COSTING: Journal of Economic, Business and Accounting
Volume 7 Nomor 5, Tahun 2024
e-ISSN : 2597-5234

PHISHING CASE DISCLOSURE STRATEGY: A CASE STUDY IN INDONESIA

STRATEGI PENGUNGKAPAN KASUS PHISHING: STUDI KASUS DI INDONESIA

Maharlina Darni Purwandari[1], Andi Urfia Awaliah[2], Bachrudin K. Una[3], Hendi Yogi Prabowo[4]
Fakultas Bisnis dan Ekonomika, Universitas Islam Indonesia, Indonesia[1,4]
Fakultas Ekonomi, Universitas Teknologi Sulawesi, Indonesia[2]
Fakultas Ilmu Sosial, Universitas Muhammadiyah Gorontalo, Indonesia[3]
maharlina.darnip@gmail.com[1], auawaliah@gmail.com[2], hendi.prabowo@uii.ac.id[3], bachrudinuna@umgo.ac.id[4]

ABSTRACT

Phishing is a case of cybercrime that attacks victims when accessing social media or online applications. Phishing perpetrators are able to manipulate identities, making it difficult for victims and the police to detect them. This research aims to analyze the role of the Yogyakarta Special Region Police (DIY) in uncovering phishing cases. Using a case study method with a qualitative approach, data collected from informants was then grouped, decoded, and the results were presented using the help of NVivo 12 plus software. The results of the research found three stages in uncovering a phishing case: First, the victim submits a complaint report to the Yogyakarta Regional Police's Integrated Police Service Center (SPKT) and communicates the incident with Cyber Sub-Directorate V. Second, if the victim's report meets criminal elements then at the investigation level the evidence is disbursed. Third, the evidence is met and transferred to the investigation stage, then the profile of the perpetrator is analyzed, traced, arrested, detained, searched, confiscated and the entire results of the investigation are transferred to the Public Prosecutor for prosecution in court. The role of the DIY Regional Police in uncovering this phishing case can increase public literacy to be more careful when surfing in cyberspace, because the risk of phishing can occur anytime, anywhere, and anyone has the potential to become a victim of cybercrime.
Keywords: *Phishing Cases, Cybercrime, Role of the DIY Regional Police*

ABSTRAK

Phishing merupakan salah satu kasus dalam cybercrime yang menyerang korban saat mengakses media social ataupun aplikasi online. Pelaku phishing mampu memanipulasi identitias yang menyebabkan sulit dideteksi oleh korban maupun kepolisian. Penelitian ini bertujuan untuk menganalisis peran Polda Daerah Istimewa Yogyakarta (DIY) dalam mengungkap kasus phishing. Menggunakan metode studi kasus dengan pendekatan kualitatif, data yang dikumpulkan dari informan kemudian dikelompokan, decoding, dan disajikan hasilnya menggunakan bantuan software NVivo 12 plus. Hasil penelitian menemukan tiga tahapan pengungakapan kasus phising: Pertama, korban mengajukan laporan pengaduan ke Sentra Pelayanan Kepolisian Terpadu (SPKT) Polda DIY dan mengkomunikasikan kejadikan dengan Siber Subdit V. Kedua, laporan korban jika memenuhi unsur pidana maka ditingkat penyelidikan dilakukan pencairan bukti. Ketiga, bukti terpenuhi dan dilihpahkan ke tahap penyidikan, maka profil pelaku dianalisis, dilacak, ditangkap, ditahan, digeledah, dilakukan penyitaan dan keseluruhan hasil pemeriksaan dilimpahkan berkasnya ke Jaksa Penuntut Umum untuk penuntutan di pengadilan. Peran Polda DIY dalam mengungkap kasus phishing ini dapat menambah literasi masyarakat untuk lebih berhati-hati ketika berselancar di dunia maya, karena resiko phishing dapat terjadi kapan saja, dimana saja, dan siapa saja berpotensi menjadi korban cybercrime.
Kata kunci: Kasus Phishing, Cybercrime, Peran Polda DIY

PENDAHULUAN

Perkembangan teknologi adalah hal yang tidak dapat dihindari. Jika suatu negara enggan untuk maju dalam teknologi, mereka berisiko tertinggal dari negara lain. Perkembangan teknologi telah mengubah banyak aspek kehidupan sehari-hari di masyarakat. Mulai dari cara berinteraksi sosial hingga cara berpikir, semuanya mengalami perubahan karena kemajuan teknologi.

Dampak dari perkembangan teknologi adalah munculnya fenomena globalisasi. Globalisasi adalah saat masyarakat dari berbagai wilayah di dunia terasa menyatu karena teknologi yang memudahkan keterhubungan. Melalui globalisasi, interaksi antar masyarakat dari belahan dunia berbeda dapat dilakukan dengan cepat tanpa kendala geografis yang signifikan (Septiano & Najicha, 2022).

Dengan semakin terbuka dan terhubungnya masyarakat global akibat perkembangan teknologi, terutama dalam menghadirkan keragaman dari berbagai belahan dunia, telah memberikan dampak signifikan pada perkembangan media sosial. Media sosial, yang menjadi salah satu hasil evolusi teknologi, menjadi *platform* yang memungkinkan interaksi yang cepat dan tanpa batas geografis bagi masyarakat dari berbagai latar belakang.

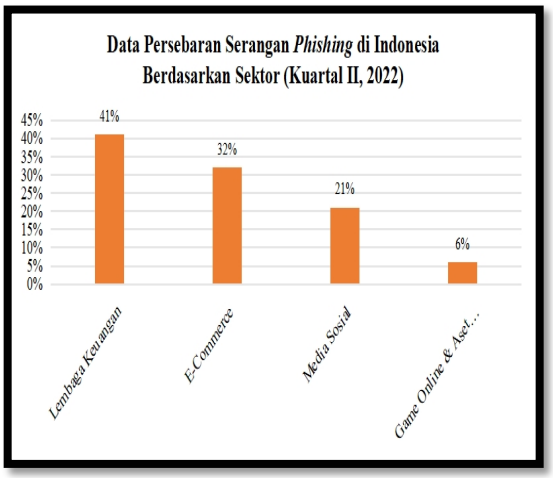
Keberadaan dunia maya menciptakan tren perkembangan teknologi global yang menggambarkan kreativitas manusia. Kehadiran internet juga memberikan kemudahan bagi individu untuk mengakses informasi dan berinteraksi di media sosial tanpa perlu pertemuan langsung. Namun, dari segi lainnya, penyalahgunaan teknologi informasi telah menimbulkan sejumlah masalah. Dalam ruang maya atau yang disebut sebagai *cyberspace*, hampir semua aktivitas dapat dilakukan. Penggunaan internet yang tidak terkendali telah menjadi penyebab utama berbagai kejahatan di dunia maya, yang juga dikenal sebagai *cybercrime*. Fenomena ini telah menjadi tren di banyak negara, termasuk Indonesia (Fitriani & Pakpahan, 2020).

Menurut Widodo (2013), *cybercrime* didefinisikan sebagai segala tindakan yang dilakukan oleh individu, sekelompok orang, atau lembaga hukum dengan memanfaatkan komputer sebagai alat untuk melakukan kejahatan, serta menjadikan komputer sebagai *target* dari tindakan kejahatan tersebut. Kasus-kasus *cybercrime* yang muncul di Indonesia menampilkan fenomena tertentu, seperti insiden pencurian kartu kredit atau *carding*, upaya peretasan (*hacking*) terhadap berbagai situs, penyadapan data transmisi orang lain, serta manipulasi data melalui penyisipan perintah yang tidak dikehendaki ke dalam program komputer.

Pada tahun 2022, jumlah insiden pergerakan data terkait serangan siber tertinggi di Indonesia tercatat pada bulan Januari sekitar 273 juta kejadian. Deteksi pergerakan yang tidak lazim ini digunakan untuk mengidentifikasi aktivitas yang tidak umum yang terkait dengan serangan dalam dunia maya. Lebih dari 976 juta insiden yang terkait dengan serangan siber berhasil terdeteksi sepanjang tahun 2022 di Indonesia.

