telephone numbers compiled from the police reports and a victims' association database; account mutation analyses; asset tracing results	Follow the money
Public sources	Official press statements and news reports on the press conference of 16 July 2024 and subsequent arrests; publications of the Financial Services Authority	Verification of figures released to the public; national context

Documentary sources were treated as the primary evidence, prioritising formal case documents when discrepancies occurred. Data analysis involved reconstructing the operator and victim crime scripts based on Cornish (1994), coding digital artefacts by type, source, crime stage, and investigative path, and linking relevant entities through digital evidence, witness statements, or both. The findings were triangulated using case documents, forensic reports, and public statements, followed by data condensation, display, and conclusion verification (Miles et al., 2020). Ethical approval and written access permission were obtained, while identities, locations, and sensitive investigative information were anonymised. Given the first author's involvement in the investigation, potential researcher bias was addressed through documentary verification, transparent reporting of discrepancies, and critical examination of limitations. These limitations include the single-case design, restricted access to foreign-held evidence, unverified financial estimates based on suspect statements, and inconsistencies in reported dates and figures. Accordingly, formal case documents were prioritised, with disputed dates reported by month and varying figures presented as ranges.

e-ISSN : 2985-6469

Results

1. Anatomy of the Freelance Online Job Scam

Following Cornish (1994), the case documents show two linked scripts. The operator script supplied and controlled the workforce, and the victim script extracted and laundered the funds. Table 2 presents both scripts, the digital evidence generated at each stage, and the investigative path through which that evidence was obtained.

Table 2. Crime script of the freelance online job scam: operator script and victim script

Script stage	Offender action	Platform/tool	Digital evidence	Investigative path
A. Operator script: recruitment, placement, and control of operators				
Preparation	Recruiters in Indonesia and Thailand offer office computer jobs in City Y with a promised monthly salary of about IDR 15 million; a domestic placement agency arranges departure and charges fees before departure	Messaging applications; domestic placement agency; visas and air tickets	Recruiter and organiser conversations and fee instructions; passport and visa data of recruits stored on the organiser's smartphone	Money; people
Pre-condition	Operators are housed in rented villas, their passports are withheld, their movement is restricted, and they work twelve-hour shifts without rest days	Rented villas and apartments in City Y, Country X; telephones, computers, and routers supplied by the organiser	Villa rental documents, expense records, and photographs of premises on the organiser's smartphone; statements of repatriated operators	Technology; people
Instrumental	Operators receive work instructions,	Work group chats;	Existing and deleted conversations	Technology;

initiation	pseudonymous accounts, and assignments by target market under foreign supervisors and an Indonesian interpreter	pseudonymous messaging accounts	recovered from the repatriated operators' telephones, showing instructions, team structure, and pseudonyms	people
Exit	Operators attempt to escape the operation, leave the premises, seek assistance from Indonesian diplomatic representatives (KJRI/KBRI), or return to Indonesia through repatriation. Their departure and subsequent reports provide information about the organisation, recruitment methods, operational structure, and identities of the organisers.	Mobile phones; communication with KJRI/KBRI; diplomatic and immigration channels; airline and repatriation arrangements.	Communications with family members and authorities; travel and immigration records; repatriated operators' mobile phones; photographs, location histories, and recovered conversations documenting the operation.	Money; people
B. Victim script: fraud, laundering, and exit				
Preparation	Organisers establish the technical and financial infrastructure required to conduct the fraud, including acquiring telephone	domain registration, source code, server logs, SIM ownership, location history	Telephone number registration and subscriber data; SIM card ownership records; domain registration and hosting	Technology; money; people

e-ISSN : 2985-6469

	numbers for mass recruitment, preparing collection bank accounts, developing or maintaining task websites, and establishing payment gateway services to receive and distribute victims' deposits.		information; website source code and server logs; bank account ownership and mutation records; payment gateway merchant and transaction records.	
Entry	Mass distribution of part-time online job offers to Indonesian telephone numbers	WhatsApp and Telegram accounts	Sender numbers reported by victims (748 numbers across the reports)	Technology
Instrumental initiation	Victims are directed to create accounts and log in to task websites or to join groups controlled by the offenders	Task websites; controlled WhatsApp and Telegram groups	Website links, registration records, and group memberships on victims' devices	Technology
Instrumental actualisation (trust building)	Simple tasks, such as liking or following social media and online shop accounts, rewarded with small commissions	Social media and online shop platforms; small transfers to victims	Task instructions; small incoming transfers recorded in victims' accounts	Technology; money
Doing	Deposits presented as a condition for tasks with larger	Collection bank accounts; payment gateway	Transfer receipts and account mutation records (1,121	Money

