ANALISIS PERAN POLDA DAERAH ISTIMEWA YOGYAKARTA DALAM PENGUNGKAPAN KASUS *PHISHING*

SKRIPSI

Oleh:

Maharlina Darni Purwandari

20312410

PROGRAM STUDI AKUNTANSI

FAKULTAS BISNIS DAN EKONOMIKA

UNIVERSITAS ISLAM INDONESIA

YOGYAKARTA

2024

ANALISIS PERAN POLDA DAERAH ISTIMEWA YOGYAKARTA DALAM PENGUNGKAPAN KASUS *PHISHING*

SKRIPSI

Disusun dan diajukan untuk memenuhi salah satu syarat dalam mencapai derajat Sarjana Strata-1 Program Studi Akuntansi pada Fakultas Bisnis dan Ekonomika Universitas Islam Indonesia

Oleh:

Nama: Maharlina Darni Purwandari

NIM: 20312410

PROGRAM STUDI AKUNTANSI

FAKULTAS BISNIS DAN EKONOMIKA

UNIVERSITAS ISLAM INDONESIA

YOGYAKARTA

2024

PERNYATAAN BEBAS PLAGIARISME

"Dengan ini saya menyatakan bahwa dalam skripsi ini tidak terdapat karya yang pernah diajukan untuk memperoleh gelar kesarjanaan di suatu perguruan tinggi dan sepanjang pengetahuan saya juga tidak terdapat karya atau pendapat yang pernah ditulis atau diterbitkan oleh orang lain, kecuali yang secara tertulis diacu dalam naskah ini dan disebutkan dalam referensi. Apabila di kemudian hari terbukti bahwa pernyataan ini tidak benar maka saya sanggup menerima hukuman/sanksi apapun sesuai peraturan yang berlaku."

Yogyakarta, 26 Februari 2024

Penulis,



(Maharlina Darni Purwandari)

HALAMAN PENGESAHAN

ANALISIS PERAN POLDA DAERAH ISTIMEWA YOGYAKARTA

DALAM PENGUNGKAPAN KASUS *PHISHING*

SKRIPSI

Diajukan oleh:

Nama: Maharlina Darni Purwandari

NIM: 20312410

Telah disetujui oleh Dosen Pembimbing

Pada tanggal, 23 Februari 2024

Dosen Pembimbing,



Hendi Yogi Prabowo, SE., M.For.Accy., Ph.D., CFrA, CAMS.

FAKULTAS
BISNIS DAN EKONOMIKA

Gedung Prof. Dr. Ace Partadiredja
Universitas Islam Indonesia
Condong Catur Depok Yogyakarta 55283
T. (0274) 881546, 885376
F. (0274) 882589
E. fbe@uii.ac.id
W. fbe.uii.ac.id

BERITA ACARA UJIAN TUGAS AKHIR/SKRIPSI

Bismillahirrahmanirrahim,

Pada Semester Genap 2023/2024, hari Selasa, tanggal 26 Maret 2024, Program Studi Akuntansi Fakultas Bisnis dan Ekonomika UII telah menyelenggarakan Ujian Tugas Akhir/Skripsi yang disusun oleh:

Nama	: MAHARLINA DARNI PURWANDARI
NIM	: 20312410
Judul Tugas Akhir	: Analisis Peran Polda Daerah Istimewa Yogyakarta dalam Pengungkapan Kasus Phishing
Dosen Pembimbing	: Hendi Yogi Prabowo, SE., M.ForAccy., CFra., Ph.D.

Berdasarkan hasil evaluasi Tim Dosen Penguji Tugas Akhir, maka Tugas Akhir (Skripsi) tersebut dinyatakan:

Lulus

Nilai : A

Referensi : Layak ditampilkan di Perpustakaan

Tim Penguji:

Ketua Tim : Hendi Yogi Prabowo, SE., M.ForAccy., CFra., Ph.D. .....

Anggota Tim : Rifqi Muhammad, Prof., SE., SH., M.Sc., Ph.D., SAS. .....

Yogyakarta, 26 March 2024

Ketua Program Studi Akuntansi,

Prof. Rifqi Muhammad, SE., SH., M.Sc., Ph.D., SAS
NIK. 033120104

MOTTO

"Allah SWT tidak akan membebani seseorang hamba melainkan sesuai dengan kemampuannya."

(Q.S. Al-Baqarah: 286)

"Sesungguhnya bersama kesulitan itu ada kemudahan, maka apabila kamu telah selesai (dari suatu urusan), tetaplah bekerja keras (untuk urusan yang lain)."

(Q.S. Al-Insyirah: 6-7)

"Saya pikir setiap orang memiliki kekuatannya masing-masing dan mereka bersinar dengan cara yang berbeda. Semua orang Istimewa."

(Lee Jeno)

"Jangan takut. Itu tidak akan membuatmu mati. Tidak apa-apa semua akan baik-baik saja."

(Hamada Asahi)

HALAMAN PERSEMBAHAN



Skripsi ini didedikasikan untuk kedua orang tua saya yang menyayangi dan mencintai saya dengan sepenuh hati. Ayah Alm.Sudarwanto, Kakek Suroto dan Nenek Ristya Bekti Djaya, Seluruh Keluarga dan Sahabat-Sahabatku.

KATA PENGANTAR



Assalamu'alaikum Warahmatullahi Wabarakatuh...

Segala puji dan syukur penulis panjatkan kehadirat Allah SWT yang telah melimpahkan segala rahmat-Nya serta kepada Nabi kita Muhammad Shallallahu'alaihi wa sallam, atas nikmat-Nya sehingga penulis dapat menyelesaikan skripsi yang berjudul **"ANALISIS PERAN POLDA DAERAH ISTIMEWA YOGYAKARTA DALAM PENGUNGKAPAN KASUS *PHISHING*"**.

Penulisan skripsi ini dilaksanakan sebagai syarat untuk mencapai Pendidikan Strata Satu (S1) pada Jurusan Akuntansi Fakultas Bisnis dan Ekonomika Universitas Islam Indonesia.

Dalam penyusunan skripsi ini, penulis ingin menyampaikan rasa terima kasih kepada semua pihak yang telah memberikan dukungan, bimbingan, dan arahan. Oleh karena itu, penulis ingin mengucapkan terima kasih kepada:

1. Allah SWT, karena atas limpahan rahmat, karunia-Nya dan hidayah-Nya, penulis memiliki kesempatan untuk menyelesaikan skripsi ini dengan baik.
2. Nabi Muhammad SAW, yang senantiasa memberikan inspirasi dan petunjuk dalam kehidupan.
3. Bapak Prof. Fathul Wahid, S.T., M.Sc., Ph.D., Rektor Universitas Islam Indonesia.

4. Bapak Johan Arifin S.E., M.Si., Ph.D., Dekan Fakultas Bisnis dan Ekonomika.
5. Bapak Dekar Urumsah, SE., S.Si., M.Com (IS)., Ph.D., Ketua Jurusan Akuntansi.
6. Bapak Prof. Rifqi Muhammad, S.E., S.H., M.Sc., Ph.D., Ketua Program Studi Akuntansi.
7. Bapak Hendi Yogi Prabowo, SE., M.For.Accy., Ph.D., CFrA., CAMS, dosen pembimbing yang memberikan waktu, arahan dan bimbingan yang luar biasa, sehingga penulis dapat menyelesaikan penelitian ini dengan baik.
8. Polda Daerah Istimewa Yogyakarta, khususnya Ditreskrimsus Unit V Siber, yang telah membantu dan menjadi objek penelitian dalam penulisan skripsi.
9. Keluarga tercinta, terutama kepada kakek Suroto dan Nenek Ristya Bekti Djaya. Serta kedua adik, Marcella Aulia Putri dan Naima Trivalencia Rahmawati. Tante Widhi Sulistyaning Ratri dan adek sepupu Maudy Adiba Rachman yang selalu memberikan semangat yang luar biasa kepada penulis, serta kepada keluarga besar yang sudah memberikan dukungan dan doa kepada penulis.
10. Ayahku tercinta alm. Sudarwanto, Buyut almh. Mukariyah dan sahabatku almh. Olga Renada Iktarani. Alhamdulillah kini penulis sudah berada di tahap menyelesaikan skripsi. Terimakasih sudah mengantarkan penulis di tempat ini. *You are forever in my heart. Until we meet again.*

11. Sahabat kuliah penulis anggota grup the konco "Yuas, Septi, Aviyah, Riyan, Faisal, Helga, Bima, Yanuar" yang selalu memberikan dukungan dan semangat dalam mengerjakan skripsi.
12. Kepada seluruh anggota Tim basketball Universitas Islam Indonesia yang selalu memberikan dukungan dan semangat dalam perjalanan kuliah penulis. Dedikasi dan kebersamaan kalian telah menjadi inspirasi yang luar biasa
13. Bapung, Raya, dan Erin yang telah memberikan dukungan, pengalaman dan selalu menjadi tempat cerita penulis selama di Yogyakarta.
14. Teman-teman KKN 255 Becerez yang selalu mendukung apapun yang penulis lakukan.
15. Sahabat lama penulis. Destiara Nurlisya Rahayu, Adella Dwike Elsya Putriana, Jony Wahyu Ibrahim, Ferdy Hahan Pradana, Aling Martha Cahyani dan Wine Eka Kusuma yang selalu menyambut penulis dengan hangat dan memberikan dukungannya selama penulis mengerjakan skripsi.
16. Seluruh pihak yang terlibat secara langsung maupun tidak langsung, yang memberikan doa dan dukungan.
17. *Tiktok* dan *Instagram*, yang memberikan informasi dalam penyelesaian skripsi.
18. NCT Dream, TXT, dan Treasure, yang lagunya menemani proses penulisan.
19. Diri sendiri yang tak pernah menyerah dalam menyelesaikan skripsi ini. Terimakasih sudah melakukan yang terbaik.

Dalam penyusunan skripsi ini, penulis sadar akan masih banyak kekurangan yang ada. Kritik dan saran yang membangun sangat penulis harapkan agar skripsi ini dapat menjadi lebih baik dan bermanfaat bagi pembaca dan pihak-pihak yang berkepentingan.

Wassalamu'alaikum Warahmatullahi Wabarakatuh…

Yogyakarta, 23 Februari 2024

Peneliti

(Maharlina Darni Purwandari)

DAFTAR ISI

HALAMAN SAMPUL.....**i**

HALAMAN JUDUL.....**ii**

HALAMAN PERNYATAAN BEBAS PLAGIARISME.....**iii**

HALAMAN PENGESAHAN.....**iv**

HALAMAN BERITA ACARA UJIAN SKRIPSI..... **v**

MOTTO..... **vi**

HALAMAN PERSEMBAHAN..... **vii**

KATA PENGANTAR.....**viii**

DAFTAR ISI.....**xii**

DAFTAR TABEL.....**xvi**

DAFTAR GAMBAR.....**xvii**

DAFTAR LAMPIRAN.....**xviii**

ABSTRAK..... **xix**

ABSTRACT..... **xx**

BAB I PENDAHULUAN.....**1**

1. 1 Latar Belakang..... 1

1. 2 Rumusan Masalah..... 8

1. 3 Fokus Penelitian..... 10

1. 4 Tujuan Penelitian.....10

1. 5 Manfaat Penelitian.....11

1. 6 Sistematika Penulisan.....11

BAB II KAJIAN PUSTAKA.....**13**

2. 1 Pengenalan Bab..... 13

2. 2 Kejahatan.....13

2. 2. 1 Tipe-Tipe Kejahatan..... 14

2. 3 Penipuan (*Fraud*)..... 15
2. 3. 1 Jenis-Jenis *Fraud*.....15
2. 4 Segitiga Kejahatan.....16
2. 5 *Cybercrime*..... 21
2. 5. 1 Jenis-Jenis Kejahatan *Cybercrime*.....21
2. 6 *Phishing*.....23
2. 6. 1 Teknik *Phishing*.....24
2. 6. 2 *Network Forencics*.....25
2. 6. 3 *Network Protocol Analyzer*.....27
2. 7 Kepolisian.....28
2. 7. 1 Fungsi Kepolisian.....29
2. 7. 2 Tugas Kepolisian..... 29
2. 7. 3 Wewenang Kepolisian..... 30
2. 8 Informasi dan Transaksi Elektronik..... 32
2. 8. 1 Penipuan Informasi dan Transaksi Elektronik (ITE).....35
2. 9 Penelitian Terdahulu.....36
BAB III METODE PENELITIAN.....42
3. 1 Pengenalan Bab..... 42
3. 2 Jenis Penelitian..... 42
3. 3 Objek Penelitian..... 44
3. 4 Fokus Penelitian..... 44
3. 5 Sistematika Penelitian..... 45
3. 5. 1 Sumber Data Primer..... 48
3. 5. 2 Sumber Data Sekunder.....49
3. 6 Teknik Analisa Data..... 50
3. 6. 1 Reduksi Data *(Data Reduction)*.....50
3. 6. 2 Tampilan Data *(Data Display)*..... 53

3. 6. 3 Menarik Kesimpulan dan Verifikasi *(Conclusion and Verification)* 54

3. 7 Pengujian Keabsahan Data.....55

BAB IV HASIL DAN PEMBAHASAN.....58

4. 1 Pengenalan Bab.....58

4. 2 Gambaran Umum Ditreskrimsus Polda Daerah Istimewa Yogyakarta..58

4. 2. 2 Tugas Subdit V Siber Polda Daerah Istimewa Yogyakarta.....61

4. 2. 3 Visi dan Misi Ditreskrimsus Polda Daerah Istimewa Yogyakarta.....62

4. 2. 4 Arti Lambang Ditreskrimsus Polda Daerah Istimewa Yogyakarta 64

4. 3 Tren Permasalahan Kasus *Phishing* di Wilayah DIY.....66

4. 3. 1 Jenis Kejahatan Siber di Polda Daerah Istimewa Yogyakarta.....70

4. 3. 2 The *Crime* Triangle.....72

4. 4 Mekanisme Pengungkapan Polda DIY terhadap Kasus *Phishing* di Wilayah Daerah Istimewa Yogyakarta.....81

4. 4. 1 Pengaduan.....84

4. 4. 2 Penyelidikan.....90

4. 4. 3 Penyidikan.....95

4. 5 Kekurangan dan Kendala yang Dihadapi Polda DIY dalam Pengungkapan Kasus *Phishing* di Daerah Istimewa Yogyakarta.....109

4. 5. 1 Kekurangan.....111

4. 5. 2 Kendala.....112

4. 6 Perbaikan yang Dapat Dilakukan Polda DIY dalam Pengungkapan Kasus *Phishing* di Wilayah Daerah Istimewa Yogyakarta.....115

4. 7 Kesimpulan Bab.....119

BAB V KESIMPULAN DAN SARAN.....121

5. 1 Pengenalan Bab..... 121

5. 2 Kesimpulan.....121

5. 3 Implikasi Penelitian..... 124

5. 4 Keterbatasan Penelitian..... 124

5. 5 Saran..... 125

5. 5. 1 Polda Daerah Istimewa Yogyakarta.....125

5. 5. 2 Masyarakat.....125

5. 5. 3 Penelitian Selanjutnya..... 126

DAFTAR PUSTAKA..... 127

LAMPIRAN..... 131

DAFTAR TABEL

Tabel 3.1 Profil Narasumber..... 49

DAFTAR GAMBAR

Gambar 1.1 Grafik Data Pengguna Sosial Media Tahun 2022.....3

Gambar 1.2 Grafik Data Serangan Siber di Indonesia Selama Tahun 2022.....5

Gambar 1.3 Grafik Data Persebaran Serangan *Phishing* di Indonesia Berdasarkan Sektor (Kuartal II, 2022).....6

Gambar 2.1 Segitiga Kejahatan **(**Sumber: Sampson, 2010).....18

Gambar 2.2 Proses Forensik (Sumber: Windarni et al., 2023)..... 25

Gambar 3.1 Langkah-Langkah Penelitian.....46

Gambar 4.1 Struktur Ditreskrimsus Polda DIY (Polda DIY, 2024).....60

Gambar 4.2 Arti Lambang Ditreskrimsus Polda DIY (Polda DIY, 2024)..... 66

Gambar 4.3 Grafik Jumlah Kasus dalam Laporan Polisi di Subdit V Siber Polda DIY Tahun 2019-2023..... 67

Gambar 4.4 Peta Analisa Tren Permasalahan Kasus *Phishing*.....69

Gambar 4.5 Peta Analisis Mekanisme Pengungkapan Polda DIY Terhadap Kasus *Phishing* di Wilayah Daerah Istimewa Yogyakarta.....83

Gambar 4.6 Peta Analisa Kekurangan dan Kendala yang Dihadapi oleh Polda DIY dalam Pengungkapan Kasus *Phishing*.....110

Gambar 4.6 Peta Analisa Kendala dan Perbaikan yang dilakukan oleh Polda DIY dalam Pengungkapan Kasus *Phishing*.....116

DAFTAR LAMPIRAN

Lampiran 1 Surat Izin Penelitian..... 132

Lampiran 2 Transkip Wawancara : Bapak Budi Cahyono Desember.....133

Lampiran 3 Transkip Wawancara : Bapak Muhammad Robani Desember.... 143

Lampiran 4 Transkip Wawancara : Bapak Riski Praditya Putra Desember....152

Lampiran 5 Transkip Wawancara : Bapak Riski Praditya Putra Januari..... 158

Lampiran 6 Peraturan-Peraturan Terkait.....162

Lampiran 7 *Framework* Matrices Permasalahan *Phishing* POLDA DIY.....169

Lampiran 8 *Framework* Matrices Mekanisme Pengungkapan Kasus *Phishing* POLDA DIY.....176

Lampiran 9 *Framework* Matrices Kekurangan yang dihadapi Polda DIY terhadap Kasus *Phishing* di wilayah DIY.....183

Lampiran 10 *Framework* Matrices Kendala yang dihadapi Polda DIY terhadap Kasus *Phishing* di wilayah DIY..... 184

Lampiran 11 *Framework* Matrices Perbaikan yang dilakukan Oleh Polda DIY terhadap Kasus *Phishing* di wilayah DIY.....188

Lampiran 12 Pedoman Wawancara Tidak Terstruktur (Polda DIY)..... 190

ABSTRAK

Penelitian ini menganalisis peran Polda Daerah Istimewa Yogyakarta dalam mengungkap kasus *Phishing*. Temuan menunjukkan tren peningkatan kasus *Phishing* terutama terkait UU ITE, dengan pelaku yang semakin canggih dalam menipu dan mencuri informasi pribadi melalui *email*, situs web palsu, dan pesan teks berbahaya. Mayoritas kasus terjadi secara *online* melalui media sosial seperti *email*, *Facebook*, dan *Instagram*, meningkatkan risiko pencurian data karena banyak korban tidak memahami tanda-tanda *Phishing*. Mekanisme pengungkapan kasus *Phishing* melibatkan pengaduan, penyelidikan, dan penyidikan. Kendala utama termasuk kesulitan dalam penangkapan pelaku, kurangnya pengolahan pengaduan, dan kesulitan identifikasi pelaku serta akses terhadap informasi perbankan. Polda DIY melakukan langkah-langkah strategis seperti sosialisasi, kerjasama dengan pihak bank, dan kolaborasi dengan media sosial dan Kementerian Komunikasi dan Informatika untuk meningkatkan kesadaran masyarakat, memperkuat penindakan terhadap pelaku kejahatan siber, dan menciptakan lingkungan yang lebih aman di ranah digital.

Kata kunci: *Phishing*, Polda Daerah Istimewa Yogyakarta, Mekanisme Pengungkapan, Kendala, Perbaikan

ABSTRACT

This research analyzes the role of the Yogyakarta Special Region Police in uncovering Phishing cases. Findings indicate a significant increase in Phishing cases, particularly related to the ITE Law, with perpetrators becoming increasingly sophisticated in deceiving and stealing personal information through email, fake websites, and harmful text messages. The majority of cases occur online through social media such as email, Facebook, and Instagram, increasing the risk of data theft as many victims do not understand the signs of Phishing. The mechanism of uncovering Phishing cases involves reporting, investigation, and prosecution. Main challenges include difficulties in apprehending perpetrators, lack of complaint processing, and difficulty in identifying perpetrators as well as access to banking information. Polda DIY takes strategic steps such as socialization, collaboration with banks, and collaboration with social media and the Ministry of Communication and Information to increase public awareness, strengthen prosecution of cybercrime perpetrators, and create a safer environment in the digital realm.

Keywords: *Phishing, Yogyakarta Special Region Police, Disclosure Mechanism, Challenges, Improvement*

BAB I

PENDAHULUAN

1. 1 Latar Belakang

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 kita. Mulai dari cara kita berinteraksi sosial hingga cara berpikir kita, 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.

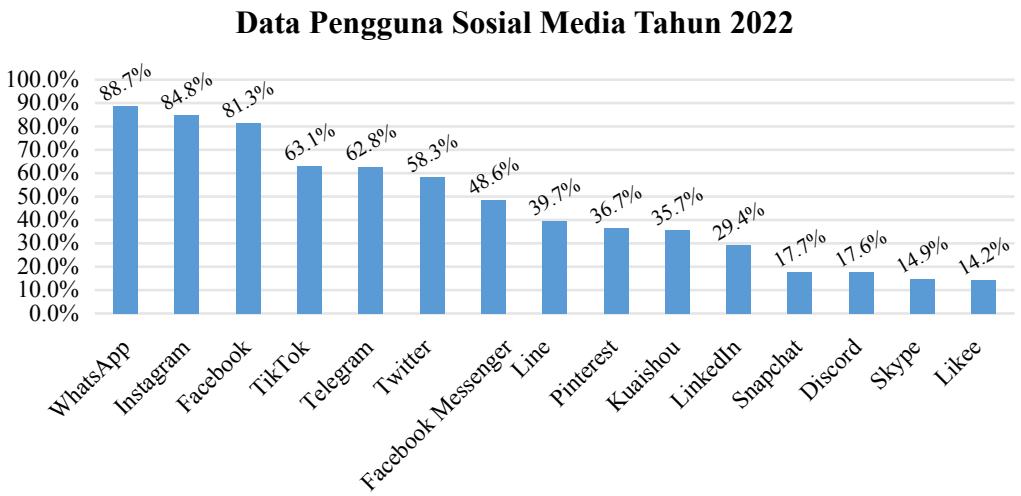
Media sosial adalah aplikasi berbasis internet yang memungkinkan pengguna untuk berkomunikasi dengan orang lain serta sebagai sumber informasi (Pratama & Sari, 2020) . Penggunaan media sosial mencakup beragam bidang

seperti kesehatan, olahraga, ekonomi, politik, hukum, dan lain sebagainya (Ramadani et al., 2020).

Beragam jenis media sosial hadir untuk memfasilitasi komunikasi, pertukaran informasi, dan aktivitas lainnya. Jaringan sosial seperti *Facebook*, *Twitter*, dan *LinkedIn* memungkinkan pengguna untuk terhubung dengan orang lain dan berbagi pesan, foto, video, serta informasi lainnya. Selain itu, terdapat juga aplikasi media berbagi video seperti *YouTube* dan *Tiktok* yang memungkinkan pengguna untuk mengunggah, menonton, dan berinteraksi dengan video dari pengguna lain.

Aplikasi berbagi foto seperti *Instagram* dan *Pinterest* memfasilitasi pengguna dalam memposting, menyimpan, serta berbagi foto dan konten visual lainnya. Ada pula aplikasi blog, seperti *Twitter* yang memungkinkan pengguna untuk menulis, mempublikasikan, dan berbagi konten dalam berbagai bentuk, mulai dari artikel hingga pesan singkat. Media sosial juga mencakup forum diskusi seperti *Quora*, di mana pengguna dapat bergabung dalam percakapan, mendiskusikan topik tertentu, dan bertukar informasi.

Aplikasi pesan instan seperti *WhatsApp, Messenger*, atau *Telegram* memfasilitasi komunikasi satu lawan satu atau dalam grup melalui pesan teks, suara, atau video. Sementara aplikasi berbagi konten profesional seperti *LinkedIn* difokuskan pada koneksi profesional, pengembangan karier, dan pertukaran informasi terkait pekerjaan.