Cybercrime, sebagai bentuk kejahatan di ranah digital, mencakup berbagai aktivitas kriminal yang melibatkan penggunaan teknologi. Salah satu contohnya adalah *illegal access* atau akses ilegal, di mana pelaku mengakses data atau sistem komputer tanpa izin yang sah (Antoni, 2017). Modus ini sering kali digunakan dalam serangan *cyber* seperti *Phishing*, di mana para pelaku menggunakan trik tipu daya untuk memperoleh informasi sensitif dari korban. Misalnya, mereka mengirimkan *email* palsu yang terlihat seperti dari institusi resmi atau perusahaan terpercaya, yang bertujuan untuk memancing korban agar mengungkapkan informasi pribadi seperti kata sandi atau informasi keuangan. Kasus-kasus seperti ini telah menjadi perhatian serius dalam ranah *cybercrime*, di mana upaya-upaya ilegal se*Mac*am ini dapat menimbulkan kerugian besar baik bagi individu maupun perusahaan.

Phishing merupakan suatu tindakan kriminal yang memanfaatkan teknik rekayasa sosial. Para pelaku *Phishing* atau yang sering disebut *phisher*, berupaya untuk memperoleh informasi sensitif pribadi, seperti nama pengguna, kata sandi, dan rincian kartu kredit yang dapat digunakan untuk melakukan tindakan pencurian identitas (Radiansyah et al., 2016).



Gambar 1. Grafik Data Persebaran Serangan *Phishing* di Indonesia
Sumber: Annur (2022)

Laporan dari Direktorat Tindak Pidana Siber Bareskrim Polri menunjukkan bahwa terdapat 5.579 serangan *Phishing* yang tercatat di Indonesia sepanjang kuartal II-2022. Jumlah serangan ini menunjukkan peningkatan sebesar 41,52% dari bulan sebelumnya, di mana pada kuartal I-2022, terdapat 3.942 serangan. Data juga menunjukkan bahwa serangan *Phishing* paling banyak mengincar lembaga keuangan dengan persentase mencapai 41%. Diikuti oleh sektor *e-commerce* yang menjadi *target* sebanyak 32%, dan media sosial sebanyak 21%. Sementara itu, hanya sekitar 6% dari serangan *Phishing* yang diarahkan untuk pencurian data di *game online* dan akun aset kripto.

Banyaknya laporan mengenai *Phishing* ini disebabkan oleh rendahnya tingkat kesadaran masyarakat. Selain itu, para pelaku *Phishing* saat ini mampu menggunakan lebih dari satu nama, sehingga melahirkan lebih banyak laporan yang diterima. Kota Daerah Istimewa Yogyakarta mengalami peningkatan kasus *Phishing* yang meresahkan masyarakat, sebagaimana dilaporkan oleh news.detik.com pada hari Kamis, 30 April 2023. Seorang Pegawai Negeri Sipil (PNS) di Yogyakarta dengan inisial DR dikabarkan mengalami tekanan psikologis dan depresi akibat menjadi korban penipuan aplikasi *online* dengan kerugian mencapai Rp 600 juta. Modus yang digunakan dalam kasus ini adalah *Phishing*, di mana pelaku mengundang korban ke grup *Telegram* untuk menyelesaikan misi di aplikasi *Tiktok*. Setelah berhasil melaksanakan misi ringan, korban diminta melakukan *top-up* saldo melalui sebuah situs web palsu yang menyerupai aplikasi *Tiktok*. Dampaknya, DR mengalami kerugian finansial yang signifikan, dan berharap agar kasusnya diusut secara menyeluruh oleh aparat penegak hukum (Saputra, 2023).

Negara Republik Indonesia, yang menegakkan sistem hukum berdasarkan Pancasila dan Undang-Undang Dasar 1945, memiliki tujuan mewujudkan kehidupan bangsa yang sejahtera, aman, tentram, dan tertib. Perbincangan seputar hukum di Indonesia tak terlepas dari kaitannya dengan masalah atau kejahatan yang terjadi. Dalam konteks kasus di atas, pihak kepolisian menerapkan penegakan hukum terkait tindak pidana *cybercrime* yang telah diatur dalam Undang Informasi dan Transaksi Elektronik (UU ITE) Nomor 11 Tahun 2008, yang kemudian mengalami perubahan melalui Undang-Undang Nomor 19 Tahun 2016. Dalam UU ITE tersebut, terdapat beberapa pasal yang berhubungan dengan

cybercrime atau kejahatan dalam dunia maya.

Cybercrime telah banyak dibahas dan diungkap dalam berbagai riset. Namun, berbeda dengan penelitian ini, peneliti memfokuskan pada salah satu cybercrime yaitu ancaman *Phishing* yang sewaktu-waktu dapat menyerang siapa saja, kapan saja dan dimana saja, termasuk saya ataupun anda. Penanganan dan investigasi terhadap kasus *cybercrime* telah berhasil diungkap oleh Polda Daerah Istimewa Yogyakarta. Sehingganya, peneliti bertujuan untuk menemukan cara atau strategi investigasi Polda Daerah Istimewa Yogyakarta dalam pengungkapan kasus Phishing. Analisis mendalam terhadap strategi investigasi dan respons pihak berwajib menjadi fokus penelitian untuk memahami dinamika serta tantangan dalam menanggulangi ancaman *Phishing* yang semakin merajalela di masyarakat Indonesia, khususnya di wilayah Daerah Istimewa Yogyakarta. Upaya ini diharapkan dapat memberikan kontribusi positif dalam meningkatkan keamanan masyarakat Indonesia yang selalu beraktivitas secara daring atau sekedar berselancar menjelajahi dunia maya.

TELAAH LITERATUR

Segitiga Kejahatan

Teori Penipuan artinya sebuah tindakan seorang atau sekelompok orang membentuk kesan bahwa sesuatu itu yang dilakukan itu tidak salah serta tidak palsu agar membuat orang lain memberikan kepercayaan. Secara formal, penipuan didefinisikan menjadi tindakan "membujuk orang lain menggunakan tipu muslihat, rangkaian kata dusta , nama palsu, keadaan palsu supaya memberikan sesuatu" (Anwar, 1979). Umumnya penipuan dilakukan untuk membuat keuntungan diri sendiri atau kelompok pelaku sendiri, dan menyebabkan kerugian pada korban penipuan. Banyak kerugian yang diderita seseorang korban penipuan, baik kerugian berupa finansial, fisik maupun psikologis. Oleh karena itu, peneliti mengangkat teori tentang "*The Crime Triangle of Routine Activity Theory"*.

Segitiga Kejahatan atau dikenal sebagai Teori Aktivitas Rutin, merupakan konsep kriminologis yang menitikberatkan pada situasi terdekat di mana tindakan kriminal terjadi. Teori ini menekankan peran lingkungan dalam membentuk perilaku manusia dan aksi kejahatan. Teori ini menjelaskan kejahatan terjadi ketika pelaku yang termotivasi bertemu dengan *target* yang cocok pada waktu dan tempat tertentu tanpa adanya penghalang yang efektif. Teori ini berpendapat bahwa mengubah karakteristik dan prevalensi peluang kejahatan dapat membantu mencegah terjadinya kejahatan (Mui & Mailley, 2015).