	commissions, escalating until withdrawals are refused	services	accounts reported)	
Post-condition	Layering of funds through further accounts and payment gateways, conversion of rupiah into Tether, and distribution of proceeds by commission	Layered accounts; payment gateways; self-custodial wallets on the TRON network	Account mutations; wallet addresses and commission records on the organiser's smartphone; vehicle and villa documents	Money; people
Exit	Offenders cut off communication with victims, abandon or replace accounts and numbers, and delete conversations from devices	Messaging accounts; task websites; work devices	Deleted conversations recovered through forensic extraction; discontinued numbers and accounts	Technology

Note. The investigative path column shows the path through which each type of evidence was obtained, listed in the order technology, money, people. Sources: Direktorat Tindak Pidana Siber (2024, 2025a); Modus Sindikat Penipuan Online (2024); Bareskrim Bongkar Scam Online Jaringan Dubai (2024).

The operator script began in Indonesia, where recruiters offered jobseekers office-based computer work in City Y with a promised monthly salary of approximately IDR 15 million (Modus Sindikat Penipuan Online, 2024). A domestic placement agency arranged their departure and charged recruitment fees. Upon arrival, their passports were confiscated, their movements restricted, and they were forced to operate scam activities for twelve hours daily without rest days. The organiser, a foreign national based in Country X, arranged visas, accommodation, and operational equipment (Direktorat Tindak Pidana Siber, 2024, 2025a). Police also investigated the organiser for trafficking in persons involving Indonesian, Thai, Chinese, and Indian workers. The investigation began following the escape and repatriation of four Indonesian operators in late May 2023.

The victim script involved unsolicited part-time job offers distributed through WhatsApp and Telegram, directing victims to task-related websites. Initially, victims received small commissions for completing simple social media and online shopping tasks. Subsequently, they were required to deposit increasingly larger amounts before their funds became inaccessible and communication

e-ISSN : 2985-6469

ceased (Direktorat Tindak Pidana Siber, 2025a). Between November 2022 and August 2023, 26 police reports were submitted to eleven police units, each holding only part of the criminal pattern. Victims' deposits were transferred through multiple bank accounts and payment gateways before conversion into Tether for overseas transfers. To conceal their activities, offenders deleted conversations and frequently replaced telephone numbers and bank accounts. However, recovered deleted conversations demonstrated that these efforts to eliminate digital traces were incomplete. This final stage reflects the exit phase of crime script analysis, referring to offenders' attempts to withdraw from criminal activities and conceal evidence (Cornish, 1994).

2. Following the Technology: Reconstructing the Digital Infrastructure

The technology investigation began with four repatriated Indonesian operators whose interviews and digital devices provided initial evidence of the scam operation. Following notification from the Indonesian Consulate General in City Y, investigators issued an information report in July 2023 and examined the operators' telephones using commercial mobile forensic extraction software. Recovered deleted conversations revealed work instructions, team structures, and the pseudonyms of supervisors and co-workers, expanding the investigation from trafficking victims to the criminal operation itself (Direktorat Tindak Pidana Siber, 2025a). Investigators subsequently consolidated information from 26 police reports and a database of 823 victims, identifying at least 748 telephone numbers and 1,121 bank accounts associated with the offenders. By matching the operators' accounts and recovered digital evidence with victims' reports, particularly a report submitted to the Criminal Investigation Agency in June 2023, investigators established connections between previously separate cases (Direktorat Tindak Pidana Siber, 2025a).

The investigation expanded following the organiser's transfer to Indonesia in June 2024. A forensic examination of his smartphone in early July revealed messaging groups connecting him with scam groups and network leaders, workers' identity and travel documents, villa rental records, financial records, vehicle ownership documents, and cryptocurrency wallet addresses (Direktorat Tindak Pidana Siber, 2024). Between September 2023 and October 2024, seven formal digital forensic examinations were conducted, each supported by expert statements for the case file (Direktorat Tindak Pidana Siber, 2025a). Attribution was established by combining digital artefacts with suspect and witness statements, while each connection in the investigative link analysis was classified according to its evidentiary source. For example, identifying individuals in group photographs as network leaders relied on the organiser's statement, whereas linking a leader to luxury vehicles was supported by insurance documents recovered from his device (Direktorat Tindak Pidana Siber, 2024).