Sumber: Laily et al., 2023

Gambar 1.1 Grafik Data Pengguna Sosial Media Tahun 2022

Berdasarkan data yang telah dipaparkan sebelumnya, terlihat bahwa *Instagram* memiliki proporsi pengguna sebesar 84,8% di Indonesia. Fakta ini menunjukkan bahwa *Instagram* adalah *platform* media sosial yang paling populer di kalangan masyarakat Indonesia, selain *WhatsApp* yang mencatat pengguna sebanyak 88,7%. Kemudahan penggunaan *Instagram*, baik bagi remaja, dewasa, maupun pelajar, terlihat dari antarmuka yang mudah dipahami. Akses ke *Instagram* dapat dilakukan melalui berbagai perangkat, termasuk *smartphone*, komputer, dan laptop, sehingga memungkinkan pengguna untuk terhubung kapan saja dan di mana saja.

Di tahun 2017, jumlah pengguna internet mencapai 143,26 juta dan terus meningkat menjadi 171,17 juta pada tahun 2018 (Asosiasi Penyelenggara Jasa Internet Indonesia, 2018) . Pertumbuhan yang signifikan ini menandai potensi besar dari para pengguna internet dalam menggunakan media sosial atau jejaring

sosial. Berdasarkan data dari Hootsuite tahun 2019, terdapat sekitar 150 juta pengguna media sosial aktif di Indonesia, yang mengalami peningkatan sebesar 15% dari tahun sebelumnya, sementara pengguna media sosial melalui perangkat *mobile* mencapai 130 juta, naik sebesar 8,3% (Riyanto, 2019).

Sisi positif dari keberadaan dunia maya ini 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 Andi Hamzah sebagaimana yang dijelaskan dalam (Antoni, 2017), *cybercrime* adalah bentuk kejahatan yang berkaitan dengan penggunaan komputer secara ilegal. 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.

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.



Sumber: Hanadian, 2023

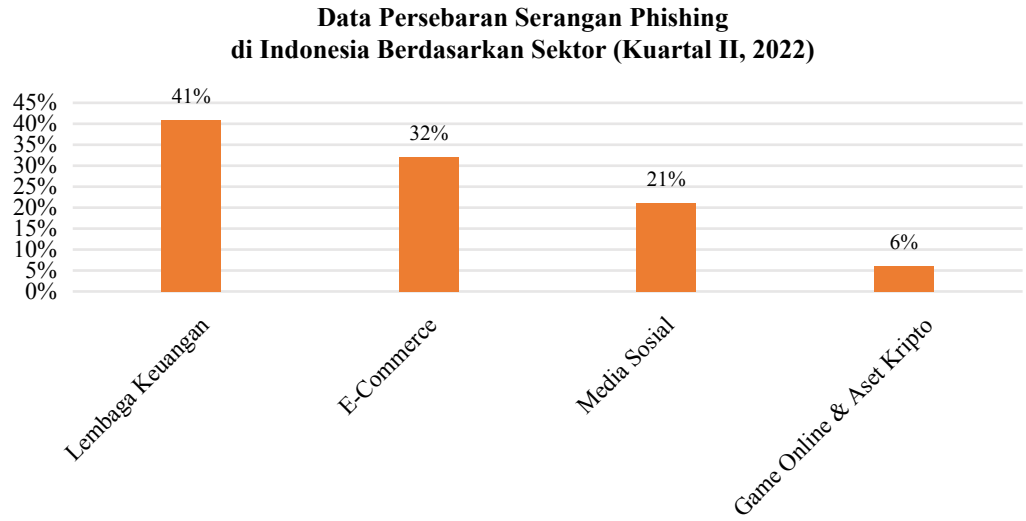
Gambar 1.2 Grafik Data Serangan Siber di Indonesia Selama Tahun 2022

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, 2017b). 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).



Sumber: Annur, 2022

Gambar 1.3 Grafik Data Persebaran Serangan *Phishing* di Indonesia Berdasarkan Sektor (Kuartal II, 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.

Dengan latar belakang tersebut, peneliti melihat relevansi dan urgensi untuk mengangkat topik penelitian mengenai **"Analisis Peran 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. Upaya ini diharapkan dapat memberikan kontribusi positif dalam meningkatkan keamanan masyarakat dalam beraktivitas daring di Daerah Istimewa Yogyakarta.

1. 2 Rumusan Masalah

Berdasarkan latar belakang diatas, rumusan masalah yang dapat diidentifikasi dalam penelitian ini adalah sebagai berikut:

1. Bagaimana tren permasalahan *Phishing* di wilayah Daerah Istimewa Yogyakarta?

Dalam hal ini, peneliti telah mengenali kasus-kasus yang terjadi di Polda DIY, termasuk pemahaman terhadap berbagai jenis kasus siber yang ditangani oleh Subdit V Siber Polda DIY. Tren penipuan *Phishing* terkait dengan teori *crime triangle*, yang mencakup *target* (korban), *offender* (pelaku), dan *place* (tempat), telah diidentifikasi oleh peneliti.

2. Bagaimana mekanisme pengungkapan Polda DIY terhadap kasus *Phishing* di wilayah Daerah Istimewa Yogyakarta?

   Dalam hal ini, peneliti telah memperoleh pemahaman mengenai keputusan yang diambil oleh Polda DIY dalam menyelidiki kasus *Phishing* di wilayah Daerah Istimewa Yogyakarta. Selain itu, peneliti juga mengetahui metode, prosedur, serta kebijakan yang diterapkan oleh Polda DIY dalam mengungkap kasus atau menangani situasi terkait *Phishing* di wilayah Daerah Istimewa Yogyakarta.

3. Apa kendala yang dihadapi oleh Polda DIY dalam pengungkapan kasus *Phishing* di wilayah Daerah Istimewa Yogyakarta?

   Dalam hal ini, peneliti telah mengamati kekurangan dan kendala yang dihadapi oleh Polda DIY dalam mengungkap kasus *Phishing* di Daerah Istimewa Yogyakarta. Hal ini disebabkan oleh kesulitan dalam menyelesaikan masalah tanpa bukti konkret atau fakta yang ditemukan oleh penyelidik.

4. Perbaikan apa yang dapat dilakukan Polda DIY dalam pengungkapan kasus *Phishing* di wilayah Daerah Istimewa Yogyakarta?

Dalam hal ini, peneliti telah mengidentifikasi perbaikan yang perlu dilakukan oleh Kepolisian Daerah Istimewa Yogyakarta (Polda DIY) dalam mengembangkan gagasan-gagasan yang efektif untuk mengungkap kasus *Phishing* di wilayah tersebut.

1. 3 Fokus Penelitian

Fokus penelitian atau inti dari yang diteliti, mencakup penjelasan mengenai dimensi mana yang menjadi pusat perhatian penelitian, dan topik ini dibahas tuntas secara komprehensif dan menyeluruh. Fokus penelitian dalam penelitian ini adalah:

1. Tempat Penelitian: Kepolisian Daerah (Polda) DI Yogyakarta. Direktorat Reserse Kriminal Khusus (DITRESKRIMSUS). Unit V Siber. Jl. Ring Road Utara, Depok, Sleman, Condongcatur, Kec. Depok, Yogyakarta, Kota Yogyakarta, Daerah Istimewa Yogyakarta.
2. Aspek Penelitian: Mengenai analisis peran Polda Daerah Istimewa Yogyakarta dalam pengungkapan kasus *Phishing*.
3. Metode Penelitian: Menggunakan metode penelitian kualitatif.

1. 4 Tujuan Penelitian

Tujuan penelitian ini adalah:

1. Mengetahui tentang Tren permasalahan *Phishing* di wilayah Daerah Istimewa Yogyakarta tahun 2019-2023.
2. Mengetahui mekanisme pengungkapan Polda DIY terhadap kasus *Phishing* di wilayah Daerah Istimewa Yogyakarta.

3. Mengetahui kendala yang dihadapi oleh Polda DIY dalam pengungkapan kasus *Phishing* di wilayah Daerah Istimewa Yogyakarta.
4. Mengetahui perbaikan yang dilakukan Polda DIY dalam pengungkapan kasus *Phishing* di wilayah Daerah Istimewa Yogyakarta.

1. 5 Manfaat Penelitian

Hasil dari penelitian studi empiris yang dilakukan oleh penelitian ini diharapkan dapat memberikan setidaknya manfaat sebagai berikut:

1. Bagi kalangan akademis dan berbagai pihak, diharapkan dapat menggunakan hasil penelitian ini sebagai referensi untuk mengembangkan penelitian dalam konteks serupa atau kajian yang terkait langsung dengan analisis peran Polda Daerah Istimewa Yogyakarta dalam mengungkap kasus *Phishing*.
2. Bagi objek penelitian di Polda Daerah Istimewa Yogyakarta, diharapkan dapat memanfaatkan hasil penelitian ini sebagai referensi untuk mengembangkan upaya pengungkapan kasus *Phishing*, sehingga kejahatan se*Mac*am itu dapat diminimalkan atau dihindarkan.
3. Bagi penulis, diharapkan bahwa penelitian ini dapat memberikan kontribusi dengan memperkaya dan meningkatkan pemahaman, pengetahuan, dan wawasan tentang analisis peran Polda Daerah Istimewa Yogyakarta dalam mengungkap kasus *Phishing*.

1. 6 Sistematika Penulisan

Penulisan laporan penelitian ini akan mengikuti format sebagai berikut:

BAB I PENDAHULUAN

Pada bab ini, penulis menjelaskan mengenai latar belakang masalah, rumusan masalah, fokus penelitian, tujuan penelitian, manfaat penelitian, dan sistematika penulisan laporan.

BAB II KAJIAN PUSTAKA

Pada bab ini, penulis menjelaskan teori yang relevan dengan topik penelitian. Selain itu, juga akan diidentifikasi studi empiris yang telah dilakukan sebelumnya mengenai topik yang sama dengan penelitian ini.

BAB III METODE PENELITIAN

Pada bab ini, penulis menjelaskan desain dan tahapan penelitian, jenis penelitian, objek penelitian, instrumen penelitian, jenis data, sumber data, teknik pengumpulan data, pengujian keabsahan data, serta teknik analisis data yang digunakan dalam penelitian.

BAB IV ANALISIS DATA DAN PEMBAHASAN

Pada bab ini, penulis menjelaskan hasil analisis data yang berasal dari observasi di tempat penelitian, seperti informasi yang terkumpul dan data hasil wawancara mengenai gambaran umum analisis peran Polda Daerah Istimewa Yogyakarta dalam mengungkap kasus *Phishing*.

BAB V KESIMPULAN DAN SARAN

Pada bab ini, penulis menjelaskan kesimpulan yang diperoleh dari analisis hasil pada bab-bab terkait, termasuk keterbatasan penelitian, dan memberikan saran untuk penelitian selanjutnya.

BAB II

KAJIAN PUSTAKA

2. 1 Pengenalan Bab

Bab ini akan menjelaskan teori-teori yang menjadi dasar dalam merencanakan penelitian, khususnya terkait dengan topik *Phishing*. Penulis mengadopsi Tinjauan Pustaka sebagai landasan teoritis untuk merumuskan pertanyaan penelitian yang akan dijawab selama studi ini berlangsung. Tinjauan Pustaka ini terkumpul dari berbagai sumber, termasuk buku, artikel, dan penelitian terdahulu yang relevan dengan topik penelitian ini. Di dalamnya, tercakup teori, definisi, serta tinjauan atas penelitian sebelumnya tentang praktek *Phishing*, upaya penanggulangan oleh kepolisian, dan strategi pengungkapan.

2. 2 Kejahatan

Kejahatan sering diartikan sebagai tindakan yang melanggar aturan hukum dan dapat mengakibatkan seseorang dikenai hukuman. Kejahatan dapat terjadi baik secara langsung maupun tidak langsung, termasuk kelalaian yang bisa menghasilkan sanksi hukum. Dalam perspektif hukum, kejahatan terlihat sebagai tindakan aktif di mana manusia melanggar hukum. Namun, "tidak berperilaku" pun dapat dianggap sebagai bentuk kejahatan, seperti penelantaran anak atau ketidak laporan pada pihak berwenang saat mengetahui tindakan kekerasan terhadap anak di sekitar kita. Dari sudut pandang moral, perilaku dianggap kejahatan hanya jika memenuhi dua faktor:

1. *mens rea* (niat melakukan perilaku), dan

2. *actus reus* (perilaku terlaksana tanpa paksaan dari orang lain).

Sebagai contoh, pembunuhan dianggap kejahatan ketika pelaku memiliki niat untuk mengambil nyawa orang lain dan pelaksanaan perbuatannya adalah hasil ide dan tindakan sendiri tanpa paksaan. Jika pelaku memiliki gangguan mental yang menyebabkan niatnya terjadi di luar kesadaran, seperti kejahatan yang terjadi saat tidur atau dalam keadaan tidak sadar, faktor mens rea dianggap tidak lengkap. Dalam kasus ini, sulit untuk dengan tegas menyatakan sebagai kejahatan, karena individu dengan gangguan mental tidak dapat dimintai pertanggungjawaban penuh atas tindakannya

2. 2. 1 Tipe-Tipe Kejahatan

(Light et al., 1989) membedakan tipe kejahatan dibagi menjadi 4, yaitu:

1. Kejahatan Tanpa Korban (*Crimes Without Victims)*

   Jenis kejahatan ini mencakup aktivitas seperti perjudian, penyalahgunaan narkoba, konsumsi minuman beralkohol hingga mabuk, serta hubungan seksual yang melanggar hukum.

2. Kejahatan Terorganisasi (*Organized Crimes)*

   Jenis kejahatan yang dilakukan dengan tujuan memperoleh keuntungan atau kekuasaan dengan melanggar hukum, contohnya, pengiriman tenaga kerja Indonesia ke luar negeri secara ilegal.

3. Kejahatan yang dilakukan oleh orang yang statusnya tinggi (*White-Collar Crimes)*

Kejahatan jenis ini melibatkan individu-individu yang memiliki status sosial yang tinggi, seperti kasus korupsi yang dilakukan oleh pejabat pemerintahan atau pengusaha terkemuka.

4. Kejahatan atas nama perusahaan (*Corporate crimes*)

   Kejahatan ini dilakukan atas nama organisasi formal dengan tujuan meningkatkan keuntungan atau mengurangi kerugian. Bentuk-bentuknya termasuk kejahatan terhadap konsumen, publik, pemilik perusahaan, dan karyawan.

2. 3 Penipuan (*Fraud*)

Fraud (penipuan), menurut (Handoyo, 2016) merupakan istilah generik dan mencakup beragam kecerdasan manusia yang dapat merencanakan, yang diambil oleh individu untuk mendapatkan keuntungan lebih dari (pihak) yang lain dengan cara yang tidak benar.

2. 3. 1 Jenis-Jenis *Fraud*

Menurut (Handoyo, 2016) sebagian besar penipuan atas nama organisasi dilakukan oleh manajer tingkat atas, terutama dalam hal laporan keuangan. Fraud biasanya dibagi menjadi 2 jenis, yaitu:

1. *Fraud* melawan organisasi

   Orang yang bekerja atau tidak bekerja untuk organisasi, melakukan kejahatan secara individu maupun secara kolektif terhadap organisasi dan menempatkan organisai sebagai korban. Dalam kebanyakan kasus, harta yang diambil oleh anggota organisasi melalui pencurian atau penggelapan. Hal ini menunjukkan bahwa pelaku memilliki kesempatan untuk melakukan penipuan.

2. *Fraud* atas nama Perusahaan

Orang yang bertanggung jawab atas transaksi atau pengambilan keputusan biasanya melakukan penipuan atas nama perusahaan. Orang-orang yang melakukan penipuan ini biasanya memiliki dua mata pisau yang tajam. Di satu sisi orang tersebut akan berusaha mengatasnamakan penyelamatan organisasi dan di sisi lain, orang tersebut juga akan mempertimbangkan untuk mengambil keuntungan dari tindakannya.

2. 4 Segitiga Kejahatan

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, 2015a).

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.

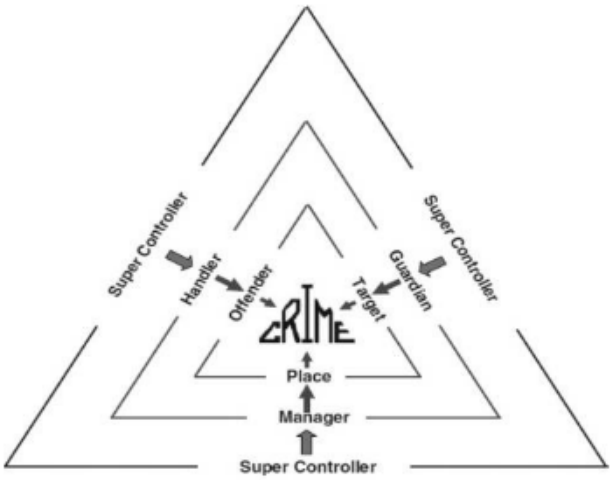
Dalam jurnal (Mui & Mailley, 2015b) , Segitiga Kejahatan diusulkan sebagai pelengkap bagi Segitiga Penipuan dalam memahami peristiwa penipuan. Dengan menerapkan teori ini pada kasus penyalahgunaan aset, dapat memberikan pandangan menyeluruh mengenai peristiwa penipuan dengan mempertimbangkan lingkungan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



Gambar 2.1 Segitiga Kejahatan **(**Sumber: (Sampson, 2010))

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,
3. dan lokasi terjadinya kejahatan.

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.

2. 5 *Cybercrime*

Pengertian *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.

Cybercrime adalah tindakan criminal yang dilakukan dengan menggunakan teknologi computer, mencakup semua bentuk tindakan criminal yang terjadi di dalam dunia maya.

2. 5. 1 Jenis-Jenis Kejahatan *Cybercrime*

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)

   Illegal access merupakan tindakan kriminal yang terjadi dengan cara melintasi atau memasuki suatu jaringan komputer tanpa izin atau pengetahuan dari pemiliknya. Hal ini melibatkan penetrasi ke dalam sistem komputer secara tidak sah atau tanpa persetujuan yang dibutuhkan dari pemilik jaringan komputer yang diakses.

2. ***Illegal Contents***

Illegal contents merupakan 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***

Data forgery merupakan 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*. Tindakan kriminal ini biasanya ditujukan pada dokumen-dokumen terkait *e-commerce* dengan menciptakan kesan kesalahan pengetikan yang pada akhirnya akan memberi keuntungan kepada pelaku. Tujuannya adalah agar korban memasukkan informasi pribadi dan nomor kartu kredit yang nantinya diduga akan disalahgunakan oleh pelaku kejahatan.

4. ***Cyber Espionage (Spionase Cyber)***

Cyber espionage 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)

Jenis kejahatan ini umumnya dilakukan dengan cara mengganggu, merusak, atau menghancurkan data, program komputer, atau sistem jaringan komputer yang terhubung ke internet. Biasanya, tindakan kejahatan ini

dilakukan dengan cara menyusupkan logic bomb, virus komputer, atau program tertentu sehingga menyebabkan data, program komputer, atau sistem jaringan komputer menjadi tidak dapat digunakan atau tidak beroperasi seperti semestinya. Terkadang, hal ini dapat mengakibatkan kontrol yang dimiliki oleh pelaku kejahatan terhadap sistem yang terkena dampak.

6. ***Offense Against Intellectual Property*** (Pelangganran Atas Hak Kekayaan Intelektual

   Jenis kejahatan ini bertujuan untuk melanggar hak atas kekayaan intelektual yang dimiliki oleh pihak lain di internet. Sebagai contoh, tindakan meniru atau meng-*copy* tampilan suatu halaman web dari situs orang lain secara ilegal.

7. ***Infringements of Privacy*** (*Infringements Privasi)*

   Tindakan kejahatan ini bertujuan untuk memperoleh informasi pribadi seseorang yang disimpan dalam formulir data pribadi yang terkomputerisasi. Jika informasi tersebut diketahui oleh pihak lain, hal itu dapat menyebabkan kerugian bagi korban baik secara materiil maupun immateriil, seperti kebocoran nomor kartu kredit, nomor PIN ATM, dan informasi pribadi lainnya.

2. 6 *Phishing*

Sebelumnya, peneliti akan menjelaskan tentang *Phishing*, sebuah tindakan dengan menggunakan rekayasa sosial sebagaimana yang dijelaskan oleh (Windarni et al., 2023a) . *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.

2. 6. 1 Teknik *Phishing*

Menurut (Windarni et al., 2023b) Seorang *phisher* melakukan kejahatan *cyber* dengan memanfaatkan beberapa teknik tertentu, di antaranya:

1. ***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.

2. **Pengiriman Berbasis Web**

Phisher menempatkan diri di antara situs web asli dan situs palsu untuk melakukan serangan "*man-in-the-middle*".

3. **Pesan Instan *(chatting)***

Pengguna menerima pesan dengan tautan ke situs web palsu yang terlihat seperti situs resmi, membuat pengguna percaya padahal sebenarnya palsu.

4. ***Trojan hosts***

Phisher mencoba masuk ke akun pengguna untuk mencuri informasi pribadi.

5. **Manipulasi tautan (*link*)**

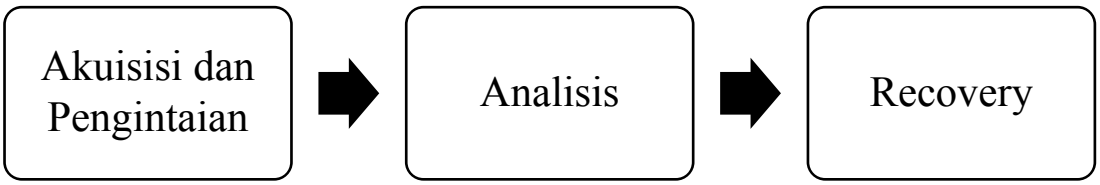
Phisher mengirim tautan ke situs web palsu yang berbeda dari yang seharusnya.

6. ***Malware Phishing***

Penggunaan malware dalam *email phisher* untuk menyerang komputer pengguna setelah mengklik tautan atau mengunduh *file*.

2. 6. 2 *Network Forencics*

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 2.2 Proses Forensik (Sumber: (Windarni et al., 2023b)

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

1. 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).

2. 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.

3. Recovery

Tahapan ini bertujuan untuk memulihkan data yang hilang akibat intrusi, terutama informasi pada disk seperti *file* atau direktori yang terpengaruh.

2. 6. 3 *Network Protocol Analyzer*

Network Protocol Analyzer menurut (Ginanjar et al., 2019) adalah alat yang digunakan untuk menganalisis paket data dalam jaringan, seperti yang dilakukan oleh *Wireshark*. *Wireshark* mampu memonitor paket data secara langsung (*real-time*), menangkap data, serta menampilkan data yang berhasil ditangkap secara komprehensif. *Wireshark* sendiri bersifat *open-source* dan dapat dijalankan pada berbagai *platform* seperti *Linux*, *Windows*, dan *Mac*. Beberapa contoh penggunaan *Wireshark* meliputi:

1. Menyelesaikan masalah-masalah jaringan.
2. Melakukan uji coba keamanan jaringan.
3. Mendeteksi kesalahan dalam implementasi protokol.
4. Mempelajari protokol jaringan.

Wireshark juga dapat digunakan untuk mengambil informasi sensitif seperti kata sandi, *cookie*, dan lain sebagainya dari jaringan. Beberapa fitur utama dari *Wireshark* meliputi:

1. Tersedia untuk *platform UNIX*, *Linux*, *Windows*, dan *Mac*.
2. Mampu menangkap paket data jaringan secara real-time.

3. Menampilkan informasi protokol secara lengkap.
4. Kemampuan untuk menyimpan data paket dalam *file* yang dapat dibuka kembali jika diperlukan.
5. Filtering paket data jaringan berdasarkan kriteria tertentu.
6. Pencarian paket data dengan kriteria spesifik.
7. Pengaturan warna pada tampilan paket data untuk memudahkan analisis.
8. Menampilkan statistik paket data dalam jaringan.
9. *Wireshark* memerlukan antarmuka fisik (*network interface card*) untuk menangkap paket data yang masuk dan keluar dari jaringan. *Wireshark* mendukung berbagai antarmuka jaringan seperti ATM, *Bluetooth, Cisco HDLC, DOCSIS, Ethernet, Frame Relay, IRDA, PPP Link, SS7, Token Ring, USB,* dan *LAN*.
10. Selain antarmuka fisik, *Wireshark* juga mendukung antarmuka virtual seperti *loopback, pipes, VLAN*, dan *WinCapRemote*.