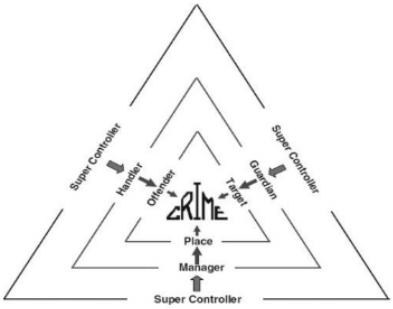
Konsep Segitiga Kejahatan memberikan pandangan luas terhadap lingkungan di mana kejahatan terjadi, termasuk pelaku serta pihak lain yang bisa mencegah atau memungkinkan terjadinya kejahatan. Dengan memeriksa konteks yang melingkupi kejahatan, teori ini memberikan perspektif komprehensif mengenai peristiwa kejahatan. Berbeda dengan fokus Segitiga Penipuan yang hanya menitikberatkan pada pelaku, Segitiga Kejahatan mempertimbangkan konteks yang lebih luas tempat kejahatan terjadi.

Segitiga Kejahatan diusulkan sebagai pelengkap bagi Segitiga Penipuan dalam memahami peristiwa penipuan (Mui & Mailley, 2015). Dengan menerapkan teori ini pada kasus penyalahgunaan aset, dapat memberikan pandangan menyeluruh mengenai peristiwa penipuan dengan mempertimbangkan lingkungan di mana

penipuan terjadi dan peran pihak-pihak terkait dalam mencegah atau memungkinkan terjadinya penipuan. Penggunaan Segitiga Kejahatan ini membuka pandangan baru dalam memahami serta menangani peristiwa penipuan.

Secara singkat, Segitiga Kejahatan atau Teori Aktivitas Rutin memberikan kerangka kerja untuk memahami faktor lingkungan dan situasional yang turut berperan dalam peristiwa kejahatan. Pendekatan ini melengkapi perspektif Segitiga Penipuan yang lebih memusatkan perhatian pada individu. Dengan demikian, pendekatan ini menawarkan pemahaman yang lebih tentang kejahatan dengan mempertimbangkan interaksi antara manusia dan lingkungannya.

Teori aktivitas rutin oleh Cohen & Felson (1979) awalnya menguraikan tiga faktor utama yang diperlukan untuk terjadinya kejahatan predator dengan kontak langsung. Kejahatan terjadi ketika: (1) ada pelaku yang terdorong untuk berkontak; (2) ada *target* yang cocok pada waktu dan tempat tertentu; dan (3) tidak ada penghalang yang efektif. Inti dari teori aktivitas rutin adalah bahwa kejahatan terjadi saat pelaku yang terdorong melakukan kontak pada waktu dan lokasi tertentu dengan *target* yang sesuai, tanpa ada pengawas yang efektif Cohen & Felson (1979). Segitiga Kejahatan, yang merupakan bagian dari Teori Aktivitas Rutin, terdiri dari tiga segitiga yang saling mempengaruhi (Gambar diatas). Ketiga elemen inti dalam segitiga yaitu: (1) calon pelaku, (2) target kejahatan, dan (3) lokasi terjadinya kejahatan.



Gambar 2. Konsep Segitiga Kejahatan

Sumber: Sampson (2010)

Segitiga bagian dalam mewakili tiga aspek yang dianggap penting untuk terjadinya suatu kejahatan. Segitiga di tengah menggambarkan pengawas dari setiap elemen dalam segitiga yang dapat mencegah kejadian kejahatan: penjaga, wali, dan pengelola tempat. Segitiga terluar melambangkan pengendali utama yang mengatur tingkah laku dari pengawas dalam segitiga tengah. Ketika pelaku berhasil menghindari pengawas, menemukan *target* yang tidak dijaga di lingkungan yang tak terawasi oleh pengelola, maka terjadilah kejahatan.

Dalam konteks penipuan, pelakunya adalah penipu atau penjahat korporat. Sasaran dari penipuan adalah korban dari kegiatan penipuan seperti aset organisasi, yang bisa berupa aset fisik seperti inventaris, atau aset virtual seperti database pelanggan. Tempat kejadian adalah organisasi itu sendiri, di mana aset biasanya berada. Segitiga tengah menggambarkan pengawas terhadap pelaku, tempat, dan sasaran. Pengawas pelaku adalah pawangnya. Pengawas tempat adalah manajernya. Pengawas sasaran adalah walinya. Penangan adalah individu yang memiliki kemampuan untuk mempengaruhi perilaku dari calon pelaku. Handler adalah seseorang yang memiliki hubungan sosial atau koneksi yang dapat mempengaruhi pelaku.

Teori aktivitas rutin Cohen & Felson (1979) menjelaskan bahwa

kejahatan terjadi saat pelaku bertemu dengan target yang tepat di waktu dan tempat tertentu tanpa pengawasan yang efektif. Felson (1986) menyoroti bahwa kehadiran seorang handler yang mempengaruhi pelaku bisa mencegah kejahatan, bahkan jika pelaku sudah berhubungan dengan target yang tepat namun tidak diawasi dengan baik.

Peran manajer, seperti yang dijelaskan oleh Eck (1994) dalam Felson (1995) adalah untuk mengendalikan akses dan perilaku di suatu tempat. Felson (1995) menyimpulkan bahwa kejahatan terjadi saat pelaku berhasil lolos dari pengawasan handler dan menemukan target yang tak dijaga di area yang sepi dari pengawasan, di mana manajer terlibat dalam pengawasan yang kurang efektif. Clarke & Harris (1992) menambahkan konsep fasilitator kejahatan, seperti fasilitator fisik (misalnya, komputer untuk penipuan), fasilitator sosial (tekanan dari teman sebaya), dan fasilitator kimia (seperti pengaruh alkohol terhadap perilaku pelaku). Memahami dampak fasilitator ini pada pelaku dapat membantu merancang strategi anti-penipuan yang efektif.

Pengendali super, yang bisa berupa institusi resmi atau entitas yang lebih tersembunyi, memiliki pengaruh pada pengawas dalam mencegah kejahatan (Sampson, 2010). Sampson (2010) menyatakan bahwa pengendali super memengaruhi pengawas berdasarkan pertimbangan rasional, di mana keputusan pengawas tentang tindakan terhadap kejahatan dipengaruhi oleh risiko, imbalan, usaha, alasan, dan dorongan yang ada. Jika pengawasan minim dan imbalan maksimal, pengendali super akan berperan penuh. Namun, jika tidak sejalan, pencegahan kejahatan bisa terabaikan.

Dengan kata lain, teori aktivitas rutin menjelaskan bahwa kejahatan terjadi ketika pelaku bertemu target yang tepat tanpa pengawasan. Pengaruh dari handler, manajer, dan wali dapat memengaruhi peluang terjadinya kejahatan. Fasilitator kejahatan dan pengendali super juga berperan penting dalam mencegah kejahatan berdasarkan pertimbangan pengawas.

Cybercrime

Cybercrime yang dikemukakan oleh Widodo (2013) merujuk pada setiap bentuk aktivitas yang dilakukan oleh individu, kelompok, atau entitas hukum yang menggunakan komputer sebagai alat untuk melakukan tindak kejahatan, baik sebagai sarana pelaksanaan maupun sebagai objek atau *target* dari kejahatan tersebut. Berikut adalah beberapa jenis kejahatan yang sering terjadi di Internet atau dunia maya, sebagaimana diidentifikasi dalam *Convention on Cyber Crime* 2001 di Budapest, Hongaria yang dikutip oleh Antoni (2017): (1) *Illegal Access/Unauthorized Access to Computer System and Service* (Akses tidak sah ke sistem komputer dan jasa). (2) *Illegal Contents* (Kejahatan dalam ranah *cybercrime* yang melibatkan penyisipan data atau informasi yang tidak akurat, tidak etis, atau yang dapat dianggap melanggar hukum atau mengganggu ketertiban umum ke dalam internet). (3) *Data Forgery* (Suatu bentuk kejahatan di dunia maya yang melibatkan pemalsuan data pada dokumen-dokumen penting yang disimpan secara elektronik melalui internet, sering kali dalam format *scripless document*. (4) *Cyber Espionage (Spionase Cyber)* merupakan tindakan kriminal yang menggunakan jaringan internet untuk melakukan pengintaian terhadap entitas lainnya dengan cara masuk ke dalam sistem jaringan komputer *(computer network system)* yang menjadi *target*-nya. (5) *Cyber Sabotage and Extortion* (Sabotase

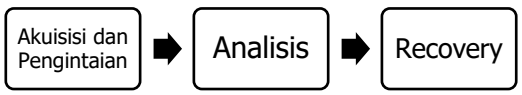
dan pemerasaan dunia maya). (6) *Offense Against Intellectual Property* (Pelangganran atas hak kekayaan intelektual). (7) *Infringements of Privacy* (Tindakan kejahatan ini bertujuan untuk memperoleh informasi pribadi seseorang yang disimpan dalam formulir data pribadi yang terkomputerisasi. seperti kebocoran nomor kartu kredit, nomor PIN ATM, dan informasi pribadi lainnya).