3. Following the Money: Reconstructing Financial Flows

The financial investigation began by analysing 1,121 bank account numbers reported by victims to identify frequently recurring first-layer collection accounts. Examination of account transactions revealed successive transfers and fund splitting, indicating layering intended to obscure the origin of illicit proceeds (Direktorat Tindak Pidana Siber, 2025a). In collaboration with the Financial Transaction Reports and Analysis Centre, investigators organised financial entities using the FollowTheMoney data model (Direktorat Tindak Pidana Siber, 2025b). Two cash-out methods were identified: the use of payment gateway services as financial intermediaries and the conversion of rupiah into Tether for overseas transfers. Cryptocurrency wallet addresses linked to the organiser, a group manager, and a financial leader were recovered from the organiser's device, although asset

recovery remained dependent on cooperation with foreign authorities and service providers (Direktorat Tindak Pidana Siber, 2024; Financial Action Task Force, 2021).

Financial tracing also revealed the network's revenue-sharing structure. According to the organiser's statement, leaders received commissions ranging from 15 to 50 per cent of monthly operational revenue, while the organiser received 10 per cent from groups supplied with workers. Reported monthly revenues varied considerably across target markets, although these estimates remain independently unverified (Direktorat Tindak Pidana Siber, 2024). Asset tracing identified two villas and seven vehicles in Country X associated with the organiser and network leaders, including vehicles registered or insured under other individuals' names, suggesting the use of nominees (Direktorat Tindak Pidana Siber, 2024, 2025a). In Indonesia, assets worth approximately IDR 2.73 billion were recovered, whereas assets in Country X remained subject to mutual legal assistance when the case documents were prepared.

4. Following the People: Reconstructing Actor Relationships

The people path reconstructed a network comprising at least seven operational roles (Figure 2). Foreign national leaders controlled the scam operations and received the largest share of revenue, with five senior figures, including four leaders and one supervisor, listed as subjects of INTERPOL Red Notices. The organiser recruited workers, arranged accommodation, equipment, and visas, and managed a separate group targeting Chinese victims. Other members included group managers, an Indonesian interpreter and supervisor, and recruiters in Indonesia and Thailand. The case documents identified at least 17 Indonesian and 10 Thai operators (Direktorat Tindak Pidana Siber, 2025b). Investigators traced domestic members through call detail records and International Mobile Equipment Identity (IMEI) data, locating them in West Java. The interpreter and supervisor was arrested in August 2023, followed by the domestic recruiter in July 2024 (Direktorat Tindak Pidana Siber, 2025a; Sindikat Scam Online Tipu 823 WNI, 2024). The Indonesian operators had different legal statuses: four repatriated operators were treated as trafficking victims and witnesses, while four others who returned between June and October 2024 were prosecuted for fraud, and another remained subject to a Red Notice. One prosecuted operator had worked in the operation for approximately three months (Direktorat Tindak Pidana Siber, 2025b; Tribratanews Polda Lampung, 2024). However, the reviewed documents do not specify the criteria used to distinguish victims from offenders, an issue examined in Section 5.3.

International cooperation extended the investigation to Country X. In November 2023, a Directorate team met local authorities, who agreed to establish a joint team subject to an INTERPOL Red Notice and an Indonesian arrest warrant. The visit also enabled investigators to verify residential and operational locations identified through digital evidence (Direktorat Tindak Pidana Siber, 2025a). A Red Notice for one operator became effective on 23 November 2023 (Tribratanews Polda Lampung, 2024). The organiser was transferred to Indonesia in late June 2024 through a process described in the case documents as extradition, while four Indonesian operators returned between June and October 2024 (Direktorat Tindak Pidana Siber, 2025a). Extradition involves the formal surrender of an individual by one state to another for prosecution or enforcement of a sentence, distinguishing it from deportation, which is primarily an immigration measure. Further coordination took place in December 2024, when the Head of the International Relations Division of the Indonesian National Police met authorities in Country X to discuss Red Notices for the remaining leaders (Direktorat Tindak Pidana Siber, 2025b).

e-ISSN : 2985-6469

The case files of all seven defendants, namely the organiser, the interpreter and supervisor, the domestic recruiter, and four operators, were declared complete by the Attorney General's Office between December 2023 and January 2025. The defendants received prison sentences ranging from two to thirteen years, with the longest sentence imposed on the organiser (Direktorat Tindak Pidana Siber, 2025a, 2025b).