2. 7 Kepolisian

Kepolisian negara republik indonesia atau POLRI adalah lembaga penegak hukum nasional dan kepolisian negara di indonesia, dimana presiden republik indonesia bertanggung jawab langsung atas mereka. Undang-Undang Republik Indonesia nomor 2 tahun 2002 Pasal 5 tentang kepolisian yang berbunyi :

(1) Kepolisian Negara Republik Indonesia merupakan alat negara yang berperan dalam memelihara keamanan dan ketertiban masyarakat, menegakkan hukum, serta memberikan perlindungan, pengayoman, dan pelayanan kepada masyarakat dalam rangka terpeliharanya keamanan dalam negeri.

(2) Kepolisian Negara Republik Indonesia adalah Kepolisian Nasional yang merupakan satu kesatuan dalam melaksanakan peran sebagaimana dimaksud dalam ayat (1).

Di Inggris, menurut (McLay, 2009) ada definisi hukum tentang fungsi dan tujuan kepolisian. Semua orang setuju bahwa polisi harus:

1. Mencegah kejahatan dan kekacauan, ekstrimisme dan terorisme.
2. Menjaga hukum dan ketertiban, dan melindungi orang dan harta benda dari tindakan kriminal (baik alami maupun buatan manusia).
3. Mendeteksi semua jenis penjahat dan berfungsi dalam sistem peradilan pidana, diawasi dan diatur oleh kejaksaan tinggi.
4. Menyediakan layanan pengawasan polisi.
5. Menurut tradisi lama, membantu semua orang yang membutuhkan mereka.

2. 7. 1 Fungsi Kepolisian

Undang-Undang Republik Indonesia Nomor 2 tahun 2002 tentang Kepolisian Negara Republik Indonesia dalam Pasal 2 yang berbunyi: fungsi kepolisian adalah salah satu fungsi pemerintahan negara di bidang pemeliharaan keamanan dan ketertiban masyarakat, penegakan hukum, perlindungan, pengayoman, dan pelayanan kepada masyarakat. Sedangkan pada Pasal 4 yang berbunyi : Kepolisian Negara Republik Indonesia bertujuan untuk mewujudkan keamanan dalam negeri yang meliputi terpeliharanya keamanan dan ketertiban masyarakat, tertib dan tegaknya hukum, terselenggaranya perlindungan, pengayoman, dan pelayanan kepada masyarakat, serta terbinanya ketenteraman masyarakat dengan menjunjung tinggi hak asasi manusia.

2. 7. 2 Tugas Kepolisian

Undang-Undang Republik Indonesia Nomor 2 tahun 2002 tentang Kepolisian Negara Republik Indonesia yang tertulis pada Pasal 13 yang berbunyi: Tugas pokok Kepolisian Negara Republik Indonesia adalah:

1. memelihara keamanan dan ketertiban masyarakat;
2. menegakkan hukum; dan
3. memberikan perlindungan, pengayoman, dan pelayanan kepada masyarakat.

2. 7. 3 Wewenang Kepolisian

Undang-Undang Republik Indonesia Nomor 2 tahun 2002 tentang Kepolisian Negara Republik Indonesia dalam Pasal 15 ayat (1) yaitu dalam rangka menyelenggarakan tugas sebagaimana dimaksud dalam Pasal 13 dan 14 Kepolisian Negara Republik Indonesia secara umum berwenang:

1. menerima laporan dan/atau pengaduan;
2. membantu menyelesaikan perselisihan warga masyarakat yang dapat mengganggu ketertiban umum;
3. mencegah dan menanggulangi tumbuhnya penyakit masyarakat;
4. mengawasi aliran yang dapat menimbulkan perpecahan atau mengancam persatuan dan kesatuan bangsa;
5. mengeluarkan peraturan kepolisian dalam lingkup kewenangan administratif kepolisian;
6. melaksanakan pemeriksaan khusus sebagai bagian dari tindakan kepolisian dalam rangka pencegahan;
7. melakukan tindakan pertama di tempat kejadian;

8. mengambil sidik jari dan identitas lainnya serta memotret seseorang;
9. mencari keterangan dan barang bukti;
10. menyelenggarakan Pusat Informasi Kriminal Nasional;
11. mengeluarkan surat izin dan/atau surat keterangan yang diperlukan dalam rangka pelayanan masyarakat;
12. memberikan bantuan pengamanan dalam sidang dan pelaksanaan putusan pengadilan, kegiatan instansi lain, serta kegiatan masyarakat;
13. menerima dan menyimpan barang temuan untuk sementara waktu.

Undang-Undang Republik Indonesia Nomor 2 tahun 2002 tentang Kepolisian Negara Republik Indonesia dalam Pasal 16 ayat (1) yaitu: dalam rangka menyelenggarakan tugas sebagaimana dimaksud dalam Pasal 13 dan 14 di bidang proses pidana, Kepolisian Negara Republik Indonesia berwenang untuk:

1. melakukan penangkapan, penahanan, penggeledahan, dan penyitaan;
2. melarang setiap orang meninggalkan atau memasuki tempat kejadian perkara untuk kepentingan penyidikan;
3. membawa dan menghadapkan orang kepada penyidik dalam rangka penyidikan;
4. menyuruh berhenti orang yang dicurigai dan menanyakan serta memeriksa tanda pengenal diri;
5. melakukan pemeriksaan dan penyitaan surat;
6. memanggil orang untuk didengar dan diperiksa sebagai tersangka atau saksi;
7. mendatangkan orang ahli yang diperlukan dalam hubungannya dengan pemeriksaan perkara; h. mengadakan penghentian penyidikan;

8. menyerahkan berkas perkara kepada penuntut umum;
9. mengajukan permintaan secara langsung kepada pejabat imigrasi yang berwenang di tempat pemeriksaan imigrasi dalam keadaan mendesak atau mendadak untuk mencegah atau menangkal orang yang disangka melakukan tindak pidana;
10. memberi petunjuk dan bantuan penyidikan kepada penyidik pegawai negeri sipil serta menerima hasil penyidikan penyidik pegawai negeri sipil untuk diserahkan kepada penuntut umum; dan
11. mengadakan tindakan lain menurut hukum yang bertanggung jawab.

2. 8 Informasi dan Transaksi Elektronik

Berdasarkan Pasal 1 dalam Undang-Undang Republik Indonesia Nomor 19 Tahun 2016 Perubahan atas Undang-Undang Republik Indonesia Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik bunyi Pasal ini yaitu: Dalam Undang-Undang ini yang dimaksud dengan:

1. Informasi Elektronik adalah satu atau sekumpulan data elektronik, termasuk tetapi tidak terbatas pada tulisan, suara, gambar, peta, rancangan, foto, *electronic data interchange* (EDI), surat elektronik (*electronic mail*), *Telegram*, *teleks*, *telecopy* atau sejenisnya, huruf, tanda, angka, Kode Akses, simbol, atau perforasi yang telah diolah yang memiliki arti atau dapat dipahami oleh orang yang mampu memahaminya.
2. Transaksi Elektronik adalah perbuatan hukum yang dilakukan dengan menggunakan Komputer, jaringan Komputer, dan/atau media elektronik lainnya.

3. Teknologi Informasi adalah suatu teknik untuk mengumpulkan, menyiapkan, memproses, mengumumkan, dan/atau menyebarkan informasi. menyimpan, menganalisis,
4. Dokumen Elektronik adalah setiap Informasi Elektronik yang dibuat, diteruskan, dikirimkan, diterima, atau disimpan dalam bentuk analog, digital, elektromagnetik, optikal, atau sejenisnya, yang dapat dilihat, ditampilkan, dan/atau didengar melalui Komputer atau Sistem Elektronik, termasuk tetapi tidak terbatas pada tulisan, suara, gambar, peta, rancangan, foto atau sejenisnya, huruf, tanda, angka, Kode Akses, simbol atau perforasi yang memiliki makna atau arti atau dapat dipahami oleh orang yang mampu memahaminya.
5. Sistem Elektronik adalah serangkaian perangkat dan prosedur elektronik yang berfungsi mempersiapkan, mengumpulkan, mengolah, menganalisis, menyimpan, menampilkan, mengumumkan, mengirimkan, dan/atau menyebarkan Informasi Elektronik.
6. Penyelenggaraan Sistem Elektronik adalah pemanfaatan Sistem Elektronik oleh penyelenggara negara, Orang, Badan Usaha, dan/atau masyarakat.

   6a. Penyelenggara Sistem Elektronik adalah setiap Orang, penyelenggara negara, Badan Usaha, dan masyarakat yang menyediakan, mengelola, dan/atau mengoperasikan Sistem Elektronik, baik secara sendiri-sendiri maupun bersama- kepada pengguna Sistem Elektronik untuk keperluan dirinya dan/atau keperluan pihak lain.

7. Jaringan Sistem Elektronik adalah terhubungnya dua Sistem Elektronik atau lebih, yang bersifat tertutup ataupun terbuka.
8. Agen Elektronik adalah perangkat dari suatu Sistem Elektronik yang dibuat untuk melakukan suatu tindakan terhadap suatu Informasi Elektronik tertentu secara otomatis yang diselenggarakan oleh Orang.
9. Sertifikat Elektronik adalah sertifikat yang bersifat elektronik yang memuat Tanda Tangan Elektronik dan identitas yang menunjukkan status subjek hukum para pihak dalam Transaksi Elektronik yang dikeluarkan Elektronik. oleh Penyelenggara Sertifikasi.
10. Penyelenggara Sertifikasi Elektronik adalah badan hukum yang berfungsi sebagai pihak yang layak dipercaya, yang memberikan dan mengaudit Sertifikat Elektronik.
11. Lembaga Sertifikasi Keandalan adalah lembaga independen yang dibentuk oleh profesional yang diakui, disahkan, dan diawasi oleh Pemerintah dengan kewenangan mengaudit dan mengeluarkan sertifikat keandalan dalam Transaksi Elektronik.
12. Tanda Tangan Elektronik adalah tanda tangan yang terdiri atas Informasi Elektronik yang dilekatkan, terasosiasi atau terkait dengan Informasi Elektronik lainnya yang digunakan sebagai alat verifikasi dan autentikasi.
13. Penanda Tangan adalah subjek hukum yang terasosiasikan atau terkait dengan Tanda Tangan Elektronik.
14. Komputer adalah alat untuk memproses data elektronik, magnetik, optik, atau sistem yang melaksanakan fungsi logika, aritmatika, dan penyimpanan.

15. Akses adalah kegiatan melakukan interaksi dengan Sistem Elektronik yang berdiri sendiri atau dalam jaringan.
16. Kode Akses adalah angka, huruf, simbol, karakter lainnya atau kombinasi di antaranya, yang merupakan kunci untuk dapat mengakses Komputer dan/atau Sistem Elektronik lainnya.
17. Kontrak Elektronik adalah perjanjian para pihak yang dibuat melalui Sistem Elektronik.
18. Pengirim adalah subjek hukum yang mengirimkan Informasi Elektronik dan/atau Dokumen Elektronik.
19. Penerima adalah subjek hukum yang menerima Informasi Elektronik dan/atau Dokumen Elektronik dari Pengirim.
20. Nama Domain adalah alamat internet penyelenggara negara, Orang, Badan Usaha, dan/atau masyarakat, yang dapat digunakan dalam berkomunikasi melalui internet, yang berupa kode atau susunan karakter yang bersifat unik untuk menunjukkan lokasi tertentu dalam internet.
21. Orang adalah orang perseorangan, baik warga negara Indonesia, warga negara asing, maupun badan hukum.
22. Badan Usaha adalah perusahaan perseorangan atau perusahaan persekutuan, baik yang berbadan hukum maupun yang tidak berbadan hukum.
23. Pemerintah adalah Menteri atau pejabat lainnya yang ditunjuk oleh Presiden.

2. 8. 1 Penipuan Informasi dan Transaksi Elektronik (ITE)

Berdasarkan Pasal 45A ayat (1) dan (2) dari Undang-Undang Republik Indonesia Nomor 19 Tahun 2016 yang mengubah Undang-Undang Nomor 11

Tahun 2008 tentang Informasi dan Transaksi Elektronik menyatakan sebagai berikut:

1. Setiap Orang yang dengan sengaja dan tanpa hak menyebarkan berita bohong dan menyesatkan yang mengakibatkan kerugian konsumen dalam Transaksi Elektronik sebagaimana dimaksud dalam Pasal 28 ayat (1) dipidana dengan pidana penjara paling lama 6 (enam) tahun dan/atau denda paling banyak Rp1.000.000.000,00 (satu miliar rupiah).
2. Setiap Orang yang dengan sengaja dan tanpa hak menyebarkan informasi yang ditujukan untuk menimbulkan rasa kebencian atau permusuhan individu dan/atau kelompok masyarakat tertentu berdasarkan atas suku, agama, ras, dan antargolongan (SARA) sebagaimana dimaksud dalam Pasal 28 ayat (2) dipidana dengan pidana penjara paling lama 6 (enam) tahun dan/atau denda paling banyak Rp1.000.000.000,00 (satu miliar rupiah).

2. 9 Penelitian Terdahulu

Penelitian terdahulu sebelumnya terdiri dari serangkaian penelitian sebelumnya yang akan digunakan oleh peneliti untuk mengaitkan dan mendukung argumen dalam penelitiannya. Meskipun tidak ada penelitian dengan judul yang identik, penulis menggunakan beberapa penelitian sebagai referensi untuk memperkaya isi penelitian ini. Lebih lanjut pembahasan mengenai hal ini dapat dijelaskan sebagai berikut:

Dalam Penelitian yang dilakukan oleh Latifahi et al. (2022) menunjukkan bahwa pandemi Covid-19 menguntungkan penggunaan layanan *financial technology*, namun juga meningkatkan ancaman kejahatan pencurian data

(Phishing). Selain itu, penelitian ini juga membahas upaya antisipasi yang dilakukan oleh industri perbankan dan layanan keuangan digital dalam mengedukasi nasabah mengenai ancaman pencurian data dan melakukan asesmen pemahaman nasabah terkait kejahatan *Phishing*.

Penelitian yang ditulis oleh Fitriani & Pakpahan (2020) menunjukkan bahwa pengguna media sosial perlu berhati-hati dan menjaga etika dalam bersosial media agar tidak terjadi penyalahgunaan atau pelanggaran hukum *cybercrime*. Selain itu, penelitian ini juga menekankan pentingnya upaya pencegahan *cybercrime* melalui perlindungan komputer dari virus, menjaga privasi, menghindari hoax, dan menyebarkan informasi yang positif. Penelitian ini memberikan pemahaman yang lebih dalam tentang dampak negatif dari penyalahgunaan media sosial dalam penyebaran *cybercrime*, serta memberikan rekomendasi untuk tindakan pencegahan yang dapat dilakukan oleh pengguna media sosial untuk melindungi diri mereka dari ancaman *cybercrime*.

Penelitian yang dilakukan oleh Vadila & Pratama (2021) berfokus pada penilaian tingkat kesadaran masyarakat Indonesia terhadap ancaman *Phishing*. Dengan melibatkan 254 responden dari berbagai latar belakang, termasuk jenis kelamin dan kelompok usia, penelitian ini menggunakan metode Analisis Ragam (ANOVA) dengan bahasa pemrograman R untuk menganalisis data.

Hasil penelitian menunjukkan bahwa masyarakat Indonesia secara umum masih belum mampu mengenali ancaman *Phishing* dengan baik. Analisis yang difokuskan pada aspek demografi, seperti jenis kelamin dan kelompok usia, menemukan bahwa tidak ada perbedaan signifikan dalam kesadaran terhadap

Phishing antara kelompok-kelompok tersebut. Dalam konteks ini, kesadaran terhadap ancaman *Phishing* tidak dipengaruhi secara signifikan oleh faktor jenis kelamin atau kelompok usia. Harapannya, hasil penelitian ini dapat menjadi landasan bagi pengembangan pembelajaran ke depannya guna meningkatkan kesadaran masyarakat terhadap ancaman *Phishing*. Dengan pemahaman yang lebih baik tentang kejahatan berbasis siber ini, diharapkan masyarakat dapat mengambil langkah-langkah pencegahan yang lebih efektif untuk melindungi diri mereka dari ancaman *Phishing*.

Penelitian yang ditulis oleh Arianto (2021) membahas peran media sosial sebagai saluran *whistleblowing* alternatif yang digunakan untuk mendeteksi praktik kecurangan *(fraud)*. Melalui penggunaan media sosial sebagai sarana pertukaran dan penyebaran informasi kewargaan, pada penelitian ini menyoroti bagaimana media sosial dapat menjadi *platform* bagi pengguna untuk melaporkan indikasi kecurangan secara anonim atau teridentifikasi.

Penelitian ini menggunakan metode kualitatif eksploratif dengan teknik pengumpulan data melalui wawancara mendalam *(in-depth interview)* untuk memahami bagaimana media sosial digunakan oleh para pengungkap fakta *(whistleblower)* dalam melaporkan praktik kecurangan yang mereka temui. Secara tradisional, sistem *whistleblowing* lebih terfokus pada saluran terintegrasi seperti website dan aplikasi khusus. Namun, partisipasi aktif dari pengguna media sosial telah mengubah dinamika ini dengan memberikan alternatif lain untuk melaporkan kecurangan.

Hasil pembahasan dari penelitian ini menyimpulkan bahwa media sosial memiliki kontribusi positif sebagai saluran whistleblowing dalam mendeteksi praktik kecurangan di berbagai entitas dan sektor publik. Dengan adanya partisipasi aktif dari warganet, media sosial memberikan ruang bagi pengungkap fakta untuk melaporkan indikasi kecurangan dengan lebih cepat dan dalam cakupan yang lebih luas. Oleh karena itu, artikel ini menggarisbawahi peran penting media sosial sebagai alat yang efektif dalam mengungkap praktik kecurangan (*fraud*) dalam masyarakat secara lebih transparan.

Pada Penelitian yang ditulis oleh Muhammad & Harefa (2023). Penelitian ini membahas tentang analisis pengaturan hukum terkait *Phishing* yang belum sepenuhnya jelas dalam aspek hukum pidana, khususnya terkait UU ITE di Indonesia. Tujuannya adalah untuk mengevaluasi kesesuaian aturan hukum saat ini dengan prinsip keadilan, dengan memperhatikan kedua belah pihak, yaitu korban dan masyarakat.

Metode penelitian yang digunakan bersifat yuridis normatif dengan pendekatan perundang-undangan dan pendekatan konseptual. Dari hasil penelitian ini, terdapat dua poin penting yang disoroti: pertama, Aturan hukum pidana yang berlaku saat ini masih cenderung berorientasi pada sistem pemidanaan lama yang lebih menekankan teori pembalasan pidana terhadap pelaku tindak pidana. Akibatnya, hak-hak korban sering kali terabaikan dalam proses penegakan hukum. Kedua, Terdapat kekurangan dalam regulasi yang mengatur secara spesifik mengenai ganti rugi terkait tindak pidana *Phishing*. Dalam hal ini, tidak ada

ketentuan hukum yang mengatur secara konkret tanggung jawab pelaku untuk mengganti kerugian secara materiil yang dialami oleh korban.

Penelitian ini menjadi penting karena memberikan kontribusi untuk melengkapi studi-studi sebelumnya yang cenderung hanya memberikan hukuman penjara terhadap pelaku tanpa memberikan pertanggungjawaban pribadi dari pelaku dalam mengembalikan kerugian yang dialami oleh korban secara materiil. Dengan demikian, penelitian ini menyoroti perlunya perubahan atau penyempurnaan dalam pengaturan hukum terkait *Phishing* untuk lebih mempertimbangkan hak-hak korban dan tanggung jawab pelaku dalam mengembalikan kerugian yang ditimbulkan oleh tindakan mereka.

Dari Penelitian sebelumnya, terlihat bahwa sebagian besar penelitiannya cenderung memusatkan perhatian pada aspek peraturan, sikap, dampak, dan relevansi undang-undang. Penelitian ini, yang dilakukan di Polda Daerah Istimewa Yogyakarta, memiliki perbedaan utama dengan penelitian sebelumnya karena membahas tentang mekanisme pengungkapan polisi terkait kasus *Phishing* serta kesulitan yang dihadapi aparat kepolisian dalam mengungkap kasus *Phishing*. Pentingnya peran polisi dalam memberikan informasi kepada korban tentang kasus yang menimpa mereka menjadi faktor, mengingat adanya kerugian yang dialami oleh individu tersebut. Oleh karena itu, peneliti memutuskan untuk menulis "Analisis Peran Polda Istimewa Yogyakarta Dalam Pengungkapan Kasus *Phishing*" sebagai judul penelitian.

BAB III

METODE PENELITIAN

3. 1 Pengenalan Bab

Bagian ini, peneliti akan menguraikan metode penelitian yang digunakan selama penelitian yang dilaksanakan di Polda DIY yang berkaitan dengan tren permasalahan serta cara pengungkapan kasus *Phishing* di wilayah Daerah Istimewa Yogyakarta. Bab ini memberikan landasan bagi pembahasan di bab-bab berikutnya yang akan membahas secara rinci mengenai metode penelitian yang diterapkan untuk menjawab pertanyaan-pertanyaan yang diajukan. Bab ini akan membahas aspek-aspek seperti metode penelitian, fokus penelitian, susunan penelitian, sumber dan jenis data, subjek penelitian, teknik pengumpulan data, pengecekan kevalidan data, serta teknik analisis yang diterapkan dalam penelitian ini.

3. 2 Jenis Penelitian

Menurut (Saryono, 2010) , penelitian kualitatif digunakan untuk mengeksplorasi, mengidentifikasi, mendeskripsikan, dan menjelaskan kualitas atau aspek-aspek dari pengaruh sosial yang tidak dapat dijelaskan, diukur, atau diilustrasikan secara tepat melalui pendekatan kuantitatif. Perbedaannya dengan penelitian kuantitatif terletak pada pendekatan yang dimulai dari data, memanfaatkan teori yang ada sebagai landasan penjelasan, dan berakhir dengan pembentukan sebuah teori. Alasan pemilihan pendekatan kualitatif dalam penelitian ini adalah untuk mendapatkan pemahaman yang lebih mendalam

terhadap prosedur yang digunakan oleh Polda DIY dalam mengungkap kasus *Phishing.*

Agar pemahaman lebih terfokus, peneliti memilih jenis penelitian kualitatif berupa studi kasus. Menurut (Yin, 1989), alasan pemilihan strategi studi kasus berasal dari jawaban terhadap tiga pertanyaan epistemologis, yakni terkait dengan tipe pertanyaan, kontrol terhadap objek, dan cakupan penelitian. Strategi studi kasus dipilih ketika jawaban-jawabannya sesuai dengan kondisi sebagai berikut:

1. Judul penelitian ini berfokus pada pertanyaan eksploratif dan deskriptif tentang bagaimana dan mengapa terjadinya suatu kejadian atau gejala sosial.
2. Penelitian ini menggunakan metode studi kasus tanpa mengontrol peristiwa sosial yang diamati. Peneliti mengamati kejadian sesuai keadaannya, menunjukkan pendekatan naturalistik yang relatif alami.
3. Fokusnya adalah pada peristiwa atau gejala sosial kontemporer dalam kehidupan nyata, memungkinkan akses melalui pengamatan partisipatif dan wawancara mendalam dengan subjek penelitian.

Dari penjelasan sebelumnya, penelitian ini menggunakan metode studi kasus sebagai 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. Tujuan penelitian juga mencakup pengidentifikasian kekurangan dan hambatan yang dihadapi oleh Polda DIY, serta memberikan rekomendasi

perbaikan yang dapat diterapkan oleh lembaga keamanan di Daerah Istimewa Yogyakarta.

3. 3 Objek Penelitian

Penelitian ini dilaksanakan di kantor Polda Daerah Istimewa Yogyakarta, Direktorat Reserse Kriminal Khusus (Ditreskrimsus), unit V Siber yang berlokasi di Jalan Ringroad Utara, Sanggarahan Condong Catur, Kabupaten Sleman, Kecamatan Depok,

Pemilihan Polda DIY sebagai lokasi penelitian didasarkan pada peran kepolisian dalam mengungkap kasus *Phishing*. Keberadaan kepolisian, terutama Direktorat Reserse Kriminal Khusus, dianggap sangat penting karena memiliki peran utama dalam menyelidiki dan menangani kejahatan daring seperti *Phishing.* Selain itu, lokasi ini dipilih karena kebutuhan akan data yang relevan dan dibutuhkan dalam penelitian. Adanya akses dan ketersediaan data yang diperlukan oleh peneliti menjadi alasan kuat dalam menentukan lokasi penelitian di Polda DIY.