Phishing

Phishing merupakan sebuah tindakan dengan menggunakan rekayasa sosial sebagaimana yang dijelaskan oleh (Windarni et al., 2023). *Phishing* adalah serangan *online* umum di mana pengguna dibujuk untuk mengunjungi situs *web* palsu. Mereka dimanfaatkan untuk mengungkapkan informasi pribadi seperti sandi, nama pengguna, dan rincian kartu kredit. Tingginya kejadian *Phishing* telah menyebabkan kerugian serius dalam privasi, bahkan mengakibatkan gangguan keuangan akibat penyalahgunaan data. Skema rekayasa sosial melibatkan penggunaan surel palsu yang berpura-pura berasal dari lembaga bisnis yang sah. Tujuannya adalah agar korban diarahkan ke situs *web* palsu yang menipu, sehingga akhirnya mereka memberikan informasi keuangan seperti nama dan sandi. Skema teknis lainnya melibatkan penyisipan perangkat lunak berbahaya ke dalam komputer untuk mencuri informasi secara langsung. Seringkali, metode ini juga menggunakan sistem untuk menipu pengguna dengan cara menyesatkan terkait nama pengguna dan sandi akun daring mereka. Bahkan, infrastruktur navigasi lokal bisa dimanipulasi untuk mengarahkan konsumen ke situs *web* palsu, atau mengalihkan mereka ke situs *web* asli melalui pengalihan yang dikendalikan oleh penipu (*phisher)*. Ini memungkinkan penjahat untuk memantau dan mencuri informasi dari konsumen.

Menurut (Windarni et al., 2023) seorang *phisher* melakukan kejahatan *cyber* dengan memanfaatkan beberapa teknik tertentu, di antaranya: *Pertama, Email Spoofing; Phisher* menggunakan teknik ini untuk mengirim *email* seakan-akan dari lembaga resmi kepada banyak orang, meminta informasi pribadi seperti nomor kartu kredit atau kata sandi. *Kedua,* Pengiriman Berbasis Web; *Phisher* menempatkan diri di antara situs web asli dan situs palsu untuk melakukan serangan "*man-in-the-middle*". *Ketiga,* Pesan Instan *(chatting); p*engguna menerima pesan dengan tautan ke situs web palsu yang terlihat seperti situs resmi, membuat pengguna percaya padahal sebenarnya palsu. *Keempat, Trojan hosts; Phisher* mencoba masuk ke akun pengguna untuk mencuri informasi pribadi. *Kelima*, Manipulasi tautan (*link*); *Phisher* mengirim tautan ke situs web palsu yang berbeda dari yang seharusnya. *Keenam*, *Malware Phishing; p*enggunaan malware dalam *email phisher* untuk menyerang komputer pengguna setelah mengklik tautan atau mengunduh *file*.

Network forensics merupakan bagian dari digital forensics yang terfokus pada pemantauan dan analisis aliran data di dalam jaringan komputer. Tujuannya adalah untuk mengumpulkan informasi, bukti hukum, dan mendeteksi akses ilegal pada jaringan tersebut. Proses forensik pada jaringan terdiri dari tiga tahap, sebagaimana yang terlihat dalam gambar berikut ini.



Gambar 3. Proses Forensik
Sumber: Windarni et al., (2023)

Gambar di atas menggambarkan tiga tahapan proses forensik pada jaringan, yang terdiri dari:

a. Akuisisi dan pengintaian (*reconnaissance*): Tahap ini mencakup kegiatan pengumpulan informasi mengenai aktivitas *Phishing* yang akan dianalisis. Pengumpulan data dapat dilakukan melalui dua metode: pertama, pengumpulan data dengan bekerja secara langsung pada sistem *online* (data yang mudah berubah), dan kedua, pengumpulan data dari disk yang terkait dengan aktivitas *Phishing* secara *offline* menggunakan berbagai perangkat bantu (data yang tidak mudah berubah).
b. Analisis: Pada tahap ini, dilakukan pengamatan mendetail terhadap data yang diperoleh dari proses *reconnaissance*. Langkah ini melibatkan dekonstruksi komponen-komponen data untuk analisis lebih lanjut. Analisis yang dilakukan mencakup evaluasi aktivitas dalam jaringan komputer baik secara *online* maupun *offline*, pemeriksaan jejak *Phishing* (baik yang berupa data yang mudah berubah atau tidak), pemeriksaan *log-file*, korelasi data dari berbagai perangkat dalam jaringan yang terkena serangan, dan pembuatan urutan kejadian dari informasi yang diperoleh.
c. *Recovery:* Tahapan ini bertujuan untuk memulihkan data yang hilang akibat intrusi, terutama informasi pada disk seperti *file* atau direktori yang terpengaruh

METODE PENELITIAN

Penelitian ini menggunakan metode studi kasus dengan pendekatan kualitatif. Peneliti terlibat secara langsung dalam interaksi dengan sumber data untuk memperoleh pemahaman mendalam mengenai masalah dan tren kasus *Phishing* di Daerah Istimewa Yogyakarta, serta proses pengungkapan yang dilakukan oleh Polda DIY terhadap kasus *Phishing* di wilayah tersebut. Dalam penelitian ini, peneliti melakukan wawancara dengan tiga informan dari Direktorat Reserse Kriminal Khusus (Direkrimsus) Polda Daerah Istimewa Yogyakarta. Berikut ini merupakan tabel yang memuat profil dari informan Direktorat Reserse Kriminal Khusus Polda Daerah Istimewa Yogyakarta.

Tabel 1. Daftar Informan

Informan	Jenis Kelamin	Pangkat	Masa Bekerja di Polda DIY
CB	Laki-laki	Bripka	>2 tahun
MR	Laki-laki	Brigadir	>3 tahun
RP	Laki-laki	Bripda	>2 tahun

Penelitian yang menggunakan metode penelitian studi kasus ini dipilih dengan alasan studi kasus berasal dari jawaban terhadap tiga pertanyaan epistemologis, yakni terkait dengan tipe pertanyaan, kontrol terhadap objek, dan cakupan penelitian. Melalui metode penelitian studi kasus, peneliti fokus mengamati kejadian sesuai keadaannya, menunjukkan pendekatan naturalistik yang relatif alami. Fokusnya adalah peristiwa atau gejala sosial kontemporer dalam kehidupan nyata, memungkinkan akses melalui pengamatan partisipatif dan wawancara mendalam dengan subjek penelitian (Yin, 1989).

Sumber data dalam penelitian ini menggunakan data primer dan data sekunder. Menurut (Nasution, 2023) data primer dalam penelitian adalah informasi utama yang diperoleh secara langsung dari subjek penelitian atau sumber pertama. Jenis data ini dianggap autentik, obyektif, dan dapat dipercaya karena menjadi landasan untuk mengatasi suatu permasalahan. Data primer ini dapat berupa hasil wawancara dengan subjek, hasil kuesioner, hasil tes, dan lain sebagainya. Sedangkan menurut (Nasution, 2023), data sekunder dalam penelitian merupakan informasi yang

tidak diperoleh secara langsung dari subjek penelitian atau sumber pertama. Jenis data ini berfungsi sebagai tambahan dan pendukung dari data primer.