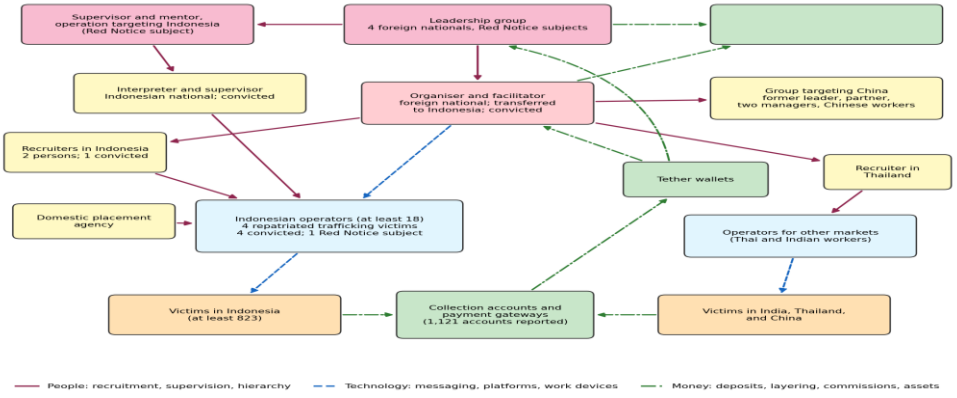


Figure 2. Anonymised networkscam operation by role. Boxes represent roles or groups, not individuals; line styles indicate the investigative path through which each link was established. Source: compiled from Direktorat Tindak Pidana Siber (2024, 2025a, 2025b)

5. Integrating the Three Paths: Network Reconstruction

The three paths became effective when their results were linked. Table 3 shows the cross-path links that allowed separate police reports to be consolidated into one case and that connected the operators, the organiser, and the leaders to the proceeds.

Table 3. Cross-path links used to consolidate police reports

Link type	Evidence	Entities connected	Effect on case
Technology–technology	Sender numbers, messaging groups, and task-website links recurring in victims' reports and matching the modus operandi documented on the repatriated operators' devices	Separate police reports and the shared messaging and platform infrastructure	Reports held by eleven police units recognised as parts of one scheme
Technology–money	Collection account numbers in task instructions and chats; first-layer accounts recurring in victims' transfer receipts;	Messaging and platform accounts, collection accounts, and wallets	Reports linked through common accounts; basis for money laundering analysis

	wallet addresses on the organiser's device		
Technology–people	Recovered conversations and pseudonyms; passport, visa, and photograph data; call detail records and handset identifiers	Pseudonymous accounts and devices, and the recruiters, supervisors, operators, and leaders who used them	Arrests of domestic members; Red Notice requests; attribution of roles for prosecution
Money–people	Commission statements, expense records, vehicle and villa documents, nominee registrations	Proceeds and assets, and the leaders, the organiser, and the managers	Attribution of proceeds; asset tracing; mutual legal assistance requests

Three patterns emerge from this integration. First, consolidation depended on identifiers that recurred across reports, above all first-layer collection accounts and messaging accounts; without them, the reports would have remained separate local fraud cases. Second, the statements and devices of the repatriated operators connected the victim script to the operator script, which allowed the fraud and the trafficking to be investigated as one enterprise. Third, the organiser's device linked the operational level to the leadership and to the assets, which supported money laundering charges and requests for mutual legal assistance. Table 4 summarises how these steps unfolded over twenty months.

Table 4. Key investigative milestones, May 2023 to January 2025

Period	Milestone	Main path or stage
Late May to June 2023	Four operators escape from the workplace and are repatriated; the Consulate General of the Republic of Indonesia in City Y notifies the Indonesian authorities	People
July 2023	Interviews with the repatriated operators and forensic extraction of their devices; information report issued; triage of 26 police reports and a database of 823 victims	Technology; money; people
August 2023	First investigation orders; coordination with the Division of International Relations on Red Notices; arrest of the interpreter and supervisor	People

e-ISSN : 2985-6469

September 2023 to October 2024	Seven formal digital evidence examinations with expert statements	Technology
November 2023	Mission to Country X; Red Notice and arrest warrant identified as prerequisites; Red Notice for one operator in effect	People
December 2023	First case file declared complete by the Attorney General's Office	Prosecution
June to July 2024	Transfer of the organiser to Indonesia; arrest of one operator and of the domestic recruiter; examination of the organiser's smartphone; press conference; return and arrest of a second operator	People; technology
September to October 2024	Return and arrest of two further operators; case files of the organiser, the recruiter, and two operators declared complete	People; prosecution
November to December 2024	Case file of a third operator declared complete; meetings in Country X on Red Notices for the remaining leaders	Prosecution; people
January 2025	Case file of the last operator declared complete and the defendant handed over to prosecutors	Prosecution