3. 4 Fokus Penelitian

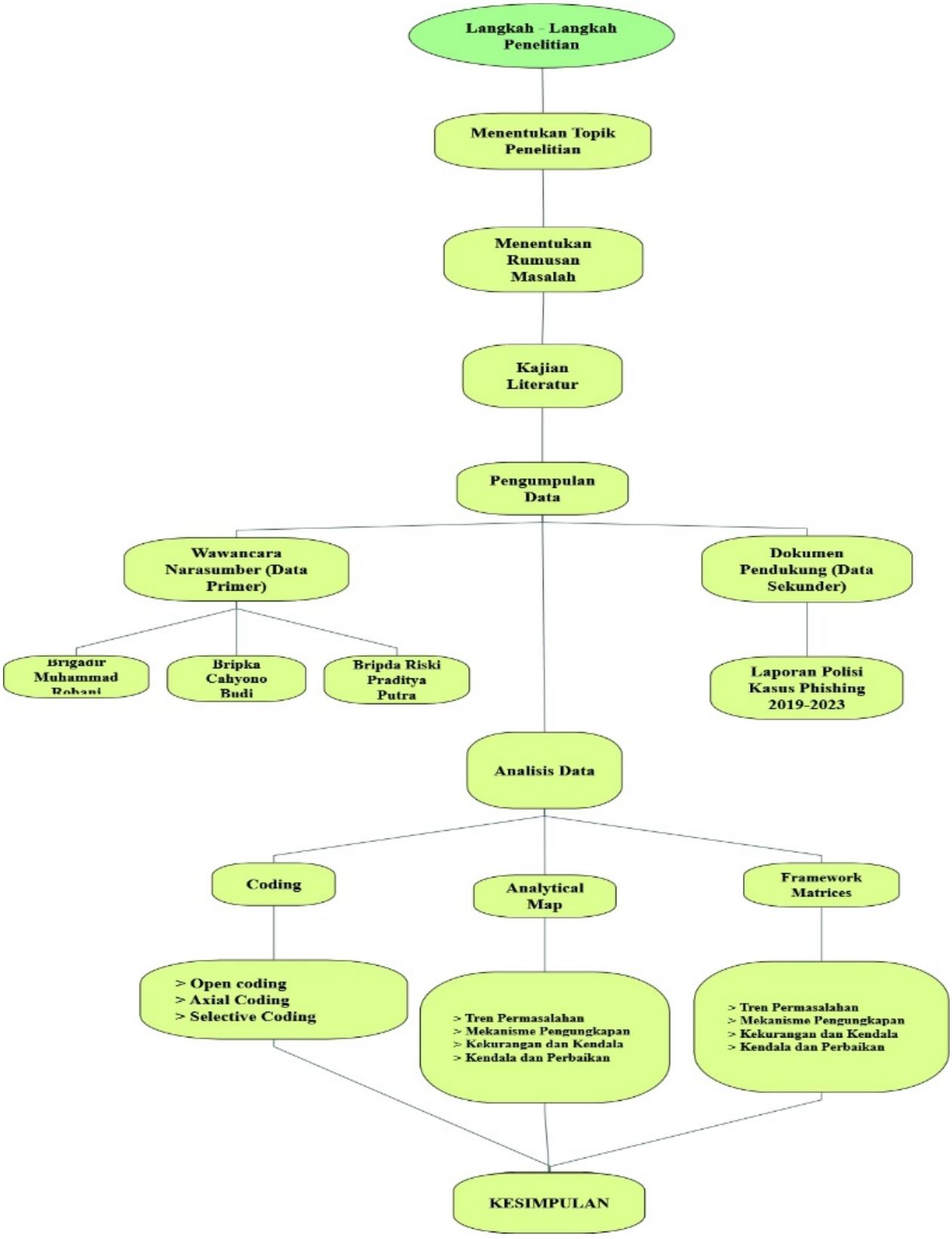
Fokus penelitian menjadi aspek yang diperhatikan dengan seksama. Fungsinya adalah untuk memberikan batasan yang konsisten pada penelitian, memastikan pembahasan sesuai dengan tujuan dan rumusan masalah. Fokus penelitian dalam konteks ini adalah sebagai berikut:

1. Tren permasalahan *Phishing* di wilayah Daerah Istimewa Yogyakarta tahun 2019-2023.

2. Mekanisme pengungkapan yang dilakukan Polda DIY terhadap kasus *Phishing* di wilayah Daerah Istimewa Yogyakarta.
3. Identifikasi kekurangan dan hambatan yang dihadapi oleh Ditreskrimsus Polda DIY dalam pengungkapan kasus *Phishing* di wilayah Daerah Istimewa Yogyakarta.
4. Saran perbaikan yang dapat dilakukan Polda DIY dalam pengungkapan kasus *Phishing* di wilayah Daerah Istimewa Yogyakarta.

3. 5 Sistematika Penelitian

Sistematika penelitian yang digunakan oleh peneliti dilakukan untuk memperoleh hasil akhir yaitu kesimpulan. Berikut merupakan sistematika penelitian yang dilakukan:



Gambar 3.1 Langkah-Langkah Penelitian

Tahapan awal dalam sebuah penelitian adalah pemilihan topik yang akan diangkat. Topik penelitian ini merupakan fokus pembahasan yang masih bersifat umum dan perlu diperinci lebih lanjut. Salah satu topik yang telah dipilih oleh peneliti adalah "Peran Polda Daerah Istimewa Yogyakarta dalam Mengungkap Kasus *Phishing*." Setelah penetapan topik, langkah selanjutnya bagi peneliti adalah merumuskan masalah yang menjadi pedoman dalam menentukan fokus dan arah penelitian. Peneliti memilih untuk mengkaji Peran Polda DIY Dalam Pengungkapan Kasus *Phishing* sebagai inti dari penelitian ini.

Langkah berikutnya yang dilakukan oleh peneliti adalah melakukan tinjauan pustaka. Tinjauan pustaka merupakan proses identifikasi, lokasi, dan analisis dokumen yang berkaitan dengan masalah yang telah ditetapkan. Dokumen ini mencakup jurnal terkait, abstrak, tinjauan, buku, data statistik, serta laporan penelitian yang relevan. Tujuan dari tinjauan pustaka adalah untuk menjawab rumusan masalah yang telah ditentukan. Jika terdapat pertanyaan yang belum terjawab, peneliti mengumpulkan data tambahan hingga dapat memberikan jawaban yang memuaskan.

Data yang sudah dikumpulkan peneliti 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. Selanjutnya, peneliti membuat "relationships" untuk menghubungkan *nodes* yang telah dibuat. Data dari sumber diatur sesuai dengan kriteria *nodes* yang telah ditetapkan.

Hasil dari proses *coding* disajikan oleh peneliti dalam bentuk *framework matrix* yang berasal dari data wawancara dengan narasumber. *Framework matrix* ini berfungsi sebagai tabel matriks untuk menganalisis data sesuai dengan kriteria yang telah ditentukan oleh peneliti. Terdapat empat *framework matrix* yang disesuaikan dengan empat rumusan masalah yang ada.

Selanjutnya, peneliti membuat Peta Analisis menggunakan bantuan *software* Nvivo 12. Peta Analisis dibuat dengan tujuan agar mempermudah pembacaan pada bab pembahasan. Peneliti memiliki empat maps yang terbagi sesuai dengan empat rumusan masalah yang telah diidentifikasi sebelumnya.

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.

3. 5. 1 Sumber Data Primer

Menurut (Abdul Fattah 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.

3. 5. 1. 1 Wawancara

Salah satu metode untuk mengumpulkan data dan informasi dalam sebuah penelitian adalah melalui wawancara dengan narasumber terkait. Menurut Moleong dalam bukunya "Metode Penelitian Kualitatif," wawancara merupakan proses tanya jawab yang dilakukan dengan tujuan tertentu antara pemberi wawancara dan subjek yang diwawancarai (Moleong, 2009).

Dalam penelitian ini, peneliti melakukan wawancara dengan tiga narasumber dari Direktorat Reserse Kriminal Khusus Polda Daerah Istimewa Yogyakarta. Berikut ini merupakan tabel yang memuat profil dari narasumber Direktorat Reserse Kriminal Khusus Polda Daerah Istimewa Yogyakarta.

Tabel 3.1 Profil Narasumber

No.	Partisipan Wawancara	Jabatan	Jenis Kelamin	Pangkat	Umur	Masa Bekerja di Polda DIY
1.	Cahyono Budi	Banit Subit V/Siber	L	Bripka	42	>2 tahun
2.	Muhammad Robani	Unit 3/Subdit V	L	Brigadir	33	>3 tahun
3.	Riski Praditya Putra	Banum Subdit V/Siber	L	Bripda	23	>2 tahun

3. 5. 2 Sumber Data Sekunder

Menurut (Abdul Fattah 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.

3. 5. 2. 1 Dokumen

Pada Pelaksanaan penelitian, peneliti mengumpulkan dokumen yang dapat digunakan sebagai sumber informasi, alat klasifikasi praktik, dan bahan evaluasi selama proses penelitian. Dalam penelitian ini, peneliti memanfaatkan dokumen Jumlah Pelaporan kasus *Phishing* di wilayah Daerah Istimewa Yogyakarta tahun 2019-2023 yang diperoleh dari Polda DIY.

3. 6 Teknik Analisa Data

Dalam penelitian kualitatif, data dikumpulkan dari berbagai sumber dengan berbagai teknik pengumpulan data (triangulasi) dan dilakukan secara berkelanjutan sampai data mencapai kejenuhan. Pengamatan yang terus menerus ini menyebabkan variasi data yang luas, sehingga teknik analisis data yang digunakan belum memiliki pola yang pasti.

Analisis data dalam penelitian kualitatif adalah proses sistematis dalam menemukan dan menyusun data dari hasil wawancara, catatan lapangan, dan sumber lainnya agar menjadi lebih mudah dipahami. Metode pengolahan data kualitatif terdiri dari tiga tahap, yaitu reduksi data, penyajian data, dan penarikan kesimpulan atau verifikasi (Sugiyono, 2018).

3. 6. 1 Reduksi Data *(Data Reduction)*

Data yang diperoleh peneliti dari lapangan pada umumnya cukup banyak dan memiliki format yang berbeda dengan data kuantitatif. Reduksi data dilakukan untuk merangkum, memilih informasi utama, memfokuskan pada aspek yang relevan, mengidentifikasi tema dan pola, serta menghilangkan yang tidak relevan. Pada tahap reduksi data, peneliti menggunakan *Software Nvivo* 12 karena dapat membantu peneliti untuk mengolah dan menganalisis data. Dalam penelitian ini, metode reduksi data yang dipakai adalah *Coding* dan *Framework Matrices.*

1. *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) . Tahapan *Coding* dimulai dengan mengidentifikasi data dari berbagai sumber untuk mengelompokkannya ke dalam *nodes* yang sesuai dengan topik serta sub-topik penelitian. Hasil dari proses *Coding* ini diarahkan pada rumusan masalah yang telah ditetapkan sebelumnya oleh peneliti.

   Hasil *coding* dari penelitian mencakup empat kategori utama yang terkait dengan rumusan masalah yang ada:

   a. *Coding* yang berkaitan dengan Tren Permasalahan Kasus *Phishing* di wilayah Daerah Istimewa Yogyakarta.
   b. *Coding* yang terfokus pada Mekanisme Pengungkapan yang dilakukan oleh Polda DIY terhadap Kasus *Phishing* di wilayah Daerah Istimewa Yogyakarta.

c. *Coding* yang menyoroti Kekurangan dan Kendala yang dihadapi oleh Polda DIY dalam proses Pengungkapan Kasus *Phishing* di wilayah Daerah Istimewa Yogyakarta.

d. *Coding* yang berhubungan dengan Upaya Perbaikan yang dapat dilakukan oleh Polda DIY dalam rangka Pengungkapan Kasus *Phishing* di wilayah Daerah Istimewa Yogyakarta.

(Creswell & John W Creswell, 2012) Menjelaskan langkah-langkah *Coding* sebagai berikut:

a. *Open Coding*

Yaitu kategori-kategori dibuat berdasarkan informasi yang diperoleh dari wawancara. Penulis membagi informasi menjadi kategori sesuai dengan empat rumusan masalah penelitian.

b. Axial Codiing

Yaitu kategori-kategori dipilih dan ditempatkan dalam suatu model teoritis. Penulis mengintegrasikan kategori yang ditetapkan pada tahap *Open Coding* ke dalam *Nodes* yang telah dibuat.

c. Selective Coding

Yaitu penulis menyusun hubungan antara kategori-kategori tersebut dalam sebuah narasi. Peneliti menggambarkan hubungan antara kategori yang sudah ditetapkan sebelumnya. *Nodes* berfungsi sebagai referensi terkait topik penelitian, dengan informasi yang relevan dan spesifik disimpan didalamnya. Peneliti juga membuat *Case Nodes* untuk menyimpan hasil wawancara dari setiap narasumbernya. Peneliti juga

membuat relasi antar *nodes* yang sudah dibuat untuk membentuk hubungan antara mereka.

2. *Framework Matrices*

Framework Matrices merupakan alat yang sangat berguna dalam mengevaluasi dan merangkum materi wawancara dalam penelitian ini. Dengan menggunakan matriks kerangka kerja, peneliti dapat mengelola data yang sangat besar menjadi lebih mudah dikelola dan dapat diinterpretasikan. Matriks ini terdiri dari kisi-kisi yang memiliki baris untuk setiap kasus yang diamati, seperti individu yang diwawancarai, dan kolom untuk kode atau tema yang relevan. Dalam setiap sel kisi, peneliti dapat memasukkan teks ringkasan yang relevan dengan kasus dan tema yang bersangkutan. (Na & Hipertensiva, n.d.).

Penggunaan matriks kerangka kerja sangat berguna dalam penelitian ini karena memudahkan peneliti dalam melihat informasi terkait tema tertentu secara komprehensif. Dengan menelusuri kolom yang sesuai, peneliti dapat fokus pada tema tersebut dan memahami berbagai aspek yang terkait. Selain itu, melalui urutan yang teratur, peneliti dapat mengeksplorasi hubungan antar tema untuk setiap individu yang diteliti, memberikan pemahaman yang lebih luas terhadap konteks pengalaman individu. Terakhir, matriks kerangka kerja memfasilitasi perbandingan antara pengalaman individu yang berbeda, memungkinkan penemuan pola dan perbedaan yang signifikan di antara partisipan penelitian.

3. 6. 2 Tampilan Data *(Data Display)*

Setelah dilakukan reduksi, langkah berikutnya yang dilakukan peneliti adalah menampilkan data agar lebih mudah dipahami. Penyajian data dapat berupa tabel, grafik, diagram, atau representasi visual lainnya untuk memberikan gambaran yang lebih jelas. Dalam penelitian ini, peneliti menggunakan metode visualisasi data *Analytical Maps*

1. *Analytical Maps*

   Dalam menggunakan *software Nvivo 12*, peneliti dibantu dalam membuat peta analisis setelah melakukan proses pengkodean terhadap data yang telah dikumpulkan. Peta analisis ini membantu dalam memahami hubungan antara *nodes* dengan berbagai dokumen yang dimiliki peneliti, baik dalam bentuk teks, visual, maupun gambar.

   Melalui bantuan *software* Nvivo 12, tercipta 4 peta analisis yang merupakan hasil dari rumusan masalah penelitian ini:

   a. Peta analisis yang menggambarkan tren permasalahan kasus *Phishing* di wilayah Daerah Istimewa Yogyakarta.
   b. Peta analisis mengenai peran Polda DIY dalam mengungkap kasus *Phishing* di wilayah Daerah Istimewa Yogyakarta.
   c. Peta analisis yang menyoroti kendala dan kekurangan yang dihadapi oleh Polda DIY dalam pengungkapan kasus *Phishing*, dengan fokus pada

keterkaitan antara kekurangan dan kendala yang dihadapi oleh lembaga tersebut.

d. Peta analisis yang menunjukkan kendala yang dihadapi oleh Polda DIY dan menyajikan saran perbaikan dari peneliti, menjelaskan langkah-langkah perbaikan yang bisa diterapkan oleh Polda DIY untuk mengatasi kendala yang ada.

3. 6. 3 Menarik Kesimpulan dan Verifikasi *(Conclusion and Verification)*

Tahap terakhir dalam analisis data kualitatif adalah menarik kesimpulan dan melakukan verifikasi. Kesimpulan awal yang dihasilkan bersifat tentatif dan dapat berubah ketika data baru ditemukan. Namun, jika bukti yang ditemukan saat pengumpulan data berikutnya valid dan konsisten, maka kesimpulan yang dihasilkan akan menjadi lebih meyakinkan. Peneliti menggunakan *software* Nvivo 12 untuk menarik kesimpulan.

3. 7 Pengujian Keabsahan Data

Untuk menjamin keandalan data, peneliti perlu melakukan uji keabsahan data. Dalam penelitian ini, diterapkan metode triangulasi yang melibatkan beberapa pendekatan dalam proses pengumpulan dan analisis data (Olsen, 2004) . Pendekatan ini bertujuan untuk memahami fenomena yang diteliti secara menyeluruh, sehingga memungkinkan pemahaman yang komprehensif dari berbagai perspektif. Dengan mengamati fenomena dari beragam sudut pandang, hal ini memungkinkan perolehan kebenaran yang lebih kuat dan dapat diandalkan. Norman K. Denzin mendefinisikan triangulasi sebagai penggabungan dan penggunaan berbagai metode untuk memeriksa fenomena terkait dari berbagai

sudut pandang dan perspektif. Konsep ini telah menjadi pendekatan umum yang digunakan oleh peneliti kualitatif di berbagai bidang. Menurut (Denzi, 2012) triangulasi mencakup empat aspek yaitu triangulasi Metode, triangulasi antar-peneliti, triangulasi teori dan Triangulasi Sumber data. Tetapi dalam penelitian ini, peneliti menggunakan 3 triangulasi, sebagai berikut:

1. Triangulasi metode

   Dalam penelitian ini, peneliti melakukan uji triangulasi metode untuk memastikan keabsahan data. Ini dilakukan dengan menggabungkan berbagai metode seperti wawancara, observasi, dan survei, serta melibatkan informan yang beragam. Dengan mempertimbangkan berbagai perspektif, peneliti dapat mendapatkan gambaran yang lebih lengkap dan mendekati kebenaran. Proses triangulasi metode ini melibatkan pembandingan data dari pendekatan yang berbeda untuk menguji konsistensi dan validitas temuan. Misalnya, jika hasil dari wawancara sesuai dengan temuan dari observasi, hal ini dapat meningkatkan keyakinan terhadap kebenaran informasi yang diperoleh. Triangulasi metode ini memberikan keuntungan tambahan dalam meminimalkan bias dan meningkatkan keandalan hasil penelitian.

2. Triangulasi sumber data

   Dalam penelitian ini, peneliti menggunakan triangulasi data dengan *framework* matriks untuk memverifikasi keabsahan data. Melalui penggabungan berbagai metode dan sumber data seperti wawancara, observasi, dokumen tertulis, arsip, catatan resmi, catatan pribadi, serta gambar atau foto, peneliti dapat memperoleh pemahaman yang lebih komprehensif tentang

fenomena yang diteliti. Contohnya, jika hasil wawancara sesuai dengan temuan dari observasi atau dengan informasi yang terdapat dalam dokumen tertulis, peneliti memperoleh keyakinan tambahan terhadap kebenaran informasi tersebut. Dengan menggunakan triangulasi data dengan *framework* matriks, peneliti dapat memastikan keakuratan informasi yang diperoleh dari berbagai sumber data.

3. Triangulasi teori

Dalam penelitian ini, peneliti menggunakan triangulasi teori untuk menguji keabsahan data. Triangulasi teori melibatkan perbandingan hasil penelitian kualitatif dengan perspektif teori yang relevan. Hal ini dilakukan untuk menghindari bias individual peneliti terhadap temuan atau kesimpulan yang dihasilkan. Dengan membandingkan informasi dengan teori yang relevan, pemahaman yang lebih mendalam dapat tercapai, meskipun tahap ini dapat menantang karena memerlukan keahlian dalam membandingkan temuan dengan perspektif teoretis yang mungkin berbeda secara signifikan.

4. Member Checking

Dalam penelitian ini, Member checking adalah proses di mana peneliti mengembalikan data atau hasil penelitian kepada pihak yang memberikan data, yaitu pihak Polda DIY, untuk memeriksa ketepatan dan kesesuaian dengan pengalaman mereka. Jika ada data yang tidak sesuai, Polda DIY akan diberi kesempatan untuk memberikan koreksi. Data yang telah dikoreksi itulah yang kemudian akan digunakan oleh penulis sebagai data penelitian.

BAB IV

HASIL DAN PEMBAHASAN

4. 1 Pengenalan Bab

Bagian ini akan merangkum temuan yang diperoleh oleh peneliti selama kegiatan penelitian lapangan, yang bertujuan untuk menjawab pertanyaan-pertanyaan yang telah dirumuskan sebelumnya. Isi dari bab ini meliputi deskripsi mengenai objek penelitian, termasuk penjelasan mengenai sejarah terbentuknya Subdit V Siber Polda DIY, tugas yang diemban oleh Subdit V Siber Polda DIY, visi dan misi Ditreskrimsus Polda DIY, serta makna dari lambang Ditreskrimsus Polda DIY. Selanjutnya, peneliti akan secara terperinci membahas masing-masing rumusan masalah dalam penelitian ini, dengan menggunakan hasil dari perangkat lunak NVivo 12 seperti peta, matriks *coding*, dan *framework* matrices. Informasi tersebut akan membantu peneliti dalam mengorganisir pembahasan dan hasil penelitian, serta memungkinkan untuk menghasilkan kesimpulan yang relevan.

4. 2 Gambaran Umum Ditreskrimsus Polda Daerah Istimewa Yogyakarta

Dalam penelitian ini, Direktorat Reserse Kriminal Khusus (Ditreskrimsus) memiliki peran yang sangat penting terkait dengan kasus *Phishing*. Berdasarkan Pasal 1 nomor 20 dari Peraturan Kepala Kepolisian Negara Republik Indonesia Nomor 22 Tahun 2010 tentang Susunan Organisasi dan Tata Kerja pada Tingkat Kepolisian Negara, Ditreskrimsus merupakan unsur pelaksanaan tugas pokok yang berada di bawah pimpinan Kapolda. Pasal 140 ayat (1) dan (2) menjelaskan bahwa Ditreskrimsus dikepalai oleh "Dirreskrimsus", di mana pimpinan

Dirreskrimsus Polda DIY bernama AKBP Idham Mahdi, S.I.K., M.A.P. yang bertanggung jawab kepada Kapolda. Adapun susunan organisasi Ditreskrimsus, sebagaimana disebutkan dalam Pasal 141, terdiri dari:

1. Subbagrenmin (Subbagian Perencanaan dan Administrasi)
2. Bagbinopsnal (Bagian Pembinaan Operasional)
3. Bagwassidik (Bagian Pengawas Penyidikan)
4. Seksi Koordinasi dan Pengawasan Penyidik Pegawai Negeri Sipil
5. Subdit (Sub Direktorat)

Subdit di Ditreskrimsus Polda DIY terdiri dari lima bagian, yaitu:

1. Subdit I Inprodag

   Bertanggung jawab atas penanganan tindak pidana yang terkait dengan sektor perindustrian, produksi, hak kekayaan intelektual, perdagangan, pangan, asuransi, perfilman, perumahan pemukiman, dan karantina.

2. Subdit II Ekonomi

   Bertanggungjawab untuk menangani tindak pidana dalam sektor perbankan dan fiskal, devisa, dan keuangan. Contohnya adalah kasus uang palsu.