Data yang sudah dikumpulkan peneliti kemudian diolah menggunakan *software* Nvivo 12, yang berguna dalam menganalisis data penelitian kualitatif seperti teks, audio, video, dan gambar. Untuk mempermudah analisis, peneliti membuat "*nodes*" untuk mengelompokkan hasil wawancara dan dokumen penelitian. *Nodes* ini merupakan inti topik pembahasan dalam rumusan masalah. Selanjutnya, peneliti membuat "*relationships*" untuk menghubungkan *nodes* yang telah dibuat. Data dari sumber diatur sesuai dengan kriteria *nodes* yang telah ditetapkan.

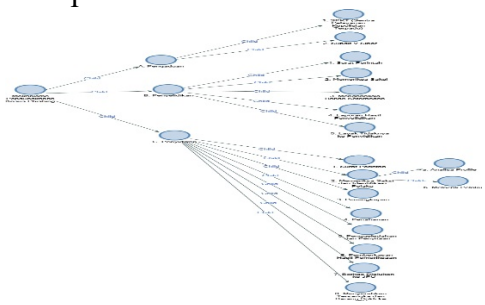
Data yang terkumpul kemudian dianalisis dengan proses *coding. Coding* merupakan langkah analisis data yang dilakukan secara berkelanjutan dengan tujuan untuk mengidentifikasi dan membentuk kategori-kategori utama berdasarkan data yang terkumpul (Bandur, 2016). Fitur *coding* ini menghubungkan pernyataan narasumber dengan narasumber yang lain dalam narasi yang berkaitan dengan topik yang disajikan.

Selanjutnya, peneliti membuat Peta Analisis menggunakan bantuan *software* Nvivo 12. Peta Analisis dibuat dengan tujuan agar mempermudah pembacaan pada bab pembahasan. Peneliti memiliki gambaran *maps* yang terbagi sesuai dengan dua rumusan masalah yang telah diidentifikasi sebelumnya. Peta analisis ini membantu dalam memahami hubungan antara *nodes* dengan berbagai dokumen yang dimiliki peneliti, baik dalam bentuk teks, visual, maupun gambar.

Data yang telah diolah dengan bantuan *software* Nvivo 12 disajikan oleh peneliti dalam bentuk narasi, tabel, Peta Analisis, dan hasil analisis. Hal ini menjadi dasar penelti untuk evaluasi terhadap "Peran Polda DIY dalam Pengungkapan Kasus *Phishing* di wilayah Daerah Istimewa Yogyakarta". Peneliti melakukan penarikan kesimpulan berdasarkan data yang telah dianalisis untuk mengakhiri penelitian ini.

HASIL DAN PEMBAHASAN PENELITIAN

Hasil penelitian dipresentasikan melalui visualisasi data dalam bentuk peta analisis, yang menggunakan hasil transkrip wawancara yang dikodekan dan diproses menggunakan NVivo 12 Plus seperti berikut ini.



Gambar 4. Peta Analisis Mekanisme Pengungkapan Kasus Phishing
Sumber: Diolah peneliti

Pengungkapan Kasus Phishing: Pengaduan Korban

Mekanisme pengungakan kasus phishing tentu bermula dari laporan atau pengaduan masyarakat. Apabila korban atau pelapor ingin melaporkan kejadian dan membuat laporan di Polda Daerah Istimewa Yogyakarta, tidak ada biaya yang diperlukan (gratis). Pihak kepolisian tidak akan meminta pembayaran apapun, sebagaimana dijelaskan oleh informan berikut:

> *"Dalam praktik phishing, tidak ada biaya yang secara langsung melibatkan korban. Semua*

biaya untuk penyelidikan dan pengusutan telah dianggarkan sebelumnya," Informan MR (2023

Laporan kasus phising di Polda Daerah Istimewa Yogyakarta dapat dilakukan pada Sentra Pelayanan Kepolisian Terpadu (SPKT) dan juga Subdit V Siber.

"Prosedur awal korban menyampaikan keluhan dalam bentuk laporan maupun aduan dengan beberapa cara. Satu melalui SPKT polda DIY dan diarahkan ke ditreskrimsus ini yang kepada polda. Tapi ada juga korban yang melaporkan melalui nomor siaga piket ditreskrimsus. Selanjutnya datang dengan membawa dokumen. Yang ketiga korban melaporkan melalui akun layanan siber layanan polri," Informan RP (2023)

Dalam proses laporan ini, masyarakat atau pelapor perlu melampirkan dokumen bukti yang mendukung proses terjadinya kasus phishing. Pelapor dapat menunjukkan bukti awal berupa tangkapan layar percakapan, informasi akun, serta nama pelaku atau nama samaran yang digunakan oleh pelaku. Selain itu, juga disertakan rekening koran atau bukti transfer, rincian website terkait, dan transaksi yang relevan yang perlu ditunjukkan. Sebagaimana yang dikemukakan informan MR berikut ini:

"Dokumen atau alat bukti harus disertakan oleh korban ketika membuat laporan kasus phishing. Apa dokumennya yaitu semua dokumen atau alat bukti yang berhubungan dengan dugaan tindak pidana yang dilakukan oleh pelaku, yang bisa menjadi petunjuk," Informan MR (2023)

Berangkat dari laporan pengaduan tersebut, kemudian Ditreskrimsus Polda akan melakukan penilian apakah kasus tersebut melibatkan unsur tindak pidana atau tidak. Keputusan tersebut akan segera disampaikan kepada korban atau pelapor melalui surat rekomendasi hasil gelar perkara, yang mencantumkan pasal tindak pidana jika diperlukan. Setelah itu, korban atau pelapor akan dipandu ke unit-unit yang sesuai di Ditreskrimsus Polda DIY.

"Memberikan surat rekomendasi gelar awal. Disini pihak kepolisian akan memberikan tanggapan atau masukan terhadap kasus korban, jika terjadi tindak pidana korban harus seperti apa," Informan RP (2023)

Tahap selanjutnya, pelapor atau korban membawa surat rekomendasi hasil gelar perkara yang berwarna pink, yang telah diisi oleh petugas piket Subdit V Siber di Direktorat Reserse Kriminal Khusus Polda DIY, karena ini terkait dengan kasus phishing. Pelapor kemudian berkonsultasi dan menjelaskan kasusnya kepada petugas Siber Polda DIY, sejalan dengan pernyataan dari informan RP berikut ini:

"Korban akan konsultasi dengan pihak siber tentang kasusnya, kalau memenuhi unsur pidana ITE lalu diarahkan ke Krimsus (Kriminal Khusus) yang

> *menangani dari Direktorat Reserse Kriminal Khusus unit Siber,"* Informan RP (2023)

Pada tahap ini, menghasilkan dua jawaban. Pertama, jika laporan tersebur memenuhi unsur pidana maka laporannya di proses ke tahap selanjutnya. Namun jika tidak, maka laporan kasus tersebut tidak dapat diposes.

> *"Kalau memenuhi unsur pidana ITE lalu diarahkan ke Krimsus (Kriminal Khusus) yang menangani dari Direktorat Reserse Kriminal Khusus unit Siber,"* Informan RP (2023)

Mengacu pada rangkaian penjelasan dari para informan tersebut, peneliti memahami bahwa proses pengaduan hingga laporan kasus phishing diproses oleh Polda Daerah Istimewa Yogyakarta (DIY) memerlukan beberapa tahapan yang persipapan data yang akurat. Data yang mengandung bukti-bukti menjadi korban dari kasus phishing. Tentu ini bukanlah hal yang mudah, mengingat kasus phishing bukti-buktinya sulit ditemukan. Belum lagi, keterbatasan korban dalam literasi digital kurang memungkinkan bukti yang diminta oleh kepolisian tidak dapat terwujud. Karena, sebagian besar korban kasus phishing menyasar masyarakat yang memiliki perlindungan akun digital lemah. Seperti, pengguanaan sandi email atau password akun yang cenderung menyesuaikan dengan tanggal lahir atau nama korban. Sebagaimana teori aktivitas rutin yang menyebutkan bahwa, kejahatan terjadi ketika target atau korban tidak berada dalam pengawasan atau perlindungan. Pengawasan atau perlindungan dalam dunia maya tiada lain adalah diri sendiri. Ketika diri sendiri tidak mampu melakukan perlindungan terhadap akun digitalnya, maka pelaku mempunyai kesempatan untuk memilih siapa saja yang menjadi target phishing.