6. Discussion

a. Comparison with Prior Studies

The findings confirm and extend earlier crime script research. Like the transnational computer fraud examined by Van Nguyen (2022), the scheme examined divided work between foreign organisers and local participants and relied on technology to reach victims without direct contact. Like the phishing networks analysed by Loggen and Leukfeldt (2022), it depended on a supply of bank accounts through which proceeds could be moved. The case differs, however, in that the fraud script depended on a preceding operator script. The recruitment, transport, confinement, and supervision of workers were preconditions of the fraud, not separate crimes that happened to occur alongside it. A crime script that begins with the first message to a victim would omit the stages at which the operation was most exposed to detection: the recruitment of workers in their home communities and their escape.

The operator script closely matches the pattern described in survivor research. The promise of a well-paid office job, pre-departure fees, the confiscation of passports, long working hours, and escape correspond to the themes identified by Lazarus et al. (2025) in Cambodia and to the recruitment pattern described by Luong (2025). The case shows that this model is not confined to Southeast Asia: it operated in Country X with a multinational workforce, consistent with the

geographic expansion reported by the United Nations Office on Drugs and Crime (2025). It also shows that the escape of trafficked workers can become the starting point of a criminal investigation, a function that survivor-based studies record but do not analyse.

With regard to policing, Button et al. (2025) and Cross (2020) describe cross-border fraud as an area in which victims' countries rarely take effective action against offenders abroad. This case provides a counter-example: the victims' country secured the transfer of the organiser and the return of several operators. At the same time, it confirms their diagnosis, because every step abroad depended on the legal prerequisites and the cooperation of the host state, and the leadership group remained out of reach. Consistent with Leukfeldt et al. (2017), the network combined offline social ties, through which recruiters found workers in their home communities, with digital ties, through which operators and supervisors coordinated their work.

b. From Case-Based to Network-Based Investigation

The central implication is a shift from handling single reports to consolidating reports through shared digital links. In a case-based approach, each of the eleven police units would have investigated a local fraud committed by an unknown offender abroad. In the network-based approach, the recurring identifiers were treated as evidence of one enterprise, and investigative resources were directed at the points that connected many reports: the first-layer collection accounts, the organiser's device, and the recruiters.

Four practices from the case have analytical relevance for comparable investigations. First, repatriation should be treated as an investigative trigger. The Directorate has since issued a standard operating procedure, dated July 2025, for handling repatriated Indonesian nationals and migrant workers, and has developed a data system for recording returnees (Direktorat Tindak Pidana Siber, 2025b). Second, identifiers from all related reports should be collected in a single database and resolved into entities with a common data model before investigative priorities are set. Third, the evidentiary source of each link should be recorded, so that investigative leads are not treated as proven facts. Fourth, investigation teams should be organised by path, with a coordinating management group and dedicated capacity for interpretation and international cooperation; the case team was organised in seven working groups on this basis (Direktorat Tindak Pidana Siber, 2025b). The Directorate reported applying the same three-path framework in 2025 to a fraudulent online marketplace and investment scheme operated from Cambodia (Direktorat Tindak Pidana Siber, 2025b). The national reporting infrastructure has also changed since the investigation. The Indonesia Anti-Scam Centre, which began operating in November 2024, receives scam reports from victims and from financial service providers and coordinates the blocking of accounts used by offenders (Otoritas Jasa Keuangan, 2026). Linking such data to police investigations would allow the consolidation that was achieved manually in this case to begin at the reporting stage.

c. Legal and Operational Constraints

The charges combined provisions of the Electronic Information and Transactions Law, the fraud provision of the Criminal Code, the Law on the Eradication of the Criminal Act of Trafficking in Persons, and the Law on the Protection of Indonesian Migrant Workers (Bareskrim Bongkar Scam Online Jaringan Dubai, 2024), together with money laundering provisions under Law No. 8 of 2010. Electronic evidence was admissible under Article 5 of the Electronic Information and Transactions Law (Law No. 11 of 2008, as amended by Law No. 19 of 2016 and Law No. 1 of 2024), which treats electronic information, electronic documents, and their printouts as an extension of the evidence recognised in procedural law. Because the investigation took place between 2023 and 2025, it was governed by the Criminal Procedure Code in Law No. 8 of 1981; the new Criminal Procedure

e-ISSN : 2985-6469

Code in Law No. 20 of 2025 took effect on 2 January 2026 and governs later cases. Under both codes, the value of digital evidence depends on documented acquisition, preservation, and examination, which in this case was provided by formal examination orders and expert statements for each device.