3. Subdit III Tipidkor

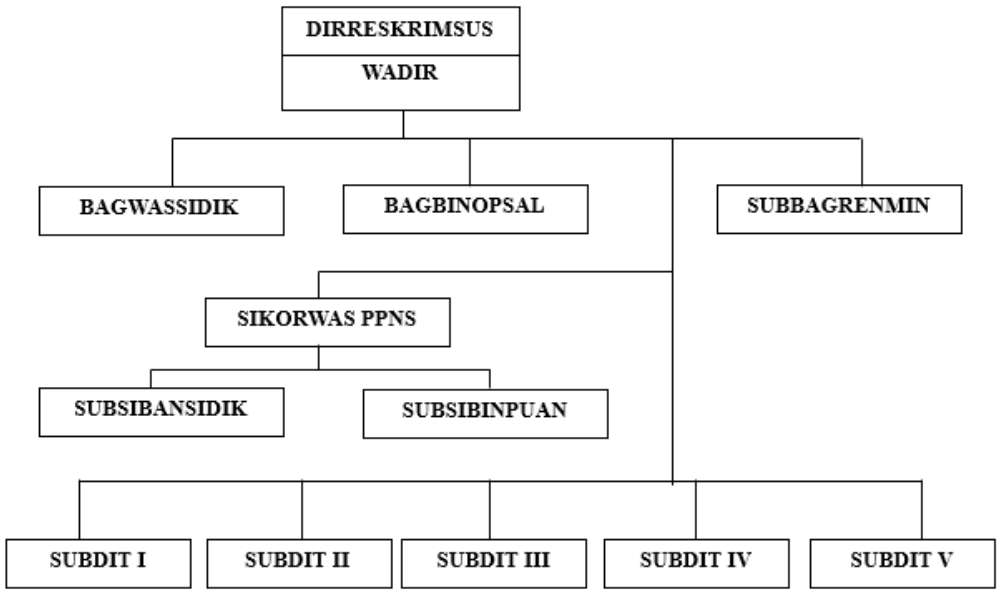
   Bertanggungjawab untuk menangani tindak pidana korupsi, termasuk kasus-kasus yang melibatkan dana bantuan, dana pemerintah, proyek pembangunan, keuangan negara, kredit usaha, dan perbuatan lain yang terkait dengan korupsi.

4. Subdit IV Tipidter

Bertanggungjawab untuk menangani tindak pidana terkait dengan sektor kehutanan, pertanian, dan lingkungan hidup. Ini meliputi kejahatan di cagar alam, pertambangan ilegal, pemanfaatan ilegal air bawah tanah, pencurian listrik, BBM ilegal, serta pelanggaran terkait tenaga kerja seperti kasus keimigrasian dan perlindungan tenaga kerja Indonesia.

5. Subdit V Siber

Bertanggung jawab menangani tindak pidana yang berkaitan dengan undang-undang informasi dan transaksi elektronik. Dalam konteks penelitian "Analisis Peran Polda Daerah Istimewa Yogyakarta dalam Pengungkapan Kasus *Phishing*," Subdit V Siber Ditreskrimsus Polda Daerah Istimewa Yogyakarta merupakan bagian yang menangani kasus tersebut. Sebelum membahas lebih lanjut mengenai tugas-tugas Subdit V Siber, peneliti akan menjelaskan latar belakang terbentuknya Subdit V Siber di Polda DIY.



Gambar 4.1 Struktur Ditreskrimsus Polda DIY (Sumber: Polda DIY, 2024)

4. 2. 2 Tugas Subdit V Siber Polda Daerah Istimewa Yogyakarta

Polda Daerah Istimewa Yogyakarta memiliki peran yang sangat penting dalam memenuhi tugas-tugasnya sesuai dengan Undang-Undang Republik Indonesia Nomor 2 Tahun 2002 mengenai Kepolisian Negara Republik Indonesia. Peran ini mencakup menjaga keamanan, memberikan pelayanan kepada masyarakat di wilayah Daerah Istimewa Yogyakarta, serta menegakkan hukum sambil memberikan perlindungan dan pengayoman. Khususnya Subdit V Siber Polda Daerah Istimewa Yogyakarta bertanggung jawab atas hal-hal berikut:

1. Subdit V bertugas melakukan penyelidikan dan penyidikan tindak pidana Siber yang terjadi di daerah hukum Polda.
2. Dalam melaksanakan tugas sebagaimana dimaksud pada ayat (1), Subdit menyelenggarakan fungsi:
    a. penyelidikan dan penyidikan tindak pidana tertentu yang terjadi di daerah hukum Polda;
    b. pemberkasan dan penyelesaian berkas perkara sesuai dengan ketentuan administrasi penyelidikan dan penyidikan tindak pidana; dan
    c. penerapan manajemen anggaran, serta manajemen penyelidikan dan penyidikan tindak pidana.
3. Dalam melaksanakan tugas sebagaimana dimaksud pada ayat (1), Subdit dibantu oleh sejumlah Unit, yang bertugas membantu pelaksanaan tugas dan fungsi Subdit.

4. 2. 3 Visi dan Misi Ditreskrimsus Polda Daerah Istimewa Yogyakarta

Adapun visi dan misi Ditreskrimum Polda Daerah Istimewa Yogyakarta adalah sebagai berikut:

1. Visi Ditreskrimsus Polda DIY

   Terwujudnya Ditreskrimksus Polda DIY yang profesional, proporsional, modern, akuntabel dalam penanganan tindak pidana khusus guna memberikan kepastian hukum dan rasa keadilan pada masyarakat di wilayah Yogyakarta.

2. Misi Ditreskrimsus Polda DIY

   a. melaksanakan penegakan hukum secara profesional, objektif, proporsional, transparan dan akuntabel guna menjamin kepastian hukum dan rasa keadilan melalui giat lidik sidik tindak pidana khusus di bidang Tindak Pidana ekonomi khusus dan *cyber*, Tindak Pidana Inprodag, Tindak Pidana Tertentu dan Tindak Pidana Korupsi di wilayah hukum Polda D.I. Yogyakarta;

   b. menyelesaikan permasalahan hukum secara profesional dan akuntabel dengan menganalisa kasus beserta penanganannya serta mempelajari dan mengkaji efektifitas pelaksanaan tugas di Ditreskrimsus Polda D.I.Yogyakarta;

   c. melaksanakan pembinaan teknis, koordinasi dan pengawasan operasional serta administrasi penyidikan oleh PPNS di wilayah hukum Polda D.I.Yogyakarta;

d. meningkatkan kemitraan dan sinergi penegakan hukum dengan masyarakat dan instansi/lembaga terkait dengan semangat gotong royong;
e. melaksanakan pengawasan penyidikan tindak pidana khusus secara optimal di lingkungan Polda D.I.Yogyakarta;
f. melakukan proses pengumpulan, pengolahan dan menyajikan informasi data berkaitan tupoksi pada program kegiatan Ditreskrimsus secara berkelanjutan;
g. meningkatkan kualitas dan kompetensi penyidik/penyidik pembantu/personel Ditreskrimsus Polda D.I.Yogyakarta yang profesional, kompeten, unggul, terpercaya, dan berkepribadian;
h. meningkatkan pelayanan di bidang tindak pidana khusus dalam upaya penegakan hukum yang berkeadilan dengan menjunjung tinggi HAM di wilayah hukum Yogyakarta;
i. meningkatkan dukungan sarana prasarana berupa peralatan yang berteknologi tinggi dan modern;
j. mewujudkan penyempurnaan sistem dan metode yang tepat dengan berbasis pada sistem informasi dan komunikasi terkini guna menunjang pelaksanaan tugas penyidikan.

4. 2. 4 Arti Lambang Ditreskrimsus Polda Daerah Istimewa Yogyakarta

Dalam penelitian dengan judul "Analisis Peran Polda Daerah Istimewa Yogyakarta dalam Pengungkapan Kasus *Phishing*," peneliti berfokus pada Direktorat Reserse Kriminal Khusus, terutama bagian Subdit V Siber yang terkait dengan kasus tersebut. Oleh karena itu, peneliti juga akan menjelaskan makna dari logo atau lambang (Ditreskrimsus Polda DIY) yang ditampilkan dalam Gambar 4.2.

1. Perisai dasar segi enam yang berwarna kuning emas.

   Melambangkan bahwa anggota dalam pelaksanaan penegakan hukum sesuai dengan undang-undang yang menjadi dasar hukumnya senantiasa bersikap tegas, arif, bijaksana, profesional, dan proporsional berlandaskan ketentuan hukum yang berlaku dengan memperhatikan hak asasi serta keadilan dan berada dalam koordinasi, pengawasan dan pembinaan teknis penyidik polri.

2. Perisai ke 2 bentuk oval warna kuning emas dengan batas pinggir bergigi yang jumlahnya (28 buah)

   Melambangkan bahwa jumlah PPNS yang telah ada sebanyak (28 instansi).

3. Arti tulisan "Sidik Sakti Indra Waspada"

   a. Sidik

      Mengandung arti jelas, terang yang memiliki makna bahwa setiap peristiwa kejahatan harus dibuat jelas dan terang berdasarkan ketentuan undang-undang yang berlaku untuk mencari kebenaran materil.

b. Sakti

- Bertindak tegas profesional dan proporsenil terhadap setiap pelaku pelanggaran atau kejahatan dari undang-undang yang menjadi dasar hukumnya.
- Melindungi yang tidak bersalah dalam arti melindungi masyarakat berdasarkan hak asasi manusia serta norma norma yang berlaku.

c. Indera

Setiap tindakan yang dilaksanakan senantiasa berdasarkan atas pengamatan yang teliti, tajam, cermat, dan objektif melambangkan proses pengamatan secara menyeluruh

d. Waspada

Mengandung arti kesiap siagaan, mawas diri secara terus menerus dengan memperhitungkan sekecil mungkin faktor kelengahan dan kealpaan

4. Lambang cakra berujung 6 warna merah dan kuning.

Memiliki makna yaitu penyidik memiliki 6 indra yang senantiasa digunakan dalam pelaksanaan tugas di bidang penegakan hukum.



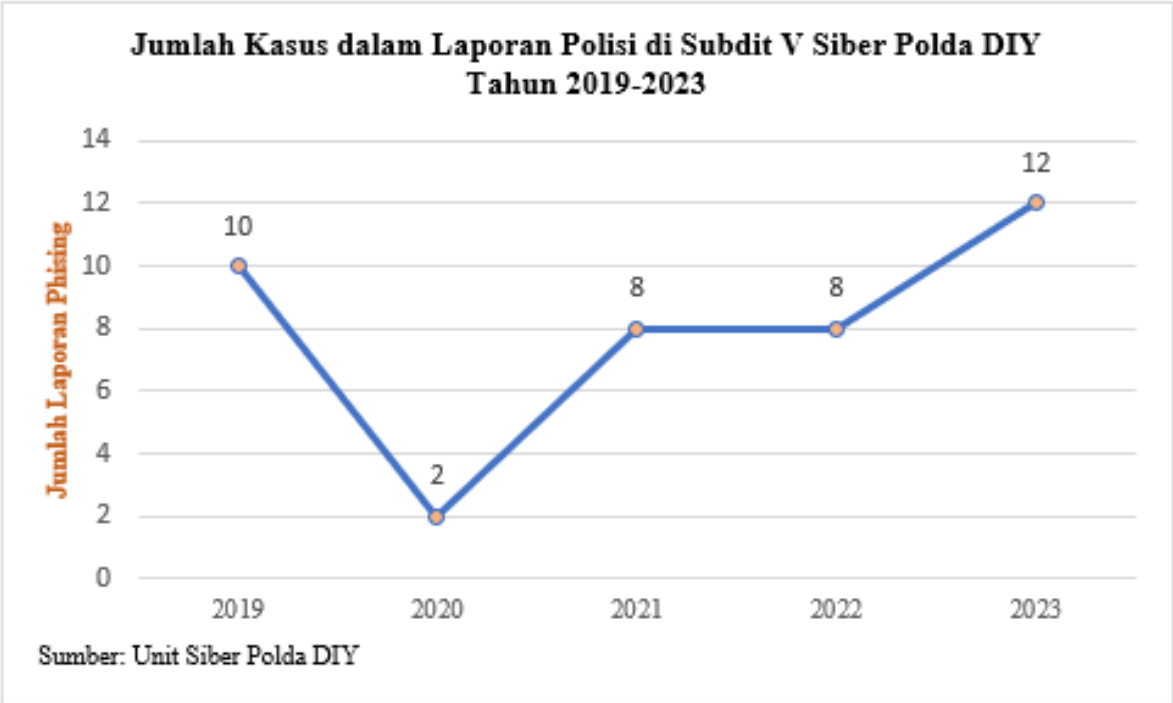
Gambar 4.2 Arti Lambang Ditreskrimsus Polda DIY
(Sumber: Polda DIY, 2024)

4. 3 Tren Permasalahan Kasus *Phishing* di Wilayah Daerah Istimewa Yogyakarta

Daerah Istimewa Yogyakarta (DIY) terkenal sebagai pusat pendidikan, budaya, dan pariwisata yang menarik perhatian banyak orang, terutama generasi milenial. Namun, dalam beberapa tahun terakhir, kasus *Phishing* di Yogyakarta meningkat secara signifikan. Kemudahan akses ke berbagai media sosial telah menyebabkan peningkatan jumlah korban *Phishing* di kota ini.

Mobilitas penggunaan media sosial semakin tinggi, terutama dalam sektor pendidikan, pariwisata, dan bisnis, memberikan akses yang mudah untuk berkomunikasi di berbagai bidang. Situasi ini memberikan peluang bagi individu tidak bertanggung jawab untuk melakukan penipuan *Phishing*. Akses mudah ke berbagai *platform* media sosial memungkinkan para pelaku dengan mudah

menyasar dan memanipulasi korban potensial. Fenomena ini menantang keamanan *online* di DIY.



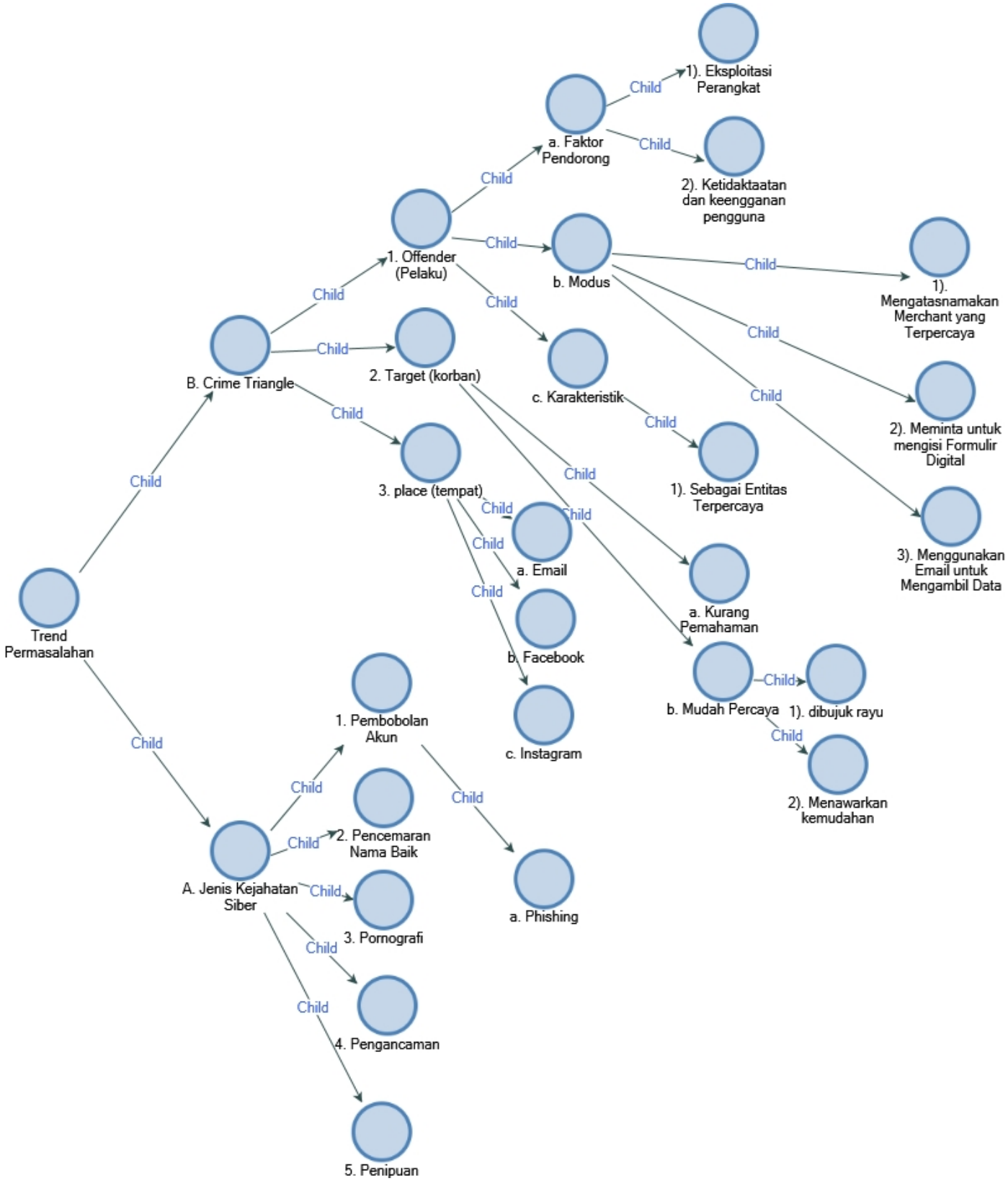
Gambar 4.3 Grafik Jumlah Kasus dalam Laporan Polisi di Subdit V Siber Polda DIY Tahun 2019-2023

Tren kasus *Phishing* di Daerah Istimewa Yogyakarta (DIY) menunjukkan fluktuasi yang signifikan dalam beberapa tahun terakhir. Pada tahun 2019, dilaporkan ada 10 kasus *Phishing* yang terjadi, menunjukkan tingkat kejadian yang cukup tinggi. Namun, terjadi penurunan drastis pada tahun 2020, dengan hanya 2 kasus yang dilaporkan. Meskipun demikian, angka kasus *Phishing* kembali meningkat pada tahun 2021 dan 2022, di mana masing-masing terdapat 8 kasus. Puncaknya terjadi pada tahun 2023, dengan tercatatnya 12 kasus *Phishing*.

Tingginya jumlah kasus *Phishing* yang dilaporkan menunjukkan adanya ancaman serius terhadap keamanan siber di DIY. Grafik tren kasus *Phishing* ini

mencerminkan fluktuasi yang perlu diperhatikan oleh pihak berwenang dan masyarakat. Meskipun tidak dapat dipungkiri bahwa ada peningkatan signifikan dalam kasus *Phishing* pada tahun 2022 dan 2023, perlu dilakukan analisis lebih lanjut untuk memahami faktor-faktor yang menyebabkan fluktuasi ini.

Penelitian lebih lanjut tentang tren kasus *Phishing* di Yogyakarta juga akan membahas konsep Segitiga Kejahatan, yang mencakup analisis terhadap *target* (korban), pelaku (*offender*), dan tempat kejadian (*place*). Dengan memahami karakteristik dan modus pelaku serta profil korban, diharapkan dapat dikembangkan strategi yang lebih efektif dalam mencegah dan menanggulangi kasus *Phishing* di DIY. Gambar IV.3 mencerminkan hasil analisis yang telah diolah oleh peneliti menggunakan perangkat lunak Nvivo 12. Rincian ini terlihat dengan jelas sebagai berikut.



Gambar 4.4 Peta Analisa Tren Permasalahan Kasus *Phishing*

4. 3. 1 Jenis Kejahatan Siber di Polda Daerah Istimewa Yogyakarta

Dalam penelitian ini, Subdit V Siber Ditreskrimsus Polda Daerah Istimewa Yogyakarta menangani berbagai jenis kejahatan siber, yang dibagi menjadi lima kategori, yaitu:

1. Pembobolan Akun (*Phishing* berkaitan dengan UU ITE)
2. Pencemaran Nama Baik
3. Pornografi
4. Pengancaman
5. Penipuan *Online*

Dalam penelitian ini, peneliti akan lebih memfokuskan pada kasus pembobolan akun dengan modus *Phishing*, yang termasuk dalam lingkup Undang-Undang Informasi dan Transaksi Elektronik (UU ITE). Teori dan penjelasan yang dikembangkan, terutama berfokus pada peran Polda DIY, khususnya Ditreskrimsus bagian Subdit V Siber, dalam menangani kasus *Phishing* ini.

Dalam konteks hukum Indonesia, Undang-Undang Informasi dan Transaksi Elektronik (UU ITE) serta Kitab Undang-Undang Hukum Pidana (KUHP) memiliki peran yang berbeda dalam menangani berbagai jenis kejahatan. KUHP secara umum mengatur tentang hukum pidana di Indonesia, sementara UU ITE lebih spesifik dalam mengatasi kejahatan yang terkait dengan teknologi informasi dan transaksi elektronik. UU ITE mencakup aspek hukum yang berkaitan dengan keamanan dan perlindungan informasi elektronik di dunia maya,

sedangkan KUHP mencakup berbagai tindak pidana, termasuk kejahatan konvensional di dunia nyata.

Penelitian ini menyoroti perbedaan antara kasus *Phishing* yang terjadi secara daring dengan penipuan yang terjadi di tempat atau secara *offline*. Kasus pembobolan akun melalui modus *Phishing* dianggap sebagai tindakan yang masuk dalam ranah UU ITE karena melibatkan unsur elektronik dan teknologi informasi. Sementara itu, kasus penipuan di tempat atau *offline* masuk dalam ranah KUHP karena tidak melibatkan unsur media elektronik atau dunia maya.

Sebagai contoh, pasal 378 dalam KUHP mendefinisikan penipuan sebagai perbuatan seseorang yang dengan niat untuk mendapatkan keuntungan, baik untuk dirinya sendiri maupun orang lain secara melanggar hukum. Sementara itu, UU ITE Pasal 28 ayat (1) dan Pasal 45A ayat (1) menyatakan bahwa setiap individu yang dengan sengaja dan tanpa hak menyebarkan berita bohong dan menyesatkan dalam transaksi elektronik dapat dihukum dengan penjara maksimal enam tahun dan/atau denda hingga satu miliar rupiah.

Sebagai contoh kasus yang melibatkan pelanggaran UU ITE, seseorang dapat terlibat dalam *Phishing* dengan menciptakan situs web atau mengirim pesan palsu untuk mendapatkan informasi pribadi dari individu lain. Pelanggaran se*Mac*am ini dapat termasuk dalam Pasal 30, Pasal 5 ayat (1), dan/atau Pasal 51 ayat (1) UU ITE. Di sisi lain, contoh penipuan yang melibatkan KUHP dapat terjadi dalam situasi kehidupan sehari-hari ketika seseorang menggunakan trik atau kebohongan untuk memanipulasi orang lain agar menyerahkan barang atau memberikan hutang, yang melanggar Pasal 378 KUHP.

Dalam kesimpulannya, UU ITE dan KUHP memiliki peran yang berbeda dalam menangani berbagai jenis kejahatan, dan penelitian ini mengidentifikasi perbedaan serta kesamaan dalam pengaturan hukum keduanya.

4. 3. 2 The *Crime* Triangle

Peneliti dalam pengungkapan hasil penelitian ini menggunakan *The Crime triangle* (Segitiga kejahatan). Segitiga kejahatan juga dikenal sebagai segitiga analisis masalah dan digunakan untuk menjelaskan faktor-faktor yang diperlukan dalam mencegah kejahatan. Kejahatan terjadi ketika pelaku *(offender)* yang termotivasi berinteraksi pada waktu dan tempat *(place)* tertentu dengan korban *(target)* yang sesuai dan kurangnya kontrol keamanan yang memadai. Kelemahan dalam sistem keamanan mempermudah pelaku kejahatan mencapai tujuannya, dan keberhasilan suatu kejahatan bergantung pada seberapa efektifnya pengamanan dalam melindungi area kejahatan.

4. 3. 2. 1 *Offender (Pelaku)*

Pelaku *Phishing* merupakan seseorang atau kelompok yang dengan sengaja memiliki tujuan untuk memperoleh informasi pribadi seseorang melalui teknik pengelabuan. Informasi yang menjadi *target Phishing* melibatkan data pribadi, data akun, dan data keuangan. Peneliti akan menjelaskan modus, karakteristik, dan faktor yang terkait dengan pelaku kasus *Phishing*.

1. Faktor Pendorong Pelaku *Phishing*

   Faktor yang mendorong perlakukan melakukan *Phishing* di Daerah Istimewa Yogyakarta sebagai berikut:

a. Eksploitasi Perangkat

Eksploitasi perangkat yang umumnya digunakan oleh pelaku bertujuan untuk memanfaatkan celah keamanan atau kerentanan pada sistem, perangkat lunak, atau jaringan. Hal ini dilakukan agar mereka dapat mengakses data atau informasi sensitif tanpa izin, mencuri kredensial, atau menyebabkan gangguan pada perangkat yang disasar. Sebagaimana diungkapkan oleh Bapak Bripka Cahyono Budi.