Pengungkapan Kasus Phishing: Penyelidikan Kasus

Laporan dari korban yang ditinjaklanjuti tentu akan Direktorat Reserse Kriminal Khusus (Ditreskrimsus) Polda DIY untuk mencari bukti tindak pidana kejahatan siber. Proses ini untuk menentukan apakah perlu dilakukan penyidikan, seperti disampaikan oleh informan berikut ini:

> *"Yang kedua adalah naik ke tahap penyelidikan, disini kami mencari bukti adanya tindak pidana,"* Informan RP (2023)

Dalam proses ini pihak kepolisian akan mengeluarkan Surat Perintah Tugas (SPT) dan Surat Perintah Penyelidikan (SPP). Setelah terbitnya SPT dan SPP, diterbitkan pula SP2HP A1 untuk memberitahu pelapor nomor handphone, nama, dan penyidik yang menangani kasus phishing. Kemudian, langkah awal yang akan dilakukan oleh Ditreskrimsus Polda DIY dalam proses penyelidikan yaitu: ***Pertama,*** pemeriksaan saksi-saksi.

> *"Setelah kami membuat surat tersebut kami melakukan pemeriksaan kepada saksi, disini kami meminta keterangan tentang kejadian yang dialami korban dan memeriksa, ada tindakan pindana yang dilakukan,"* Informan RP (2023)

Kedua, menganalisis bahan keterangan. Menganalisis bukti, seperti

akun media sosial, nomor handphone, rekening bank, website, dan tautan terkait dalam peristiwa tindak pidana (kasus phishing). Sebagai contoh, korban memencet tautan yang dikirimkan pelaku melalui media sosial, menyebabkan kehilangan uang dalam dompet digitalnya. bahwa korban memeriksa saldo uangnya yang dikirim melalui nomor dompet digital.

> *"Setelah itu menganalisa bukti yang didapat dari korban, kita pilah-pilih lagi, apakah ada kaitannya dengan tindak pidana. Jika kita menemukan adanya tindak pidana yang diterima oleh korban kami akan membuat laporan hasil penyelidikan,"* Informan RP (2023)

Ketiga, laporan hasil penyelidikan. Pada tahap ini Subdit V Siber Polda DIY, menangani laporan hasil penyelidikan yang mencakup informasi seperti akun penipu, lokasi, waktu, dan kejadian, untuk menentukan apakah terjadi tindak pidana atau tidak. Seperti yang dijelaskan oleh informan RP sembari menunjukan contoh dari laporan hasil penyelidikan.

> *"Laporan hasil penyelidikan ini adalah temuan-temuan yang dilakukan penyidik. Disitu para penyidik dapat menentukan, sebenarnya kasus ini bisa masuk ke tahap penyidikan tidak,"* Informan RP (2023).

Keempat, penentuan ke tahap penyidikan. Tahap ini menjadi bagian akhir dari proses penyelidikan. Setelah mengumpulkan hasil penyelidikan seperti akun penipu, pelapor, saksi, dan bukti awal, tim penyelidikan akan membuat keputusan atau kesimpulan. Jika hasilnya mengindikasikan adanya unsur tindak pidana, proses akan dilanjutkan ke tahap penyidikan. Sebaliknya, jika tidak ada unsur tindak pidana, penyelidikan akan dihentikan, dan surat pemberhentian penyelidikan akan dibuat dan ditandatangani oleh Direktur Ditreskrimsus Polda DIY. Hal ini sebagaimana pernyataan dari 2 informan di bawah ini.

> *"Untuk tindak lanjut penanganan (menghentikan penyelidikan atau melanjutkan ke tahap penyidikan,"* Informan MR (2023)

> "*Disitu para penyidik dapat menentukan, sebenarnya kasus ini bisa masuk ke tahap penyidikan tidak. Nanti pelapor biasanya komunikasi dengan penyidik untuk menanyakan perkembangan perkaranya gimana,"* Informan RP (2023).

Pengungkapan Kasus Phishing: Tahap Penyidikan

Masuk pada tahap penyidikan, maka proses ini merupakan investigasi mendalam yang akan dilakukan oleh aparat kepolisian yang ada di Ditreskrimsus Polda DIY. Proses investigasi dilakukan secara mendalam untuk mengungkap fakta-fakta yang mendukung terjadinya kasus phishing. Terdapat beberapa dokumen yang akan dikeluarkan oleh Ditreskrimsus Polda DIY ketika kasus masuk tahap penyedikan, diantaranya:

Pertama, penerbitan Sringas (Surat Perintah Tugas) dan Sprin (Surat Perintah). Springas berbeda dengan Sprin, dimana springas merupakan surat dari pimpinan yang menugaskan tim penyidik untuk melaksanakan tugas

tertentu dalam penyidikan, sementara sprin adalah perintah langsung untuk melakukan penyidikan tindak pidana *phishing* dan menyusun rencana pelaksanaannya. Meskipun tujuannya hampir sama, springas fokus pada tugas penyidik, sedangkan sprin menitikberatkan pada perintah terkait proses penyidikan. Setelah diterbitkan surat perintah penyidikan dan surat perintah tugas untuk kasus *phishing* di Polda DIY, maka akan dibuat kembali SP2HP untuk menginformasikan kepada pelapor bahwa perkara tersebut naik ke tahap penyidikan. Tim penyidik juga akan mengeluarkan surat pemberitahuan dimulainya penyidikan (SPDP) dengan lampiran laporan polisi dan surat perintah penyidikan, tanpa menyebut nama tersangka.

> *"Kami akan membuat springas, sprin, SP2HP dan SPDP. Springas itu untuk menegaskan, lalu untuk surat SPDP akan dikirimkan ke JPU kurang dari 7 hari setelah surat penyidikan turun,"* Informan RP (2023)

Kedua, pemeriksaan saksi. Meskipun pada tahap penyidikan sudah dilakukan pemeriksaan saksi, namun ketika kasus masuk pada tahap penyelidikan maka pemeriksaan saksi-saksi tetap dilakukan. Tahap pemeriksaan saksi pada proses penyelidikan dan penyidikan ini berbeda. Dalam penyelidikan, saksi, terutama saksi korban, memberikan keterangan untuk mengumpulkan informasi mengenai keberadaan tindak pidana penipuan jual beli online. Sementara itu, dalam penyidikan, saksi diminta memberikan bukti yang dapat membantu mengidentifikasi tersangka, seperti postingan akun penipu, alamat pelaku, screenshoot transfer korban, dan pengakuan bahwa telah terjadi tindak pidana yang terungkap dalam percakapan online. Semua barang bukti yang disampaikan saksi kemudian disita oleh penyidik. Hal ini sesuai dengan narasi yang disampaikan oleh informan MR dan juga informan RP.