Cross-border action relied on three channels: police-to-police cooperation through the Division of International Relations and INTERPOL, extradition, and mutual legal assistance. The legal bases were Law No. 1 of 1979 on Extradition, the extradition treaty between Indonesia and Country X signed in 2014 and Law No. 1 of 2006 on Mutual Legal Assistance in Criminal Matters. The main operational lesson concerns timing. The host authorities would not act without a Red Notice and an arrest warrant, and the case documents describe about a year of coordination before the Red Notices and the transfers were achieved (Direktorat Tindak Pidana Siber, 2025a). Preparing these documents at the start of an investigation with foreign suspects would shorten this interval. Assets located abroad and cryptocurrency held in self-custodial wallets remain difficult to recover even after they have been traced.

The treatment of forced operators raises the most difficult question. Article 18 of Law No. 21 of 2007 provides that victims who commit criminal acts because they were forced to do so by traffickers are not punished, and the Office of the United Nations High Commissioner for Human Rights (2023) recommends that people found in scam operations be screened for indicators of trafficking before decisions on prosecution are made. In this case, the operators who escaped and reported were treated as victims, while operators who returned later were prosecuted. The distinction may reflect real differences in their freedom to leave and in their participation, but the documents do not record the screening that was applied. A documented screening procedure at the point of repatriation or arrest, covering recruitment, fees, the confiscation of documents, restrictions on movement, and the possibility of leaving, would protect victims, strengthen the prosecution of those who participated voluntarily, and avoid discouraging future escapees from reporting.

Conclusion

This study concludes that the transnational freelance online job scam operated through two interconnected crime scripts: the recruitment and coercion of foreign workers as scam operators, and the systematic exploitation of victims through task-based online fraud and layered financial transactions. Digital forensic evidence enabled investigators to reconstruct these operations by connecting recovered communications, telephone numbers, bank accounts, financial transactions, individuals, and assets. Integrating the technology, money, and people pathways transformed fragmented information from 26 police reports across eleven police units into a consolidated criminal network investigation. This integration supported the identification of operational structures, financial flows, domestic participants, and overseas leadership, ultimately contributing to seven convictions. These findings demonstrate that combining digital forensic analysis with crime script reconstruction and cross-path investigative linkages provides a practical framework for investigating complex transnational scams.

Future investigations should prioritise the consolidation of identifiers across related reports, document the evidentiary basis of every investigative link, initiate international cooperation at an early stage, and assess potential trafficking victimisation before making charging decisions against recruited operators. Law enforcement agencies and policymakers should strengthen inter-agency coordination, digital forensic capabilities, financial intelligence exchange, and mutual legal assistance mechanisms to address the cross-border nature of these crimes. Further research should compare scam investigations

across different geographical regions to examine the applicability of the two-script framework, employ quantitative network analysis to assess the contribution of shared identifiers to case consolidation, and conduct trauma-informed research with repatriated workers to develop more reliable indicators distinguishing forced criminal participation from voluntary involvement. These efforts could strengthen both investigative effectiveness and the protection of individuals exploited through forced criminality.

Acknowledgements

The authors would like to express their gratitude to the Directorate of Cyber Crime, Criminal Investigation Agency of the Indonesian National Police (Dittipidsiber Bareskrim Polri), for granting access to the investigative documents and providing the institutional support necessary for this research. The authors also acknowledge the contributions of the investigators and relevant parties whose cooperation facilitated the completion of this study.

References

Bareskrim bongkar scam online jaringan Dubai, kerugian capai Rp 59 M. (2024, July 16). kumparanNEWS. https://kumparan.com/kumparannews/bareskrim-bongkar-scam-online-jaringan-dubai-kerugian-capai-rp-59-m-238lZ6f59EI

Button, M., Hock, B., Suh, J. B., & Koh, C. S. (2025). Policing cross-border fraud 'Above and below the surface': Mapping actions and developing a more effective global response. Crime, Law and Social Change, 83, Article 5. https://doi.org/10.1007/s10611-024-10186-2

Casey, E. (2011). Digital evidence and computer crime: Forensic science, computers and the Internet (3rd ed.). Academic Press.