> "Ada juga yang istilahnya dia itu permasalahan, seperti misal mba nya mau melakukan transaksi di ATM, mungkin transaksi itu ada trouble atau gangguan yang mungkin mba sudah transfer tapi tidak sampai ke rekening yang dituju. Mungkin karena error." Budi (2023)

b. Ketidaktaatan dan Keengganan Pengguna

Ketidaktaatan dan penolakan dari pengguna yang menjadi korban *Phishing* mencakup perilaku kurang patuh dan kurangnya kesediaan untuk mengikuti praktik keamanan. Ini dapat mencakup keengganan untuk memverifikasi identitas sebelum memberikan informasi pribadi atau mengabaikan peringatan keamanan, yang dapat memberikan peluang bagi penyerang *Phishing* untuk berhasil menjalankan upayanya. Seperti yang diungkapkan oleh bapak Bripka Cahyono Budi (2023), mereka mungkin akan meminta nomor ATM, rekening, PIN, atau data pribadi lainnya dengan alasan tertentu, seperti membantu atau memberikan bantuan palsu. Ketika korban panik, mereka cenderung memberikan informasi tersebut tanpa berpikir panjang, padahal seharusnya kode rahasia seperti PIN atau OTP bersifat privasi dan hanya diketahui oleh pemiliknya. Jika informasi tersebut jatuh ke tangan orang lain, maka akun dan privasi korban dapat

terancam. Meskipun kerugian yang dialami mungkin akan diganti, namun jika kesalahan berasal dari korban sendiri dalam memberikan informasi rahasia, hal tersebut mungkin tidak dapat dipertanggungjawabkan.

2. Modus Pelaku dalam *Phishing*

   a. Mengatasnamakan Merchant Terpercaya

      Modus pelaku yang digunakan biasanya mengatasnamakan merchant terpercaya. Dalam kasus *Phishing* umumnya melibatkan upaya penipuan dengan menyamar sebagai entitas bisnis yang sah dan dapat dipercaya. Penyerang/pelaku mencoba meniru tampilan situs web atau komunikasi resmi dari merchant terkemuka untuk memancing korban memberikan informasi pribadi atau keuangan mereka. Seperti yang dijelaskan oleh Bapak Brigadir Muhammad Robani (2023), modus tersebut sering kali mengatasnamakan merchant terkait dengan belanja *online*.

      Maksudnya adalah untuk memanfaatkan kepercayaan pengguna terhadap merchant tersebut, sehingga mereka secara tidak curiga mengungkapkan data sensitif yang kemudian dapat disalahgunakan oleh pelaku *Phishing*.

   b. Meminta untuk Mengisi Formulir Digital/*Link*

      Maksud dari meminta untuk mengisi formulir digital atau mengklik *link* dalam modus *Phishing* adalah untuk menipu korban agar memasukkan informasi pribadi atau keuangan mereka. Penyerang membuat formulir palsu atau tautan yang menyerupai layanan atau situs resmi untuk mengelabui korban. Tujuannya adalah untuk mencuri

kredensial login, informasi kartu kredit, atau data pribadi lainnya. Korban yang tidak waspada dan mengisi formulir atau mengikuti tautan ini dapat mengalami pencurian identitas atau kehilangan informasi penting. Bapak Brigadir Muhammad Robani Menjelaskan mengenai cara pelaku untuk mengirimkan *link*.

> "Meminta korban untuk mendaftarkan akun instragam atau bahkan media sosialnya sebagai syarat penggunaan layanan merchant. Contoh, misal di instragam saya mau menggunakan layanan centang biru, saya harus masukan akun instragam saya karena pelaku mengirimkan formulir digital." (Robani, 2023)

c. Menggunakan *Email* untuk Mengambil Data

Modus kasus *Phishing* melalui *email* bertujuan untuk memperoleh data pribadi atau keuangan dengan cara menyesatkan penerima *email*. Penyerang menggunakan *email* palsu yang meniru komunikasi resmi dari lembaga atau perusahaan terpercaya. Dalam *email* tersebut, korban diiming-imingi dengan informasi palsu atau diperingatkan tentang situasi yang mendesak, sering kali disertai dengan tautan atau lampiran yang sebenarnya bersifat berbahaya. Tujuan akhirnya adalah agar korban memberikan informasi sensitif atau mengklik tautan yang dapat mengarah pada eksekusi kode berbahaya. Dalam penjelasan bapak Brigadir Muhammad Robani mengenai penggunaan *email* untuk pengambilan data korban.

> "Atau dengan cara baru, biasanya pelaku ini akan mengambil alih akun *email* kita setelah itu pelaku akan merubah sandi, password, akun pemulihan, nomer pemulihan akan dirubah semua dan akhirnya akan digunakan oleh pelaku untuk menggunakan beberapa media sosial kita yang menggunakan *email* sebagai data awal."(Robani, 2023)

3. Karakteristik Pelaku *Phishing*

   a. Sebagai Entitas Terpercaya

      Pelaku *Phishing* cenderung menyamar sebagai entitas terpercaya karena itu memudahkan mereka mendapatkan kepercayaan dari calon korban. Dengan menyusun tampilan atau pesan yang meniru organisasi atau layanan yang dikenal oleh korban potensial, pelaku *Phishing* dapat menciptakan ilusi keamanan. Hal ini membuat korban lebih rentan terhadap manipulasi, karena mereka mungkin tidak curiga dan lebih cenderung memberikan informasi pribadi atau mengklik tautan yang sebenarnya bersifat merugikan. Oleh karena itu, karakteristik menyamar sebagai entitas terpercaya adalah strategi efektif bagi pelaku *Phishing* untuk mencapai tujuan penipuannya. Menurut bapak Bripka Cahyono Budi (2023), seharusnya tindakan seperti itu seharusnya dilakukan oleh pihak bank secara resmi. Sementara menurut Brigadir Muhammad Robani (2023), tren *Phishing* saat ini melibatkan pemalsuan identitas berbagai entitas, seperti merchant, individu, atau *platform* digital, dengan tujuan mencari kesalahan atau kelengahan dari korban yang menggunakan atau membutuhkan layanan tersebut.

4. 3. 2. 2 *Target (Korban)*

Korban *Phishing* merupakan seseorang atau entitas yang terjebak oleh praktik penipuan *online*. Mereka dapat menjadi *target* penyerangan *Phishing* yang menggunakan trik seperti *email* palsu atau situs web tiruan. Korban pada umumnya diiming-imingi atau disesatkan untuk mengungkapkan informasi

pribadi atau keuangan, yang kemudian dapat disalahgunakan oleh pelaku *Phishing*. Adapun penyebab korban mengalami *Phishing* diantaranya:

1. Kurang pemahaman

Kurang pemahaman korban dalam kasus *Phishing* mencakup ketidakmampuan mereka untuk mengenali upaya penipuan *online*. Ini terjadi ketika korban tidak sepenuhnya memahami tanda-tanda atau teknik yang digunakan oleh penyerang, sehingga mereka dapat terjebak dalam memberikan informasi pribadi atau keuangan secara tidak sengaja. Faktor ini memperbesar risiko pencurian data karena kurangnya kesadaran tentang upaya penipuan yang dilakukan oleh pelaku *Phishing*. Seperti yang dijelaskan oleh bapak Bripka Cahyono Budi dan Brigadir Muhammad Robani mengenai kurang pemahaman korban.

> "Kalau sudah beralih ke orang lain pasti sudah otomatis akun kita dipegang orang lain. Kadang orang itu kurang pemahamannya disitu."(Budi, 2023).

> "kesadaran perlu ditingkatkan, karena masyarakat DIY cenderung belum memahami karakteristik dan fungsi medsos yang digunakan sehingga ada ketidakpahaman tersebut seringkali digunakan sebagai celah oleh para pelaku tindak pidana. Terkendala, masyarakat masih pasif. Karena mereka sendiri tidak peduli dan hanya media untuk komunikasi." (Robani, 2023)

a. Mudah Percaya

Mudah percaya pada korban *Phishing* mengacu pada kecenderungan korban untuk dengan cepat mempercayai informasi atau tautan yang diterima dari penyerang *Phishing*. Disebabkan oleh kurangnya kehati-hatian atau pemahaman tentang teknik penipuan *online*. Korban yang mudah percaya cenderung memberikan informasi pribadi atau

keuangan mereka tanpa memverifikasi keaslian sumber, sehingga memudahkan pelaku *Phishing* untuk mencapai tujuannya. Sebagaimana yang dijelaskan oleh bapak Bripka Cahyono Budi. Berikut faktor yang menyebabkan korban mudah percaya terhadap pelaku diantaranya:

b. Dibujuk Rayu

Dalam *Phishing* mengacu pada upaya yang dilakukan oleh penyerang untuk mempengaruhi korban agar memberikan informasi pribadi atau keuangan. Ini bisa mencakup iming-iming hadiah palsu, ancaman palsu, atau cerita yang dirancang untuk mengelabui korban. Penyerang menggunakan teknik ini untuk merayu korban agar turut serta dalam praktik *Phishing* tanpa curiga, sehingga memudahkan mereka untuk mendapatkan akses ilegal atau mencuri data sensitif. Menurut Bripka Cahyono Budi (2023), dalam praktik *Phishing*, salah satu strategi pertama yang digunakan untuk menipu korban adalah dengan menggunakan bahasa yang bersifat membuai atau merayu.

2. Menawarkan Kemudahan

Melibatkan penawaran palsu dari pelaku kepada korban dengan tujuan memancing mereka memberikan informasi pribadi atau keuangan. Contoh termasuk klaim palsu tentang keuntungan atau insentif, seperti diskon besar, hadiah, atau layanan eksklusif. Penyerang mencoba membuat korban merasa bahwa dengan berpartisipasi atau mengikuti instruksi yang diberikan, mereka akan mendapatkan manfaat atau kemudahan tertentu. Ini adalah trik untuk

memanfaatkan rasa ingin tahu atau keinginan korban, sehingga mereka dengan mudah terjebak dalam praktik *Phishing*.

> "kalau mengelabui korbannya yang pertama itu mungkin dengan bahasa *Phishing* itu kayak bujuk rayu, jadi mereka itu menawarkan kemudahan. Misal kita mempunyai tabungan rekening di bank tertentu. Misal bank A, bank B dan bank C nanti kalau mengeluarkan produk itu ada keringanan untuk biaya transaksinya. Yang biasanya Rp 6.000 atau Rp 10.000 mungkin jadi Rp 2.500 atau Rp 3.000 atau sebaliknya kita tetap menggunakan beban transaksi yang lama dari situlah mungkin awal mulanya." (Budi, 2023).

4. 3. 2. 3 *Place (Tempat)*

Dalam kasus *Phishing*, "tempat" biasanya merujuk pada lingkungan *online*. Proses terjadinya *Phishing* melalui komunikasi digital, seperti *email* palsu, situs web tiruan, atau pesan teks yang dirancang untuk menipu korban. Oleh karena itu, tempat terjadinya *Phishing* dapat melibatkan *platform online* seperti *email*, situs web palsu, atau media sosial, di mana penyerang berusaha memperdaya korban agar memberikan informasi pribadi atau keuangan mereka.

1. *Email*

   Penyerang *Phishing* seringkali memilih *email* sebagai tempat untuk menjalankan upayanya karena *email* merupakan sarana komunikasi yang umum digunakan dan dapat mencapai banyak orang. Mereka mengirimkan *email* palsu yang menyerupai pesan resmi dari organisasi atau layanan terpercaya, mencoba membuat korban percaya. *Email* memberikan *platform* yang efektif untuk menyertakan tautan berbahaya atau lampiran yang dapat digunakan untuk mencuri informasi sensitif ketika korban memercayai keaslian pesan tersebut. Oleh karena itu, *email* sering dijadikan tempat utama

oleh pelaku *Phishing* untuk menjalankan transaksi penipuannya. Seperti yang dijelaskan oleh bapak Brigadir Muhammad Robani.

> "Pelaku *Phishing* sering menggunakan *email* sebagai sarana karena *email* merupakan salah satu komunikasi daring yang umum digunakan dan tersebar luas." (Robani, 2023)

2. *Facebook*

Pelaku *Phishing* menggunakan *Facebook* karena *platform* ini menyediakan akses ke banyak informasi pribadi pengguna, seperti detail personal, hubungan sosial, dan kebiasaan. Dengan memanfaatkan fitur pesan atau membuat halaman palsu, pelaku *Phishing* dapat menyebarkan penipuan dan mencuri informasi sensitif dari pengguna yang mungkin kurang waspada. Dalam penjelasan bapak Brigadir Muhammad Robani.

> "*Facebook*, media sosial besar dengan jumlah pengguna yang sangat besar. Pelaku *Phishing* menggunakan *Facebook* karena di *platform* ini terdapat beragam informasi pribadi pengguna, mulai dari detail personal hingga hubungan sosial. Dengan memanfaatkan fitur pesan atau membuat halaman palsu, pelaku *Phishing* dapat menyebarkan penipuan dan mencuri informasi sensitif dari pengguna *Facebook* yang kurang waspada." (Robani, 2023).

3. *Instagram*

Pelaku *Phishing* menggunakan *Instagram* sebagai tempat untuk menjalankan upaya penipuan karena *Instagram* merupakan *platform* media sosial populer dengan banyak pengguna. Mereka dapat membuat akun palsu atau mengirim pesan palsu melalui direct message untuk menarik perhatian korban. *Instagram* juga menyediakan berbagai fitur, seperti tautan dalam bio dan story, yang dapat dimanfaatkan untuk menyematkan tautan *Phishing* atau mengarahkan korban ke situs web palsu. Oleh karena itu, popularitas dan

fungsionalitas *Instagram* membuatnya menjadi *target* yang menarik bagi pelaku *Phishing* untuk mencoba menipu pengguna dan memperoleh informasi pribadi mereka. Seperti yang dijelaskan oleh bapak Brigadir Muhammad Robani.

> "*Instagram* itu *platform* berbagi foto dan video yang populer, di mana banyak pengguna membagikan momen pribadi dan informasi secara visual. Pelaku *Phishing* dapat memanfaatkan fitur ini untuk membuat penipuan yang menarik, seperti akun palsu yang meniru selebriti atau perusahaan, guna menarik perhatian pengguna dan mendapatkan informasi pribadi." (Robani, 2023).

4. 4 Mekanisme Pengungkapan Polda DIY terhadap Kasus *Phishing* di Wilayah Daerah Istimewa Yogyakarta

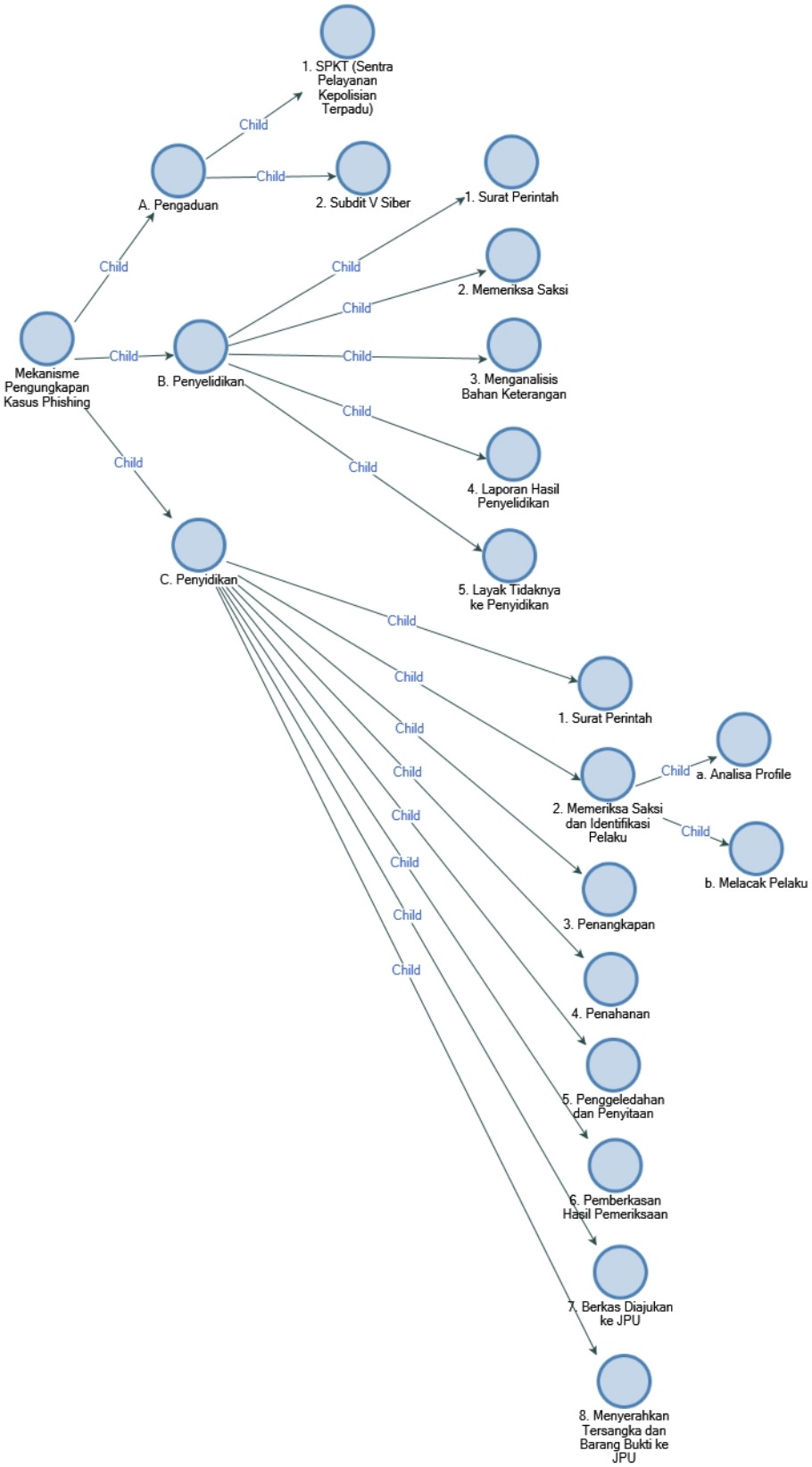
Mekanisme pengungkapan mencakup serangkaian langkah yang diambil oleh tim penyidik Subdit V Siber Polda DIY dalam menangani perkara, dimulai dari pengaduan awal pelapor hingga proses penyidikan. Jika korban mengalami tindak kriminal atau *Phishing*, pelapor dapat melaporkan kejadian tersebut di kantor polisi terdekat, seperti Polsek, Polres, Polda, atau Mabes Polri. Sebagai contoh, jika korban Y dari masyarakat kota Yogyakarta terkena tindak pidana *Phishing*, pelaporan kasus harus dilakukan di kantor polisi terdekat, misalnya Polda DIY. Meskipun pelaku berada di luar wilayah kota Yogyakarta, Polda DIY tetap bertanggung jawab dalam penanganan kasus tersebut.

Berdasarkan Peraturan Pemerintah Republik Indonesia Nomor 23 Tahun 2007 mengenai Daerah Hukum Kepolisian Negara Republik Indonesia, Pasal 4 ayat (1) menyatakan bahwa :

1. Daerah hukum Kepolisian Markas Besar (MABES) Polri untuk wilayah Negara Kesatuan Republik Indonesia.

2. Daerah Hukum Kepolisian Daerah (POLDA) untuk Wilayah Provinsi.
3. Daerah hokum Kepolisian Resort(POLRES) untuk wilayah Kota/Kabupaten.
4. Daerah hukum Kepolisian Sektor (POLSEK) untuk wilayah Kecamatan.

Di samping itu, *Software* NVivo 12 dimanfaatkan untuk analisis hasil wawancara peneliti mengenai prosedur pengungkapan kasus *Phishing* di Polda DIY di Daerah Istimewa Yogyakarta. Pelapor pertama-tama mengunjungi bagian piket Ditreskrimsus sebelum memulai proses penyelidikan. Jika ditemukan indikasi tindak pidana, penyidikan akan dilakukan sebagai langkah selanjutnya.



Gambar 4.5 Peta Analisis Mekanisme Pengungkapan Polda DIY Terhadap Kasus *Phishing* di Wilayah Daerah Istimewa Yogyakarta

4. 4. 1 Pengaduan

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 Brigadir Muhammad Robani (2023), dalam praktik *Phishing*, tidak ada biaya yang secara langsung melibatkan korban. Semua biaya untuk penyelidikan dan pengusutan telah dianggarkan sebelumnya.

Berikut adalah Mekanisme pengungkapan kasus *Phishing* di Daerah Istimewa Yogyakarta yang terkait dengan pelaporan pelapor kepada SPKT dan piket Subdit V Siber Polda Daerah Istimewa Yogyakarta:

1. **SPKT (Sentra Pelayanan Kepolisian Terpadu)**

   Sentra Pelayanan Kepolisian Terpadu (SPKT) memiliki fungsi memberikan pelayanan kepolisian kepada masyarakat melalui penerimaan dan penanganan laporan atau pengaduan, pemberian bantuan atau pertolongan, serta pelayanan surat keterangan. Ruang Sentra Pelayanan Kepolisian Terpadu Polda Daerah Istimewa Yogyakarta menjadi lokasi pertama bagi pelapor (korban) dalam melaporkan kasus *Phishing*. Berikut adalah mekanisme pelaporan ke SPKT Polda DIY:

   a. Pelapor membawa identitas diri (KTP) dan bukti-bukti penipuan terkait peristiwa/kejadian.

      Pelapor mengunjungi ruang SPKT, mengisi buku tamu, dan kemudian menyampaikan laporannya kepada petugas SPKT Polda DIY.

Hal ini sesuai dengan informasi dari bapak Brigadir Muhammad Robani S.H dan Bripda Riski Praditya Putra Polda DIY, yang menekankan bahwa.

"...Setelah itu korban membuat laporan awal ke SPKT depan" (Putra, 2023)

"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 yang tadi." (Robani, 2023)

Kemudian, pihak pelapor 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. Sesuai dengan yang dijelaskan oleh pelapor. Sebagaimana yang dikemukakan oleh bapak Brigadir Muhammad Robani S.H

"...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 (screenshot percakapan,website yang digunakan oleh pelaku maupun akun dari pelaku, dll)" (Robani, 2023)

b. Jika ditindaklanjuti petugas akan menyusun surat rekomendasi untuk gelar awal perkara

Ketika korban atau pelapor mengadakan konsultasi di bagian piket Ditreskrimsus Polda, mereka akan menceritakan peristiwa *Phishing* yang mereka alami dan menunjukkan bukti yang cukup. Petugas piket akan menilai 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. Bripda Riski Praditya Putra, Banum Pembantu Subdit V Siber Polda DIY, menyatakan hal tersebut sesuai dengan ungkapannya.

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

Surat rekomendasi hasil gelar awal perkara yang berwarna pink tidak hanya digunakan dalam kasus tindak pidana *Phishing*, melainkan juga pada berbagai kasus lain yang terkait dengan "Direktorat Reserse Kriminal Khusus" seperti penipuan, *illegal logging*, pencemaran nama baik, peretasan akun, pornografi, korupsi, dan berbagai kasus lain yang relevan dengan Ditreskrimsus.

2. Subdit V Siber

Mekanisme Pengungkapan Pelapor dari ruang SPKT ke Piket Ditreskrimsus bagian Subdit V Siber Polda DIY sebagai berikut:

a. Pelapor (Korban Kasus *Phishing*) Mengunjungi Ditreskrimsus untuk melakukan Konsultasi dan jika:

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 bapak Bripda Riski Praditya Putra

> "...Setelah itu 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." (Putra, 2023)

Pelapor atau korban (kasus penipuan jual beli *online*) diharuskan memenuhi persyaratan berikut ketika melakukan konsultasi di piket Direktorat Reserse Kriminal Khusus bagian Subdit V Siber Polda DIY. Persyaratan tersebut mencakup:

1) Menyertakan fotokopi KTP/KK
2) Menunjukkan tangkapan layar transfer
3) Menunjukkan tangkapan layar percakapan
4) Membawa salinan rekening koran, tangkapan layar aplikasi, dan informasi mengenai website yang digunakan oleh pelaku.

b. Jika kasus dapat ditindaklanjuti, petugas atau piket bagian Subdit V Siber Ditreskrimsus mengisi formulir rekomendasi hasil gelar awal perkara.