> *"Penyidikan dilakukan untuk mengumpulkan bukti lebih lanjut, menentukan tersangka, dan mencari kejelasan terhadap peristiwa," informan MR (2023)*

> *"Setelah itu kami memeriksa saksi-saksi, saksi-saksi diminta memberikan bukti yang dapat membantu mengidentifikasi tersangka, seperti postingan akun penipu, alamat pelaku, screenshoot transfer korban, dan pengakuan bahwa telah terjadi tindak pidana yang terungkap dalam percakapan online surat tersebut," Informan RP (2023)*

Ketiga, analisa profile pelaku. Dalam tahap ini, proses analisa profil melibatkan evaluasi dan interpretasi informasi terkait seseorang atau sesuatu yang berhubungan dengan pelaku. Hal ini sesuai dengan apa yang di ungkapkan oleh informan MR dan RP berikut ini:

> *"Penyidikan dilakukan untuk mengumpulkan bukti lebih lanjut, menentukan tersangka, dan mencari kejelasan terhadap peristiwa dengan cara melakukan analisa profil,"* Informan MR (2023)

> *"Pada saat memeriksa saksi-saksi kami juga melakukan analisa profile untuk melihat*

latar belakang pelaku ini, seperti apa dia di kehidupan sehari-hari," Informan RP Putra (2023)

Dalam proses analisa profile terdapat beberapa aspek yang menjadi kunci keberhasilan pengungkapan kasus phishing, yaitu sebagai berikut:

a) Identitas Personal. Pada aspek ini, pihak kepolisian melakukan pencarian informasi seperti nama, usia, tempat tinggal, pekerjaan, dan pendidikan yang terkait dengan pelaku.
b) Jejak Digital. Aspek ini, dilakukan penelusuran aktivitas online, termasuk media sosial, untuk memahami perilaku, minat, dan interaksi sosial dari para pelaku.
c) Riwayat Pekerjaan dan Pendidikan. Pihak kepolisian juga menyelidiki pengalaman pekerjaan dan latar belakang pendidikan yang mendorong pelaku melakukan aksinya.
d) Hubungan Sosial. Selain informasi pribadi mengenai pelaku, proses investigasi juga melibatkan pencarian informasi terkait hubungan sosial dan bagaimana kehidupan yang dilakukan sehari-hari oleh pelaku, hubungannya antar keluarga, teman, atau kerabatnya.
e) Aktivitas Finansial. Aspek ini sangat penting, untuk menemukan riwayat transaksi keuangan atau kredit yang berhasil dihimpun ketika pelaku menjalankan aksinya.
f) Perilaku dan Kepribadian. Pada aspek ini, dilakukan identifikasi pola perilaku dan kepribadian melalui aktivitas online dan offline yang selama ini dilakukan oleh pelaku.

Keempat, melacak pelaku. Setelah informasi telah terkumpul maka langkah berikutnya adalah melacak keberadaan pelaku. Melacak pergerakan pelaku dapat dilakukan menelusuri jejak digital untuk mempermudah identifikasi pelaku seperti: nomor ponsel, Email, link, dan transaksi ATM. Rekaman CCTV mendukung upaya pelacakan ini. Kebiasaan pelarian, termasuk kunjungan kepada keluarga dekat, dapat membantu pelacakan. Koordinasi dengan anggota komplotan berguna untuk membangun profil pelaku. Informasi dari masyarakat dan informan menjadi aspek krusial. Melacak pelaku juga dapat dilakukan dengan penyebaran data melalui DPO (Daftar Pencarian Orang) di kepolisian dan kerja sama internasional, seperti melalui Interpol dan Red Notice, dilakukan untuk mengejar pelaku kejahatan yang kemungkinan tidak berada di Indonesia. Proses melacak keberadaan pelaku ini sesuai dengan pernyataan dari informan RP.

"Setelah kami dapatkan latar belakangnya, kami melacak pelaku tersebut, posisi terakhirnya dimana, pelaku sedang melakukan apa dan nanti kita akan koordinasi," Informan RP (2023)

Kelima, penangkapan pelaku. Tahap ini akan dilakukan oleh pihak Polda DIY ketika mengetahui apakah itu benar-benar pelaku, dengan cara mengumpulkan bukti-bukti yang mengarahkan kepada pelaku. Hal ini sesuai dengan pernyataan dari informan RP.

"Kalau di penyidikan itu bisa upaya paksa untuk penangkapan itu bisa. Kalau pelakunya ketangkap itu berdasarkan sprinkep, springledah itu ada, sprinkes, sprinlidik itu pasti wajib kita bawa sebagai dasar kami," Informan RP (2023)

Keenam, penahanan pelaku. Pada tahap penahanan dalam kasus *phishing* yang ditangani oleh Tim Penyidik Subdit V Siber Polda DIY melibatkan prosedur, di mana setelah melakukan penangkapan, seorang pelaku harus diperiksa maksimal dalam waktu 1X24 jam. Setelah pemeriksaan, tim penyidik harus segera menentukan apakah pelaku tersebut akan ditahan atau tidak. Dalam konteks penanganan kasus phishing, tidak ada mekanisme perpanjangan penahanan yang dilakukan oleh pengadilan. Hal ini sebagaimana pernyataan dari informan berikut:

> *"Setelah pelaku tertangkap nanti kita masukan sel (penahanan), kami melakukan penahanan berdasarkan bukti dan surat ya mba. jadi tidak asal menahan orang seperti ada etikanya. disamping itu kami juga akan mengolah berkasnya. Penahanan dilakukan 1x24 jam dan harus segera menetapkan apakah pelaku ditahan atau tidak,"* Informan RP (2023)

Ketujuh, penggeledahan dan penyitaan. Tim penyidik dalam menjalankan tugas penggeledahan dan penyitaan melakukan pemeriksaan tubuh (barang-barang) seperti di dalam tas, pakaian, dan menemukan dompet yang berisi kartu ATM, nomor rekening, serta ponsel yang memuat akun yang terlibat dalam kegiatan penipuan di platform sosial seperti Instagram atau Facebook. Jika terjadi kekurangan alat bukti selama proses penggeledahan, maka penyidik diwajibkan untuk melakukan penggeledahan di tempat tinggal pelaku dengan cara mengeluarkan surat penggeledahan.

> *"Kami juga melakukan penggeledahan dan penyitaan barang bukti pelaku. Penggeledahannya terhadap barang, alat buktinya itu semisal seperti telfon, buku tabungan yang biasanya digunakan pelaku untuk melakukan kejahatan tersebut,"* Informan RP (2023)

Kedelapan, pemberkasan hasil pemeriksaan dan pelimpahan berkas, barang bukti serta tersangka ke JPU. Tahap ini dilakukan pemberkasan hasil pemeriksaan dengan mengumpulkan dokumen penyidikan dari tahap awal pengungkapan phishing hingga pemeriksaan hasil penggeledahan dan penyitaan membentuk berkas merah. Berkas tersebut kemudian dilimpahkan ke Jaksa Penuntut Umum (JPU) di Kejaksaan Tinggi (Kejati) Negeri Yogyakarta, sebagai lembaga yang berkompeten untuk menangani penuntutan terhadap tindak pidana phishing. Seperti yang diungkapkan oleh informan berikut ini.

> *"Setelah berkasnya jadi (rampung), kita geser (serahkan) ke Kejanti. Sampai alurnya itu masuk ke tahap 1 atau pengiriman berkas perkara. Setelah tahap 1 selesai, biasanya kalau ada kekurangan dari pihak kejaksaan akan mengirimkan surat P19 yang berisi tentang kurangnya apa, nanti ditulis di surat itu. Kita nanti melengkapi itu,"* Informan RP (2023)

Selanjutnya, setelah JPU menganggapi bahwa berkas perkara

phishing sudah lengkap, tim penyidik Subdit V Siber Polda DIY menerima surat (P21) dari Jaksa Penuntut Umum. Selanjutnya, tim penyidik mengantarkan tersangka beserta barang bukti kepada Jaksa Penuntut Umum. Sebagaimana pernyataan dari informan RP dan MR berikut ini:

> *"Setelah kita melengkapinya kita kirimkan kembali lagi itu nanti kalau udah diterima Kejaksaan akan muncul P21. Nah setelah P21 itu muncul, itu bisa dilakukan Tahap 2. Tahap 2 yaitu tersangka, pelimpahan berkas perkara dan barang bukti,"* Informan RP (2023)