Casino, F., Dasaklis, T. K., Spathoulas, G., Anagnostopoulos, M., Ghosal, A., Böröcz, I., Solanas, A., Conti, M., & Patsakis, C. (2022). Research trends, challenges, and emerging topics in digital forensics: A review of reviews. IEEE Access, 10, 25464–25493. https://doi.org/10.1109/access.2022.3154059

Cornish, D. B. (1994). The procedural analysis of offending and its relevance for situational prevention. In R. V. Clarke (Ed.), Crime prevention studies (Vol. 3, pp. 151–196). Criminal Justice Press.

Cross, C. (2020). 'Oh we can't actually do anything about that': The problematic nature of jurisdiction for online fraud victims. Criminology & Criminal Justice, 20(3), 358–375. https://doi.org/10.1177/1748895819835910

Direktorat Tindak Pidana Siber. (2024). [Pembaruan penyidikan terhadap tersangka utama berdasarkan barang bukti digital dan berita acara pemeriksaan] [Investigation update on the principal suspect based on digital evidence and examination records] [Unpublished link analysis chart]. Badan Reserse Kriminal Kepolisian Negara Republik Indonesia.

Direktorat Tindak Pidana Siber. (2025a). Naskah akademik tentang pengungkapan kasus transnasional dan organized crime sindikat penipuan online, money laundry dan TPPO modus lowongan kerja palsu di Dubai, UEA [Academic manuscript on the disclosure of a transnational organised crime case involving an online fraud, money laundering, and trafficking syndicate using fake job vacancies in Dubai, United Arab Emirates] [Unpublished internal document]. Badan Reserse Kriminal Kepolisian Negara Republik Indonesia.

Direktorat Tindak Pidana Siber. (2025b). Pengungkapan kasus transnasional dan organized crime sindikat penipuan online, money laundry dan TPPO modus lowongan kerja palsu di Dubai,

e-ISSN : 2985-6469

UEA [Disclosure of a transnational organised crime case involving an online fraud, money laundering, and trafficking syndicate using fake job vacancies in Dubai, United Arab Emirates] [Unpublished presentation slides, updated 27 August 2025]. Badan Reserse Kriminal Kepolisian Negara Republik Indonesia.

Dwyer, S. C., & Buckle, J. L. (2009). The space between: On being an insider-outsider in qualitative research. International Journal of Qualitative Methods, 8(1), 54–63.

Financial Action Task Force. (2021). Updated guidance for a risk-based approach to virtual assets and virtual asset service providers.

FollowTheMoney. (n.d.). FollowTheMoney (FtM). Retrieved September 24, 2026, from https://followthemoney.tech/

Kerugian penipuan online sentuh Rp 16.495 triliun. (2024, July 16). Liputan6. https://www.liputan6.com/bisnis/read/5645415/kerugian-penipuan-online-sentuh-rp-16495-triliun

Khan, H. S., Atif, S. M., & Mustufa, A. (2025). Digital forensics in action: The role of digital forensics in cybercrime investigations: A comprehensive study of tools, processes, and legal aspects. NUML International Journal of Engineering and Computing, 3(2). https://doi.org/10.52015/nijec.v3i2.85

Kipngetich, A. (2025). A review of online scams and financial frauds in the digital age. GSC Advanced Research and Reviews, 22(1), 302–329. https://doi.org/10.30574/gscarr.2025.22.1.0025

Lazarus, S., Chiang, M., & Button, M. (2025). Assessing human trafficking and cybercrime intersections through survivor narratives. Deviant Behavior. Advance online publication. https://doi.org/10.1080/01639625.2025.2470402

Leukfeldt, E. R., Kleemans, E. R., & Stol, W. P. (2017). Cybercriminal networks, social ties and online forums: Social ties versus digital ties within phishing and malware networks. The British Journal of Criminology, 57(3), 704–722.

Levi, M., & Reuter, P. (2006). Money laundering. Crime and Justice, 34(1), 289–375.

Loggen, J., & Leukfeldt, R. (2022). Unraveling the crime scripts of phishing networks: An analysis of 45 court cases in the Netherlands. Trends in Organized Crime, 25(2), 205–225.