Ketika korban berkonsultasi di piket Siber Polda DIY, dimana mereka merinci kasus *Phishing* yang dialami dan menunjukkan bukti yang memadai, petugas Subdit V Siber Polda DIY melakukan penilaian apakah kasus yang dijelaskan oleh korban/pelapor memiliki unsur tindak pidana atau tidak. Dijelaskan oleh bapak Bripda Riski Praditya Putra

> "...Kalau memenuhi unsur pidana ITE lalu diarahkan ke Krimsus (Kriminal Khusus) yang menangani dari Direktorat Reserse Kriminal Khusus unit Siber. Setelah itu, korban nanti menceritakan kronologinya seperti apa terus kapan,dimana pokoknya semua itu diceritakan nanti yang piket ini biasanya kalau tindak pidana itu memenuhi unsur itu langsung

dibuatkan surat laporan. Jadi, mengisi kertas pink, kertas pengaduan nanti itu kronologi disitu diisi seperti hari, tanggal, unsur pidananya apa setelah itu nanti kembali lagi ke SPKT untuk dibuatkan Surat Pengaduan. ” (Putra, 2023)

Setelah menguraikan kronologi kasusnya, petugas mengisi formulir berwarna pink tersebut untuk keperluan penyusunan surat pengaduan. Proses ini bertujuan agar surat pengaduan dapat dibuat dengan informasi yang lengkap dan akurat, mencakup rincian kejadian serta kerugian yang dialami oleh pelapor (korban) dalam kasus *Phishing.*

c. Pelapor (Korban) membawa surat rekomendasi hasil gelar awal perkara ke Subdit Ditreskrimsus.

Sebagaimana yang diungkapkan oleh Bripda Riski Praditya Putra,

“Setelah dari sana nanti mendapatkan Surat Pengaduan terus dibawa lagi ke sini mba (Krimsus) dengan membawa kertas pink tersebut.” (Putra, 2023)

Setelah menguraikan kronologi kasusnya, petugas mengisi formulir berwarna pink tersebut untuk keperluan penyusunan surat pengaduan. Proses ini bertujuan agar surat pengaduan dapat dibuat dengan informasi yang lengkap dan akurat, mencakup rincian kejadian serta kerugian yang dialami oleh pelapor (korban) dalam kasus *Phishing*.

Kemudian, petugas SPKT mengeluarkan Surat Tanda Penerimaan Laporan (STPL) dan laporan pengaduan (Model B) atas arahan dari Direktorat Reserse Kriminal Khusus Polda DIY, bagian Subdit V Siber. Format surat laporan yang dibuat oleh petugas SPKT mencakup identitas pelapor, kronologi kejadian penipuan *Phishing*, dan kerugian yang dialami oleh pelapor (korban). STPL ini berfungsi sebagai bukti resmi yang tidak

boleh dihapus, dan harus selalu dibawa oleh pelapor/korban untuk mengakses perkembangan penyidikan terhadap kasus *Phishing* tersebut. Surat ini akan ditandatangani oleh pelapor dan pejabat yang berwenang atau pimpinan SPKT Polda Daerah Istimewa Yogyakarta, sesuai dengan informasi yang disampaikan dalam pengungkapan bapak Bripda Riski Praditya Putra

> "...Setelah dari sana nanti mendapatkan Surat Pengaduan terus dibawa lagi ke sini mba (Krimsus) dengan membawa kertas pink tersebut. kita akan membuat SPTL (surat tanda penerimaan laporan) agar nanti korban ingin mengetahui perkembangan kasusnya wajib membawa SPTL. oh iya mba, laporan pengaduan itu ada 2 jenis yaitu, laporan pengaduan model A dan laporan pengaduan model B." (Putra, 2023)

Adapun perbedaan model A dan model B yang berkaitan dengan Pasal 5 (Peraturan Kepala Kepolisian Negara Republik Indonesia Nomor 14 Tahun 2012 tentang Manajemen Penyidikan Tindak Pidana) yaitu:

1) Laporan Polisi/Pengaduan terdiri dari:
   a. Laporan Polisi Model A dan
   b. Laporan Polisi Model B.
2) Laporan Polisi Model A sebagaimana dimaksud pada ayat (1) huruf a adalah laporan polisi yang dibuat oleh anggota Polri yang mengalami, mengetahui atau menemukan langsung peristiwa yang terjadi.
3) Laporan Polisi Model B sebagaimana dimaksud pada ayat (1) huruf b adalah laporan polisi yang dibuat oleh anggota Polri atas laporan pengaduan yang diterima dari masyarakat,

Laporan polisi Model A adalah laporan yang disusun oleh petugas kepolisian setelah menyaksikan langsung suatu kejadian,

contohnya, seorang polisi di daerah Kaliurang mendengar dan melihat kasus *Phishing*. Dalam hal ini, polisi membuat laporan sendiri tanpa menginstruksikan korban untuk melapor ke SPKT. Sebaliknya, laporan polisi Model B dibuat oleh pelapor atau korban yang melaporkan peristiwa kepada pihak berwajib, seperti ruang SPKT, dan meminta kepolisian untuk menyelidiki masalah yang dialaminya.

Setelah laporan Model B dibuat, surat tanda penerimaan laporan (STPL) diterbitkan oleh SPKT. STPL tersebut dikirimkan oleh pihak SPKT Polda DIY ke Subdit V Siber Polda DIY untuk tindak lanjut kasus *Phishing*. Jika pelapor ingin mengetahui perkembangan kasus atau mengurusnya, pelapor membawa STPL sebagai bukti saat berbicara dengan petugas piket Ditreskrimsus bagian Subdit V Siber. Saat diminta bukti STPL, petugas piket Subdit V Siber akan memeriksa nomor surat yang tercantum di lampiran STPL dan memastikan kesesuaian dengan nomor yang ada di lampiran laporan Model B yang dipegang oleh petugas Siber. Selanjutnya, petugas piket Siber Polda DIY akan memeriksa tanggal, bulan, serta hasil perkembangan kasus dalam proses penyelidikan dan penyidikan.

4. 4. 2 Penyelidikan

Menurut "Undang-Undang Republik Indonesia Nomor 8 Tahun 1981 tentang Kitab Undang-Undang Hukum Acara Pidana (KUHAP)," penyelidikan adalah serangkaian tindakan mencari bukti tindak pidana, misalnya *Phishing*,

untuk menentukan apakah perlu dilakukan penyidikan. Penyidik, seperti disampaikan oleh bapak Bripda Riski Praditya Putra

“...Yang kedua adalah naik ke tahap penyelidikan, disini kami mencari bukti adanya tindak pidana.” (Putra, 2023)

Berdasarkan "Peraturan Kepala Kepolisian Negara Republik Indonesia Nomor 14 Tahun 2012 tentang Manajemen Penyidikan Tindak Pidana" menyebutkan sasaran penyelidikan melibatkan

1. orang,
2. benda/barang,
3. tempat,
4. kejadian/peristiwa, dan
5. kegiatan.

Jika berkas korban kasus *Phishing* memenuhi syarat piket "Direktorat Reserse Kriminal Khusus Polda DIY," dan pihak kepolisian juga akan menyelidiki kasus *Phishing* tersebut.

1. Membuat Surat Perintah Tugas, Surat Perintah Penyelidikan, dan SP2HP A1

Surat Perintah Tugas (SPT) merupakan perintah pimpinan untuk melaksanakan tugas penyelidikan *Phishing* . Sementara, Surat Perintah Penyelidikan (SPP) memungkinkan penyelidik melakukan tugas seperti penyitaan, penangkapan, dan penggeledahan sesuai hukum. Bripda Riski Praditya Putra menyatakan bahwa Siber Polda DIY membuat rencana penyelidikan tanpa format baku, hanya menjadwalkan kapan, di mana, dan merencanakan kegiatan yang dapat berubah. Setelah terbitnya SPT dan SPP,

diterbitkan pula SP2HP A1 untuk memberitahu pelapor nomor *handphone*, nama, dan penyidik yang menangani kasus *Phishing*. Menurut Bripda Riski Praditya Putra Subdit V Siber Polda DIY,

> "...Yang pertama kami lakukan itu menyusun surat perintah tugas, surat perintah penyelidikan dan membuat SP2HP A1 yang dilakukan oleh penyidik." (Putra, 2023)

Seorang penyelidik wajib membuat rancangan penyelidikan sesuai Pasal 16 "Peraturan Kepala Kepolisian Negara Republik Indonesia Nomor 14 Tahun 2012 tentang Manajemen Penyidikan Tindak Pidana." Rencana tersebut minimal mencakup

a. surat perintah penyelidikan,
b. identitas penyidik,
c. objek,
d. sasaran,
e. *target* hasil penyelidikan,
f. kegiatan sesuai hukum, peralatan yang diperlukan, waktu pelaksanaan, dan
g. kebutuhan anggaran penyelidikan.

2. Memeriksa Saksi – Saksi

Dalam Pasal 1 nomor 26 "Undang-Undang Republik Indonesia Nomor 8 Tahun 1981 tentang Kitab Undang Undang Hukum Acara Pidana (KUHAP)," disebutkan bahwa saksi adalah individu yang dapat memberikan keterangan terkait suatu perkara pidana yang dia dengar, lihat, atau alami sendiri, dengan memberikan alasan dari pengetahuannya. Namun, dalam putusan Mahkamah Konstitusi (MK), definisi saksi diperluas, mencakup tidak

hanya mereka yang mengalami atau mendengar, tetapi juga setiap orang dengan pengetahuan yang terkait langsung dengan suatu tindak pidana.

> "Lalu setelah kami membuat surat tersebut kami melakukan pemeriksaan kepasa saksi, disini kami meminta keterangan tentang kejadian yang dialami korban dan memeriksa, ada tindakan pindana yang dilakukan." (Putra,2023)

Bripda Riski Praditya Putra, dalam pengungkapannya tentang kasus *Phishing* di Polda DIY, menjelaskan bahwa pemeriksaan saksi terbatas pada pelapor dan saksi dari korban/pelapor. Pemeriksaan dilakukan melalui wawancara untuk mendapatkan keterangan tentang kejadian, dengan tujuan menentukan apakah terdapat unsur tindak pidana atau tidak dalam kasus yang dilaporkan.

3. 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. Bripda Riski Praditya Putra menjelaskan tentang menganalisis bahan keterangan.

> "...Seperti nomor telfon, dompet digital, rekening, *link* yang menjadi alat bukti korban pada saat terjadinya kasus *Phishing*. Setelah itu menganalisa bukti yang didapat dari korban, kita pilah-pilih lagi mba, apakah ada kaitannya dengan tindak pidana. jika kita menemukan adanya tindak pidana yang diterima oleh korban kami akan membuat laporan hasil penyelidikan" (Putra,2023).

4. Membuat Laporan Hasil Penyelidikan

Dalam "Peraturan Kepala Kepolisian Negara Republik Indonesia Nomor 12 Tahun 2009 tentang Pengawasan dan Pengendalian Penanganan Perkara Pidana di Lingkungan Kepolisian Negara Republik Indonesia" pasal 1 nomor 25 adalah laporan tertulis atau lisan kepada atasan yang memerintahkan mengenai hasil penyelidikan. Subdit V Siber Polda DIY, menangani LPH yang mencakup informasi seperti akun penipu, lokasi, waktu, dan kejadian, untuk menentukan apakah terjadi tindak pidana atau tidak. Seperti yang dijelaskan oleh Bapak Bripda Riski Praditya Putra dalam membuat laporan hasil penyelidikan.

> "...Laporan hasil penyelidikan ini adalah temuan-temuan yang dilakukan penyidik. mulai dari informasi korban, waktunya, lokasinya kapan dan pelakunya. Disitu para penyidik dapat menentukan, sebenarnya kasus ini bisa masuk ke tahap penyidikan tidak" (Putra,2023).

5. Menentukan Layak Tidaknya di tahap Penyidikan

Berdasarkan penjelasan dari Brigadir Muhammad Robani dan Bripda Riski Praditya Putra Subdit V Siber Polda DIY mengenai penentuan layak atau tidaknya di tahap penyidikan.

> "Untuk tindak lanjut penanganan (menghentikan penyelidikan atau melanjutkan ke tahap penyidikan)" (Robani, 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" (Putra, 2023).

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.

4. 4. 3 Penyidikan

Dalam Pasal 1 nomor 2 dan nomor 1 dalam "Undang-Undang Republik Indonesia Nomor 8 Tahun 1981 Tentang Kitab Undang-Undang Hukum Acara Pidana (KUHAP)" menjelaskan bahwa penyidikan adalah serangkaian tindakan penyidik sesuai dengan ketentuan undang-undang, bertujuan mencari dan mengumpulkan bukti guna mengungkap tindak pidana, serta menemukan pelakunya. Penyidik adalah pejabat polisi negara Republik Indonesia atau pegawai negeri sipil yang diberi wewenang khusus oleh undang-undang untuk melakukan penyidikan. Seperti yang dijelaskan oleh bapak Brigadir Muhammad Robani dan Bripda Riski Praditya Putra mengenai penyidikan.

“Bisa ditingkatkan ke penyidikan” (Robani, 2023).

“Setelah dari penyelidikan naik ke penyidikan, penyidikan ini kita melakukan investigasi lebih mendalam untuk mengungkapkan fakta yang didapatkan” (Putra, 2023).

1. **Membuat Surat Perintah Tugas Penyidikan (Springas), Surat Perintah Penyidikan (Sprin), SP2HP, Rencana Penyidikan dan Surat Pemberitahuan Dimulainya Penyidikan (SPDP)**

   Springas (surat perintah tugas) berbeda dengan sprin, (surat perintah) karena springas adalah 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, 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. SPDP akan dikirim ke JPU Kejati Yogyakarta dalam waktu 7 hari setelah dikeluarkan surat perintah penyidikan. Seperti yang disampaikan oleh bapak Bripda Riski Praditya Putra mengenai pembuatan springas, sprin, sp2hp, rencana penyidikan dan spdp

> "...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."(Putra, 2023)

2. Memeriksa Saksi – Saksi

Perbedaan antara memeriksa saksi dalam proses penyelidikan dan penyidikan terletak pada fokusnya. 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. Bapak Brigadir Muhammad Robani dan Bripda Riski Praditya Putra mengungkapkan pemeriksaan saksi-saksi

> "...Penyidikan dilakukan untuk mengumpulkan bukti lebih lanjut, menentukan tersangka, dan mencari kejelasan terhadap peristiwa."(Robani, 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." (Putra, 2023)

Dalam Pasal 20 Undang-Undang Republik Indonesia Nomor 8 Tahun 1981 tentang Kitab Undang Undang Hukum Acara Pidana (KUHAP), disebutkan bahwa jika dianggap perlu, penyidik berhak meminta pendapat dari orang ahli atau individu yang memiliki keahlian khusus. Dalam konteks tim penyidik Subdit V Siber Polda DIY, mereka memerlukan bantuan ahli digital forensik untuk menganalisis bukti-bukti digital dan bekerja sama dengan penyedia layanan untuk mengungkap atau mendeteksi identitas pelaku. Adapun mekanisme pengungkapan dalam melakukan investigasi terhadap pelaku sebagai berikut:

a. Menganalisa pro*file*

Menganalisa profil melibatkan evaluasi dan interpretasi informasi terkait seseorang atau sesuatu. Proses ini dapat mencakup aspek-aspek berikut:

1) Identitas Personal

Menilai informasi seperti nama, usia, tempat tinggal, pekerjaan, dan pendidikan.

2) Jejak Digital

Menelusuri aktivitas *online*, termasuk media sosial, untuk memahami perilaku, minat, dan interaksi sosial.

3) Riwayat Pekerjaan dan Pendidikan

Menyelidiki pengalaman pekerjaan dan latar belakang pendidikan

4) Hubungan Sosial

Bagaimana kehidupan yang dilakukan sehari-hari, hubungannya antar keluarga, teman, atau kerabat.

5) Aktivitas Finansial

Memeriksa riwayat transaksi keuangan atau kredit

6) Perilaku dan Kepribadian

Mengidentifikasi pola perilaku dan kepribadian melalui aktivitas *online* dan *offline*.

Seperti yang dijelaskan oleh bapak Brigadir Muhammad Robani dan Bripda Riski Praditya Putra mengenai analisa profil.

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

"...Pada saat memeriksa saksi-saksi kami juga melakukan analisa pro*file* untuk melihat latar belakang pelaku ini, seperti apa dia di kehidupan sehari-hari." (Putra, 2023)

b. Melacak Pelaku

Melacak pergerakan seseorang melalui 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. Penyebaran data melalui DPO di kepolisian dan kerja sama internasional, seperti melalui Interpol dan *Red Notice*, dilakukan untuk mengejar pelaku kejahatan. Seperti yang dijelaskan oleh bapak Bripda Riski Praditya Putra tentang melacak pelaku

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

3. Identifikasi Pelaku Melalui Gelar Perkara, Kemudian melakukan Panggilan/Penangkapan Pelaku

Dalam pasal 1 nomor 14 Undang-Undang Republik Indonesia Nomor 8 Tahun 1981 tentang Kitab Undang Undang Hukum Acara Pidana (KUHAP), tersangka merujuk kepada seseorang yang, berdasarkan bukti permulaan, layak diduga sebagai pelaku tindak pidana. Selanjutnya, mengenai penentuan status tersangka dalam "Peraturan Kepala Kepolisian Negara Republik Indonesia Nomor 12 Tahun 2009 tentang Pengawasan dan Pengendalian Penanganan Perkara Pidana di Lingkungan Kepolisian Negara Republik Indonesia" pada Pasal 66 ayat 1 dan 2 sebagai berikut:

a. Status sebagai tersangka hanya dapat di tetapkan oleh penyidik kepada seseorang setelah hasil penyidikan yang dilaksanakan memperoleh bukti permulaan yang cukup yaitu paling sedikit dua jenis alat bukti.
b. Untuk menentukan memperoleh bukti permulaan yang cukup yaitu paling sedikit dua jenis alat bukti sebagaimana di maksud pada ayat 1 di tentukan melalui gelar perkara. Yang dimana gelar perkara dalam hal ini untuk membantu pimpinan dalam menentukan tersangka dengan bukti - bukti yang sudah jelas dikumpulkan maka pimpinan mengeluarkan surat penetapan tersangka. Setelah surat tersebut dikeluarkan maka terbitlah 3 surat yaitu surat perintah penangkapan, surat perintah penggeledahan dan surat perintah penyitaan, kemudian tim penyidik melakukan penangkapan, penggeledahan dan penyitaan. Seperti yang dijelaskan oleh bapak Bripda Riski Praditya Putra

> "...Setelah itu kami akan melakukan gelar perkara pelaku untuk mengetahui apakah itu benar-benar pelaku. dengan mengumpulkan bukti-bukti yang mengarahkan kepada pelaku. kalau sudah mengetahui pelakunya siapa, 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."(Putra, 2023)

Dalam Pasal 1 nomor 20 Undang-Undang Republik Indonesia Nomor 8 Tahun 1981 tentang Kitab Undang Undang Hukum Acara Pidana (KUHAP), penangkapan dijelaskan sebagai tindakan penyidik yang mengakibatkan pengekangan sementara kebebasan tersangka/terdakwa jika terdapat cukup bukti demi kepentingan penyidikan, penuntutan, dan/atau peradilan sesuai dengan aturan undang-undang. Berikut adalah

syarat-syarat "Penangkapan" dalam pengungkapan kasus penipuan jual beli *online* di Polda Daerah Istimewa Yogyakarta yang sesuai dengan KUHAP:

1) Penangkapan yang tidak sewenang-wenang

   Ditetapkan terhadap individu yang terbukti melakukan kejahatan/tindak pidana, seperti kasus *Phishing*. Penangkapan wajib didasarkan pada bukti awal/permulaan yang memadai sesuai dengan Pasal 184 ayat 1 KUHAP, mencakup alat bukti yang sah seperti keterangan saksi, keterangan ahli, surat, petunjuk, dan keterangan terdakwa.

2) Tidak melakukan kekerasan

   Sesuai dengan Pasal 10 huruf C Peraturan Kepala Kepolisian Negara Republik Indonesia Nomor 8 Tahun 2009, kekerasan tidak boleh digunakan kecuali jika diperlukan untuk mencegah kejahatan, membantu penangkapan pelanggar hukum, atau tersangka, sesuai dengan aturan penggunaan kekerasan.

3) Hak-hak tersangka harus dipenuhi

   Termasuk memberikan surat penangkapan dan menentukan apakah tersangka menggunakan nasehat hukum atau tidak.Jika tersangka tidak menggunakan nasehat hukum, surat penolakan penasehat hukum dibuat. Hak-hak tersangka, baik penolakan maupun penerimaan, dibacakan setelahnya tim penyidik melakukan pemeriksaan tersangka.

4. Melakukan Penahanan

Dalam Pasal 1 Bagian 21 Undang-Undang Republik Indonesia Nomor 8 Tahun 1981 tentang Kitab Undang-Undang Hukum Acara Pidana (KUHAP), penahanan diartikan sebagai tindakan menempatkan tersangka atau terdakwa pada lokasi tertentu oleh penyidik, penuntut umum, atau hakim. Penetapan penahanan dilakukan sesuai dengan ketentuan undang-undang, baik dalam hal maupun cara pelaksanaannya. Dalam pasal 20 KUHAP membagi penahanan menjadi tiga, yaitu:

a. Untuk kepentingan penyidikan, penyidik/penyidik pembantu berwenang melakukan penahanan.
b. Untuk kepentingan penuntutan, penuntutan umum berwenang melakukan penahanan atau penahanan lanjutan.
c. Untuk kepentingan pemeriksaan hakim di sidang

Pada sistem 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. Seperti yang dijelaskan oleh bapak Riski Praditya Putra

"...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."(Putra, 2023)

Dalam pasal 109 ayat 2 “Undang – Undang Republik Indonesia Nomor 8 Tahun 1981 Tentang Kitab Undang – Undang Hukum Acara Pidana (KUHAP)” Dalam hal penyidik menghentikan penyidikan karena tidak terdapat cukup bukti atau peristiwa tersebut ternyata bukan merupakan tindak pidana atau penyidikan dihentikan demi hukum, maka penyidik memberitahukan hal itu kepada penuntut umum, tersangka atau keluarganya. Hal yang membedakan surat pemberhentian proses penyidikan (SP3 Lidik) dengan surat perintah pemberhentian penyidikan (SP3) adalah jika surat pemberhentian proses penyidikan (SP3 Lidik) dikeluarkan apabila proses penyelidikan tidak memiliki unsur pidana sedangkan surat pemberhentian proses penyidikan dikeluarkan dikarenakan kurangnya keterangan saksi dan kurangnya alat bukti yang kuat terkait dengan kasus penipuan berkedok investasi *online* maka diterbitkanlah SP3 (Surat perintah Penghentian Penyidikan) dan diberikan kepada kejaksaan, dan SP2HP A5 ke pelapor sebagai tanda pemberhentian hasil penyidikan.

5. Melakukan Penggeledahan, Penyitaan, Ajukan Permohonan atau Persetujuan ke Pengadilan Negeri

Tindakan penyidik untuk melakukan penggeledahan ditentukan oleh hasil gelar perkara, sebagaimana diatur dalam Pasal 1 nomor (17) dan (18) Undang-Undang Republik Indonesia Nomor 8 Tahun 1981 tentang Kitab Undang-Undang Hukum Acara Pidana (KUHAP). Dalam undang-undang tersebut, terdapat dua jenis penggeledahan, yakni:

a. Penggeledahan rumah

Penggeledahan rumah merujuk pada langkah penyidik untuk memasuki tempat tinggal dan area tertutup lainnya guna melakukan pemeriksaan, penyitaan, atau penangkapan sesuai ketentuan yang diatur dalam undang-undang.

b. Penggeledahan badan

Penggeledahan badan adalah tindakan untuk melakukan pemeriksaan terhadap badan dan/atau pakaian tersangka dengan tujuan mencari barang yang diduga kuat berada di tubuhnya atau dibawanya, dan nantinya barang tersebut dapat disita. Definisi penyitaan, sebagaimana dijelaskan dalam Pasal 1 nomor 16, mencakup serangkaian langkah penyidik untuk mengambil alih dan/atau menyimpan benda bergerak, berwujud atau tidak, demi kepentingan pembuktian dalam proses penyidikan, penuntutan, dan peradilan.