> *"Setelah selesai, hasil penyidikan bersama barang bukti atau tersangka diserahkan ke JPU. Peran Jaksa adalah menuntut di persidangan. Dengan demikian, tugas polisi menerima laporan, melakukan penyelidikan selesai sampai pada tahap penyidikan. Sedangkan tugas Jaksa dimulai dari situ untuk menuntut di Pengadilan,"* Informan MR (2023)

PENUTUP

Kesimpulan

Mekanisme pengungkapan kasus phishing oleh Polda Daerah Istimewa Yogyakarta melalui tiga tahapan: ***Pertama***, pengaduan dilakukan pada saat korban melapor ke Sentra Pelayanan Kepolisian Terpadu (SPKT) Polda DIY dengan membawa identitas dan bukti terkait kasus phishing. Korban dapat menceritakan kronologi kejadian kepada petugas. Jika dugaan melibatkan tindak pidana, surat rekomendasi gelar awal perkara disusun. Korban berkonsultasi dengan petugas Siber Subdit V. Jika kasus memenuhi unsur pidana, formulir rekomendasi gelar awal perkara diisi. Surat rekomendasi dibawa ke SPKT untuk Surat Pengaduan dengan informasi lengkap. ***Kedua,*** penyelidikan dilakukan untuk mencari bukti tindak pidana dan menentukan apakah perlu penyidikan. Surat Perintah Tugas dan Penyelidikan dibuat, saksi diperiksa, bukti dianalisis, dan laporan disusun. Hasilnya menentukan lanjut ke penyidikan atau tidak. ***Ketiga***, jika kasus lanjut ke tingkat penyidikan, maka proses penyidikan melibatkan langkah-langkah seperti pembuatan Springas, pemeriksaan saksi, analisis profil pelaku, pelacakan, identifikasi melalui gelar perkara, penangkapan, penahanan, penggeledahan, penyitaan, dan pemberkasan hasil pemeriksaan. Setelah penyidikan, berkas diserahkan ke Jaksa Penuntut Umum (JPU) untuk penuntutan di pengadilan. Pihak kepolisian mengumpulkan bukti dan menjalankan penyidikan, sementara jaksa menangani penuntutan. Proses ini memastikan penegakan hukum adil dengan tujuan mengungkap dan menindak pelaku kejahatan dengan bukti yang cukup di hadapan hukum. Meskipun langkah pengungkapan kasus phishing ini sangat jelas tahapannya, namun proses pengungkapan seringkali mengalami kendala yang signifikan. Seperti, kekurangan data atau bukti dalam menetapkan pelaku, minimnya literasi masyarakat terkait bukti yang mendukung pengejaran pelaku, dan kesulitan indetifikasi pelaku yang berada di luar negeri, serta akses terhadap informasi perbankan juga melengkapi kendala yang sering terjadi dalam pengungkapan kasus phishing.

Peneliti menyadari, penelitian ini masih memiliki keterbatasan. Hal itu dikarenakan peneliti tidak dapat

mengakses data kasus phishing secara keseluruhan. Sebagian besar data tersebut masih dalam proses penyelidikan atau penyidikan oleh pihak berwenang, sehingga datanya belum dapat dibuka ke publuk. Selain itu, terdapat beberapa data yang tidak dapat ditampilkan dalam penelitian ini karena bersifat rahasia dan sensitif. Hal ini mengisyaratkan adanya kendala dalam mengungkapkan informasi tertentu yang mungkin dapat mengganggu proses investigasi atau melibatkan privasi individu. Oleh karena itu, penelitian ini masih memerlukan kajian yang lebih mendalam terkait mekanisme pengungkapan kasus *phishing*. Perlu dilakukan upaya lebih lanjut untuk memahami secara detail proses tersebut serta mengatasi kendala-kendala yang mungkin muncul selama proses investigasi. Peneliti selanjutnya diharapkan mampu menyajikan hasil yang lebih kompleks, dengan melibatkan pihak korban ataupun pelaku dalam melengakapi proses analisis peran Polda DIY dalam pengungkapan kasus phishing di Yogyakarta.

DAFTAR PUSTAKA

Annur, C. M. (2022). *Ada 5 Ribu Serangan Phishing Terjadi di RI pada Kuartal II2022, Ini Lembaga yang Paling Banyak Diincar*. Databoks. https://databoks.katadata.co.id/datapublish/2022/08/23/ada-5-ribu-serangan-Phishing-terjadi-di-ri-pada-kuartal-ii-2022-ini-lembaga-yang-paling-banyak-diincar

Antoni. (2017). Kejahatan Dunia Maya (Cybercrime) dalam Simak Online. *Nurani: Jurnal Kajian Syari`ah Dan Masyarakat*, *17*(2), 261–274. https://doi.org/https://doi.org/https://dx.doi.org/10.19109/nurani.v17i2.1192

Anwar, M. (1979). *Hukum Pidana Bagian Khusus (KUHP II)*. Percetakan Offset Alumni.

Bandur, A. (2016). *Penelitian Kualitatif Metodologi, Desain dan Teknik Analisis Data dengan Nvivo 11 Plus*. Mitra Wacana Media.

Clarke, R. V., & Harris, P. M. (1992). Auto Theft and Its Prevention. *Crime and Justice*, *16*, 1–54.

Cohen, L. E., & Felson, M. (1979). Social Change and Crime Rate Trends: A Routine Activity Approach. *American Sociological Review*, *44*(4), 588–608.

Felson, M. (1986). *Routine Activities, Social Controls, Rational Decisions, and Criminal Outcomes*. Springer-Verlag.

Felson, M. (1995). Those Who Discourage Crime. *Journal Crime and Place, 4*(3), 53–66.

Fitriani, Y., & Pakpahan, R. (2020). Analisa Penyalahgunaan Media Sosial untuk Penyebaran Cybercrime di Dunia Maya atau Cyberspace. *CAKRAWALA*, *20*(1), 21–27.

Mui, G., & Mailley, J. (2015). A Tale of Two Triangles: Comparing the Fraud Triangle with Criminology's Crime Triangle. *Accounting Research Journal*, *28*(1), 45–58. https://doi.org/https://doi.org/10.1108/ARJ-10-2014-0092

Nasution, A. F. (2023). *Metode Penelitian Kualitatif*. Harfa Creative.

Radiansyah, I., Rusdjan, C., & Priyadi, Y. (2016). Analisis Ancaman Phishing Dalam Layanan Online Banking. *Journal of Innovation in Business and Economics*, *7*(1). https://doi.org/https://doi.org/10.22219/jibe.vol7.no1.1-14

Sampson, R. J. (2010). Gold Standard Myths: Observations on the

Experimental Turn in Quantitative Criminology. *Journal of Quantitative Criminology*, *26*, 489–500.

Saputra, A. (2023). *Gadaikan SK Ratusan Juta, PNS Ini Malah Jadi Korban Phishing*. Detik.Com. https://news.detik.com/berita/d-6696948/gadaikan-sk-ratusan-juta-pns-ini-malah-jadi-korban-Phishing

Septiano, A. K., & Ulfatun Najicha, F. (2022). Upaya Peningkatan Rasa Nasionalisme Dengan Pendidikan Kewarganegaraan Kepada Generasi Muda Di Era Perkembangan Teknologi. *Jurnal Global Citizen: Jurnal Ilmiah Kajian Pendidikan Kewarganegaraan*, *11*(1), 63–66. https://doi.org/10.33061/jgz.v11i1.7460

Widodo. (2013). *Memerangi Cybercrime (Karakteristik, Motivasi, dan Strategi Penanganannya dalam Prespektif Kriminologi)*. Aswaja Pressindo.

Windarni, V. A., Nugraha, A. F., Ramadhani, S. T. A., & Istiqomah, D. A. (2023). Deteksi Website Phishing Menggunakan Teknik Filter Pada Model Machine Learning. *Information System Journal*, *6*(1), 39–43. https://doi.org/https://doi.org/10.24076/infosjournal.2023v6i01.1268

Yin, R. (1989). *Case Study Research: Design and Methods*. Sage.