Luong, H. T. (2025). "Simple job, high salary": Unveiling the complexity of scam-forced criminality in Southeast Asia. Humanities & Social Sciences Communications, 12, Article 1305. https://doi.org/10.1057/s41599-025-05605-1

Luong, H. T., & Ngo, H. M. (2024). Understanding the nature of the transnational scam-related fraud: Challenges and solutions from Vietnam's perspective. Laws, 13(6), Article 70. https://doi.org/10.3390/laws13060070

Miles, M. B., Huberman, A. M., & Saldaña, J. (2020). Qualitative data analysis: A methods sourcebook (4th ed.). SAGE.

Modus sindikat penipuan online, tawari kerja paruh waktu, total kerugian di 4 negara Rp1,5 T. (2024, July 16). Tribunnews. https://www.tribunnews.com/nasional/2024/07/16/modus-sindikat-penipuan-online-tawari-kerja-paruh-waktu-total-kerugian-di-4-negara-rp15-t

Morselli, C. (2009). Inside criminal networks. Springer.

Moyo, T. J., Gunes, O., & Jirotka, M. D. (2025). Investigating human trafficking recruitment online: A study of fraudulent job offers on social media platforms. Proceedings of the ACM on Human-Computer Interaction, 9(2), Article CSCW118, 1–31. https://doi.org/10.1145/3711016

Office of the United Nations High Commissioner for Human Rights. (2023). Online scam operations and trafficking into forced criminality in Southeast Asia: Recommendations for a human rights

response. https://bangkok.ohchr.org/wp-content/uploads/2023/08/ONLINE-SCAM-OPERATIONS-2582023.pdf

Otoritas Jasa Keuangan. (2026, January 21). Indonesia Anti-Scam Centre berhasil kembalikan Rp161 miliar dana masyarakat korban scam [Press release]. https://ojk.go.id/id/berita-dan-kegiatan/siaran-pers/Pages/IASC-Berhasil-Kembalikan-Rp161-Miliar-Dana-Masyarakat-Korban-Scam.aspx

Sindikat scam online tipu 823 WNI, modus tawari korban kerja di Dubai. (2024, July 16). detikNews. https://news.detik.com/berita/d-7441517/sindikat-scam-online-tipu-823-wni-modus-tawari-korban-kerja-di-dubai

Sparrow, M. K. (1991). The application of network analysis to criminal intelligence: An assessment of the prospects. Social Networks, 13(3), 251–274.

Tribratanews Polda Lampung. (2024, July 21). Polri tangkap tersangka scam online internasional, kerugian korban Rp 1,5 triliun. https://www.tribratanews.lampung.polri.go.id/detail-post/polri-tangkap-tersangka-scam-online-internasional-kerugian-korban-rp-1-5-triliun

United Nations Office on Drugs and Crime. (2025). Inflection point: Global implications of scam centres, underground banking and illicit online marketplaces in Southeast Asia. https://www.unodc.org/roseap/uploads/documents/Publications/2025/Inflection_Point_2025.pdf

Van Nguyen, T. (2022). The modus operandi of transnational computer fraud: A crime script analysis in Vietnam. Trends in Organized Crime, 25, 226–247. https://doi.org/10.1007/s12117-021-09422-1

Yin, R. K. (2018). Case study research and applications: Design and methods (6th ed.). SAGE.

Zimmerman, C., & Watts, C. (2003). WHO ethical and safety recommendations for interviewing trafficked women. World Health Organization.

Law of the Republic of Indonesia No. 1 of 1979 on Extradition.

Law of the Republic of Indonesia No. 8 of 1981 on Criminal Procedure Law.

Law of the Republic of Indonesia No. 1 of 2006 on Mutual Legal Assistance in Criminal Matters.

Law of the Republic of Indonesia No. 21 of 2007 on the Eradication of the Criminal Act of Trafficking in Persons.

Law of the Republic of Indonesia No. 11 of 2008 on Electronic Information and Transactions.

Law of the Republic of Indonesia No. 8 of 2010 on the Prevention and Eradication of the Crime of Money Laundering.

Law of the Republic of Indonesia No. 19 of 2016 on the Amendment to Law No. 11 of 2008 on Electronic Information and Transactions.

Law of the Republic of Indonesia No. 18 of 2017 on the Protection of Indonesian Migrant Workers.

Law of the Republic of Indonesia No. 1 of 2024 on the Second Amendment to Law No. 11 of 2008 on Electronic Information and Transactions.

Law of the Republic of Indonesia No. 20 of 2025 on the Criminal Procedure Code..