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, penyidik diwajibkan untuk melakukan penggeledahan di tempat tinggal pelaku dengan cara mengeluarkan surat penggeledahan. Dalam penjelesana yang diberikan oleh bapak Bripda Riski Praditya Putra

“...Kami juga melakukan penggeledahan dan penyitaan barang bukti pelaku. penggeledahannya terhadap barang ya mba, alat buktinya itu semisal seperti telfon, buku tabungan yang biasanya digunakan pelaku untuk melakukan kejahatan tersebut.”(Putra, 2023)

Berikut format surat terkait penggeledahan dan penyitaan yang digunakan di Polda Daerah Istimewa Yogyakarta dalam kasus *Phishing*, sesuai "Lampiran Peraturan Kepolisian Negara Republik Indonesia Nomor 6 Tahun 2010 tentang Manajemen Penyidikan Bagi Penyidik Pegawai Negeri Sipil":

a. Surat Permintaan Izin Khusus Penggeledahan kepada Ketua Pengadilan
b. Surat Laporan untuk Persetujuan Penggeledahan kepada Ketua Pengadilan
c. Surat Perintah Penggeledahan
d. Berita Acara Penggeledahan Rumah Tinggal atau Tempat-tempat Tertutup Lainnya
e. Laporan untuk Mendapatkan Persetujuan Penyitaan kepada Ketua Pengadilan
f. Surat Perintah Penyitaan
g. Berita Acara Penyitaan
h. Surat Tanda Penerimaan

Kegiatan penggeledahan ini disesuaikan dengan Pasal 5 Ayat 1 Bagian B yang terdapat dalam "Undang - Undang Republik Indonesia Nomor 8 Tahun 1981 Tentang Kitab Undang - Undang Hukum Acara Pidana (KUHAP)" yang mencakup:

a. Penangkapan, larangan meninggalkan tempat, penggeledahan, dan penahanan;
b. Pemeriksaan dan penyitaan surat;
c. Mengambil sidik jari dan memotret seseorang;
d. Membawa dan menghadapkan seseorang pada penyidik.

Prosedur penggeledahan yang dilakukan oleh tim Subdit V Siber Polda Daerah Istimewa Yogyakarta dalam kasus penipuan jual beli *online* sesuai dengan ketentuan Pasal 33 dalam "Undang - Undang Republik Indonesia Nomor 8 Tahun 1981 Tentang Kitab Undang - Undang Hukum Acara Pidana (KUHAP)" adalah sebagai berikut:

1) Dengan mendapatkan izin tertulis dari ketua pengadilan negeri setempat, penyidik memiliki wewenang untuk melakukan penggeledahan yang dianggap perlu dalam rangka penyidikan.
2) Jika diperlukan, berdasarkan perintah tertulis dari penyidik, petugas kepolisian negara Republik Indonesia dapat memasuki rumah.
3) Setiap kali memasuki rumah, tindakan tersebut harus disaksikan oleh dua orang saksi, terutama jika tersangka atau penghuni rumah memberikan persetujuan.
4) Setiap kali memasuki rumah, tindakan tersebut harus disaksikan oleh kepala desa atau ketua lingkungan, dan dua orang saksi, jika tersangka atau penghuni rumah menolak atau tidak hadir.

5) Dalam waktu 2 hari setelah melakukan penggeledahan, suatu berita acara dan turunannya harus disusun dan disampaikan kepada pemilik atau penghuni rumah yang bersangkutan.

Berdasarkan ketentuan Pasal 34 dalam undang-undang yang disebutkan di atas, diatur bahwa penyidik tidak diizinkan untuk memeriksa atau menyita surat, buku, dan tulisan lain yang tidak memiliki kaitan dengan tindak pidana (*Phishing*) yang sedang diselidiki, kecuali jika benda-benda tersebut terkait dengan tindak pidana yang bersangkutan atau diduga telah digunakan dalam melakukan tindak pidana (*Phishing*) tersebut. Dalam hal tersebut, penyidik wajib segera melaporkan kepada ketua pengadilan negeri setempat untuk mendapatkan persetujuan sebelum melanjutkan tindakan lebih lanjut.

Sementara pada Pasal 34 ayat (1), disebutkan bahwa dalam keadaan yang sangat mendesak dan perlu, di mana penyidik harus segera bertindak dan tidak memungkinkan untuk mendapatkan izin terlebih dahulu, dengan tetap memperhatikan ketentuan Pasal 33 ayat (5), penyidik dapat melakukan penggeledahan dengan rincian sebagai berikut:

a) Pada halaman rumah tersangka bertempat tinggal, berdiam atau ada dan yang ada di atasnya.
b) Pada setiap tempat lain tersangka bertempat tinggal, berdiam atau ada.
c) Di tempat tindak pidana dilakukan atau terdapat bekasnya.
d) Tempat penginapan dan tempat umum lainnya

6. Pemberkasan Hasil Pemeriksaan

Pemberkasan hasil pemeriksaan ini melibatkan kumpulan dokumen penyidikan dari tahap awal pengungkapan *Phishing* hingga pemeriksaan hasil penggeledahan dan penyitaan, membentuk berkas merah. Seperti yang dijelaskan oleh bapak Bripda Riski Praditya Putra (2023), berkas yang dibuat memiliki warna merah dan berisi seperti berita acara serta analisis penyelidik. Berikut ini daftar isi pada berkas dalam buku merah antara lain:

a. Sampul berkas perkara
b. Uraian sampul berkas
c. Profil tersangka
d. Daftar isi berkas perkara
e. Berita acara pendapat
f. Daftar saksi
g. Daftar ahli
h. Daftar barang bukti
i. Daftar tersangka
j. Surat - surat lain atau lampiran

7. Berkas Diajukan Ke Jaksa Penuntut Umum

Berkas diajukan ke JPU Setelah tim penyidik Subdit V Siber Polda DIY menyelesaikan berkas *Phishing* (berkas merah), berkas tersebut akan diserahkan ke Jaksa Penuntut Umum di Kejaksaan Negeri Yogyakarta sebagai lembaga yang berkompeten untuk menangani penuntutan terhadap tindak pidana *Phishing*. Seperti yang diungkapkan oleh bapak Bripda Riski Praditya Putra

> "...Jadi setelah berkasnya jadi kita geser 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, dilampirkan mba. Kita nanti melengkapi itu, setelah itu kita melengkapinya."(Putra, 2023)

8. Menyerahkan Tersangka dan Barang Bukti Ke Jaksa Penuntut Umum

Setelah Jaksa Penuntut Umum menganggap 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 dalam pengungkapan bapak Bripda Riski Praditya Putra dan Brigadir Muhammad Robani

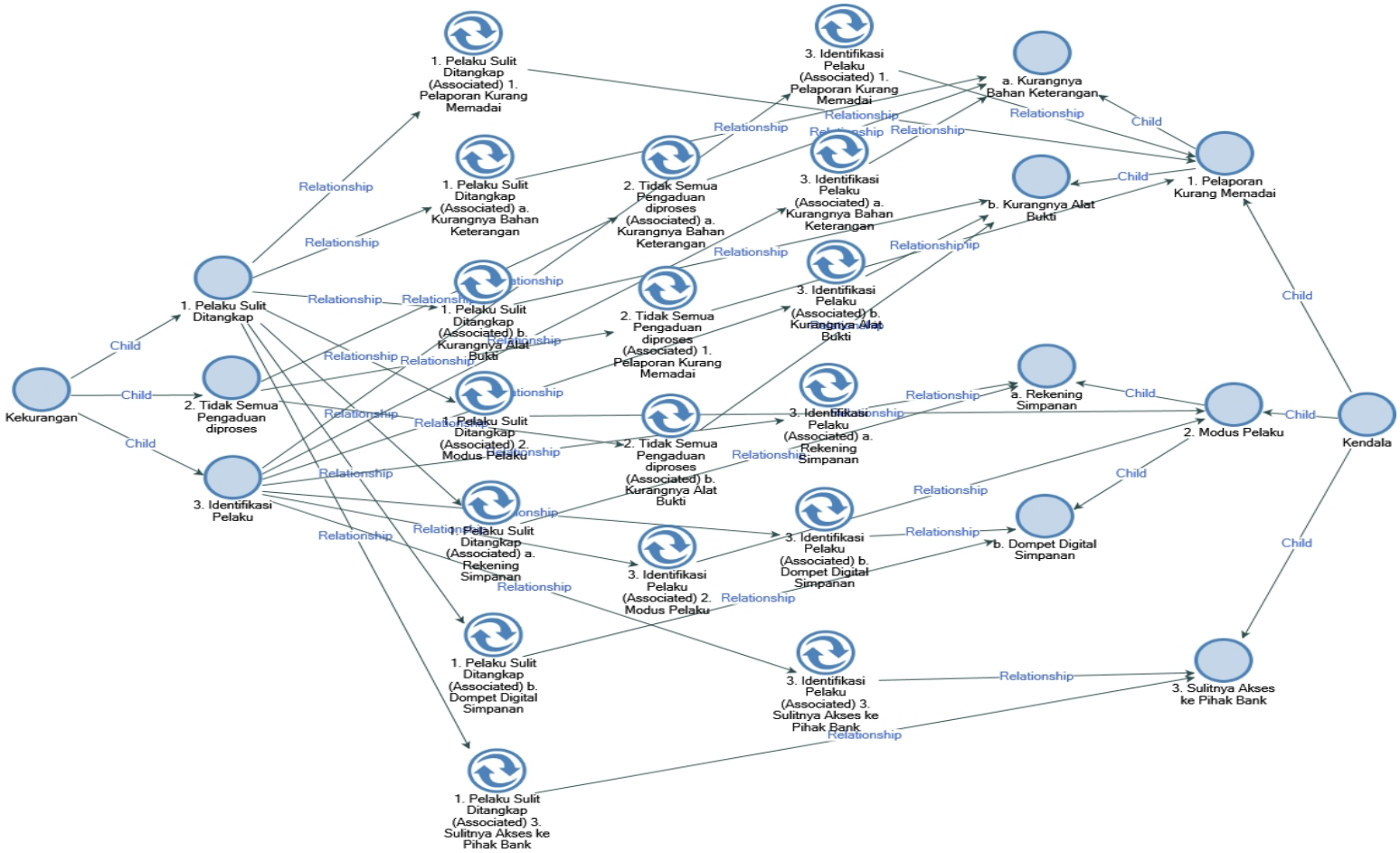
> "...Setelah kita melengkapinya kita kirimkan kembali lagi itu nanti kalau udah diterima kejaksaan akan muncul P21. nah setelah P21 itu muncul, itu bisa dilakukan Tahap 2. Tahap 2 yaitu tersangka, pelimpahan berkas perkara dan barang bukti."(Putra, 2023)

> "...Setelah selesai, hasil penyidikan bersama barang bukti atau tersangka diserahkan ke JPU (Jaksa Penuntut Umum). Peran jaksa adalah menuntut di persidangan. Dengan demikian, tugas polisi melibatkan menerima laporan, melakukan penyelidikan, dan selesai sampai pada tahap penyidikan, sedangkan tugas jaksa dimulai dari situ untuk menuntut di pengadilan."(Robani, 2023)

4. 5 Kekurangan dan Kendala yang Dihadapi Polda DIY dalam Pengungkapan Kasus *Phishing* di Daerah Istimewa Yogyakarta

Subdit V Siber Polda Daerah Istimewa Yogyakarta menghadapi kendala dalam proses pengungkapan kasus *Phishing*, terutama terkait penanganan pelapor dan keterbatasan penyidik. Peneliti selanjutnya akan memetakan hubungan antara kekurangan dan kendala yang dihadapi oleh Subdit V Siber Polda DIY dalam

pengungkapan kasus *Phishing*. Analisis yang digunakan peniliti yaitu dengan menggunakan aplikasi Nvivo 12.



Gambar 4.6 Peta Analisa Kekurangan dan Kendala yang Dihadapi oleh Polda DIY dalam Pengungkapan Kasus *Phishing*

Sumber:Diolah oleh Peneliti Menggunakan NVIVO 12

4. 5. 1 Kekurangan

Dalam mekanisme pengungkapan kasus *Phishing* oleh Subdit V Siber Polda DIY, terdapat kekurangan, yakni:

1. Pelaku Sulit Ditangkap

Pelaku *Phishing* sulit ditangkap oleh Subdit V Siber karena terkendala dengan mereka ahli dalam menyembunyikan identitas dan jejak digital. Mereka menggunakan alat penyamaran dan jalur *online* yang sulit dilacak oleh pihak penyidik. Sebagaimana yang dijelaskan oleh bapak Bripda Riski Praditya Putra

> "kurangnya bahan -bahan awal untuk melaporkan kasus itu juga kendala.pelaku sekarang juga pinter ya mba, seiring berjalannya dan berkembangnya teknologi, itu juga kendala bagi kami."(Putra, 2023)

2. Tidak Semua Pengaduan di proses

Berdasarkan Teori Agency antara korban/pelapor dan pihak Polda DIY (Agent) akan melibatkan kerjasama antara korban atau pelapor dengan Polda DIY dalam pengungkapan kasus *Phishing*, namun terdapat konflik selama prosesnya. Konflik ini muncul karena adanya kekurangan informasi dari pelapor dan kurangnya bukti yang disediakan oleh mereka dalam penanganan kasus *Phishing* oleh Subdit V Siber. Seperti yang dijelaskan oleh bapak Bripda Riski Praditya Putra

> "Tidak semua pengaduan di proses karena kita lihat apakah kasus ada unsur tindak pidananya. Kalau tidak bisa secara bukti nanti itu kita akan gelarkan seperti apa, mencari solusinya bagaimana, terus biasanya kita sampaikan ke pelapor kendalanya seperti apa kita sampaikan mba, karenakan mengungkap kasus tindak pidana penipun *online*, illegal Acces itu engga mudah juga."(Putra, 2023)

3. Identifikasi Pelaku Sulit

Identifikasi pelaku sulit bagi Subdit V karena adanya hambatan terkait kurangnya kemampuan personil, penggunaan identitas palsu oleh pelaku, serta penggunaan rekening dan dompet digital sebagai alat penyembunyian. Dalam ungkapan yang dijelaskan oleh bapak Bripda Riski Praditya Putra

> "pada saat kita mengidentifikasi pelaku juga makin sulit salah satunya dengan pelaku membuang nomernya itu, lalu kalau pakai *email*/media sosial itu pakai akun dari hasil beli, bukan akun yang asli. kita memproses kasus tersebut juga lumayan mba karena kita butuh informasi yang relevan."(Putra, 2023)

4. 5. 2 Kendala

Kendala yang dihadapi oleh Polda DIY dalam pengungkapan kasus *Phishing* di Wilayah Daerah Istimewa Yogyakarta sebagai berikut:

1. Pelaporan Kurang Memadai

a. Kurangnya Bahan Keterangan dari Korban

Peran pelapor atau saksi sangat penting dalam mendukung pengungkapan kasus, sebagai sumber informasi untuk mempercepat penanganan perkara. Namun, dalam praktiknya, bahan keterangan yang diberikan oleh pelapor seringkali kurang memadai. Tim penyidik Subdit V Siber Polda DIY menghadapi kesulitan saat meminta informasi sederhana seperti nomor *handphone*, yang tidak selalu dapat diperoleh dengan lancar dari pihak pelapor. Sebagaimana yang dijelaskan oleh bapak Bripda Riski Praditya Putra mengenai kurangnya bahan keterangan

> "...Biasanya kekurangan dari pelapor sih mba, yang komunikasinya ke kami itu kurang. kurangnya bahan -bahan awal untuk melaporkan kasus itu juga kendala."(Putra, 2023)

"...Jadi ketika buket awalnya itu lengkap dapat membantu, tapi ketika buketnya dari awal itu sudah gak bisa dibuktikan oleh korban itu kami kesulitan juga mba. "(Putra, 2023)

b. Kurangnya Alat Bukti dari Korban

Peran pelapor atau saksi sangat penting dalam mendukung pengungkapan kasus. Alat bukti yang kurang dapat menjadi kendala karena keberhasilan penyidikan sangat bergantung pada keberadaan bukti yang kuat dan relevan. Jika pelapor atau saksi tidak dapat menyediakan bukti yang memadai, penyidik dapat menghadapi kesulitan dalam membentuk kasus yang kokoh, sehingga menghambat proses pengungkapan dan penuntutan hukum. sebagaimana yang dijelaskan oleh bapak Bripda Riski Praditya Putra

"...Alat bukti juga diperlukan, karena dengan adanya barang bukti bisa mendapatkan keterangan saksi dan sebagai bahan pembuktian"(Putra, 2023)

2. Modus yang digunakan pelaku

a. Rekening tampungan

Tim penyidik Unit V Siber menghadapi kesulitan mengungkap kasus *Phishing* karena pelaku memanfaatkan banyak rekening. Rekening tampungan digunakan sebagai tempat sementara untuk menampung dana hasil penipuan. Dalam konteks kasus *Phishing*, pelaku cenderung menggunakan beberapa rekening bank untuk menyulitkan penyelidikan. Penggunaan lebih dari satu rekening membuat pelacakan transaksi dan identifikasi pelaku menjadi lebih sulit bagi tim penyidik. Sebagaimana yang dijelaskan oleh bapak Bripda Riski Praditya Putra

> “Jadi nomer rekening pelaku itu menggunakan rekening tampungan. Dan rekening tampungan itu di jual belikan dalam artian pelaku itu mencari rekening random namanya. Intinya pelaku ini beli ke orang, kebanyakan rekening ini dari Jawa Barat. Jadi pelaku ini beli dulu rekeningnya lalu rekening itu dibuat misalnya 5 rekening itu dibuat untuk uang tampungan dari modus *Phishing* tersebut.”(Putra, 2024)

b. Dompet digital tampungan

Dompet digital digunakan sebagai alat tampungan. Tim penyidik menghadapi kesulitan dalam mengungkap kasus *Phishing*, mirip dengan kendala yang terjadi pada rekening tampungan. Pelaku membeli banyak akun dompet digital untuk menyimpan uang hasil penipuan, dengan tujuan membuat penyidik sulit mengidentifikasinya. Seperti yang dijelaskan oleh bapak Bripda Riski Praditya Putra

> “...Kalau tidak rekening tampungan ya dompet digital tampungan. Setelah dari situ, ada pelaku yg transfer lagu ke ATM tampungan lagi habis itu ke nomor rekeningnya sendiri.”(Putra, 2024)

c. Tim Penyidik Subdit V Siber Polda DIY Mengalami Kesulitan Akses ke Pihak Bank

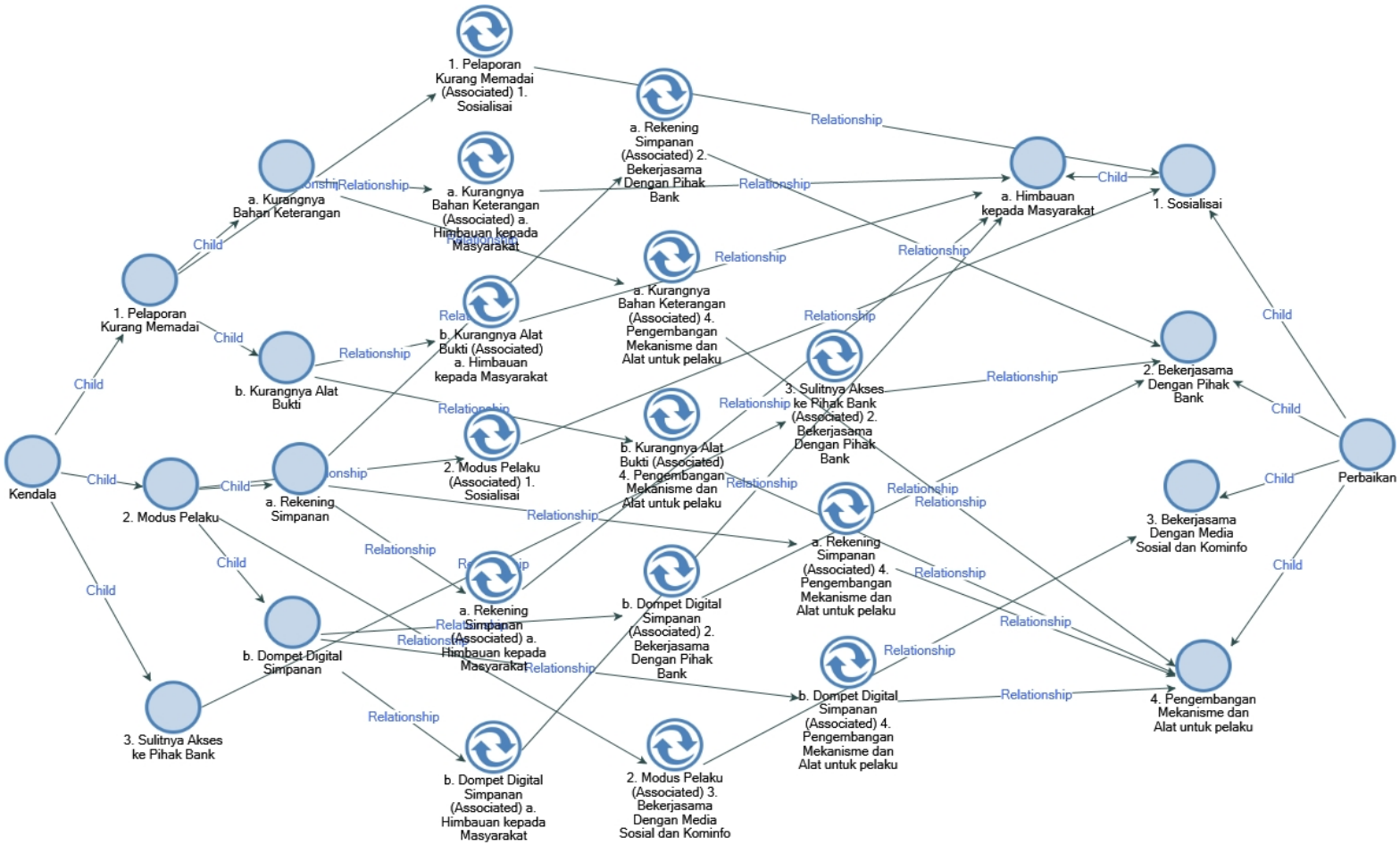
Data pada rekening dan dompet digital pelaku *Phishing* penting bagi tim penyidik Subdit V Siber Polda DIY karena seringkali pelaku menggunakan layanan perbankan. Namun, Bank tidak bisa memberikan informasi identitas pelaku berdasarkan "Peraturan Undang-Undang Republik Indonesia Nomor 10 Tahun 1998 Tentang Perbankan," yang menegaskan kerahasiaan informasi nasabah. Berdasarkan pengungkapan oleh bapak Bripka Cahyono Budi dan Bripda Riski Praditya Putra

> “Ya, karena gini mba di Undang-undang perbankan itukan ada untuk data pribadi ataupun nomer rekening apa itu semua ada peraturan peraturannya meskipun kita itu ada tindak pidana kita kan harus

> berkomunikasi, kita harus bersurat mba. Engga serta merta meskipun dia itu sudah diduga sebagai pelaku kita untuk membuka rekening dan sebagainya itu kita harus jelas dasarnya harus legal dulu, resmi."(Budi, 2023)
>
> "Kalau koordinasi itu pasti, soalnya kan memiliki ranah, Ranah itu juga di dunia perbankan juga, bank-bank itu juga punya ranah. Jadi kita gak asal langsung masuk ke lembaga gitu. Istilahnya kita permisilah. Koordinasi itu wajib."(Putra, 2023)
>
> Tim penyidik Subdit V Siber Polda DIY mengalami kesulitan mendapatkan izin dari Bank, yang memerlukan persetujuan dari Gubernur Bank Indonesia. Meskipun proses pembuatan izin cepat, respon dari Bank membutuhkan waktu yang lama. Walaupun tim penyidik mengetahui identitas pelaku, data seperti alamat pada rekening dan dompet digital mungkin bukan milik pelaku sejati karena banyak yang membeli atau memalsukan identitas, termasuk nama dan alamat orang lain, sehingga sulit diungkapkan.

4. 6 Perbaikan yang Dapat Dilakukan Polda DIY dalam Pengungkapan Kasus *Phishing* di Wilayah Daerah Istimewa Yogyakarta

Berdasarkan kendala dan kekurangan di atas, Polda Daerah Istimewa Yogyakarta perlu mengambil langkah-langkah perbaikan guna meningkatkan efektivitas pengungkapan kasus *Phishing*. Peneliti menyarankan perbaikan pada kemampuan, sarana, dan prasarana dalam menangani kasus penipuan *Phishing* di Daerah Istimewa Yogyakarta. Untuk menjelaskan usulan tersebut, peneliti akan menggunakan Peta Analisis dari aplikasi Nvivo 12.



Gambar 4.7 Peta Analisa Kendala dan Perbaikan yang dilakukan oleh Polda DIY dalam Pengungkapan Kasus *Phishing*

Sumber:Diolah oleh Peneliti menggunakan NVIVO 12

1. Sosialisasi Himbauan Kepada Masyarakat

Polda DIY aktif dalam melakukan sosialisasi kepada masyarakat melalui media sosial dengan memberikan penjelasan mengenai ciri-ciri dan modus kejahatan *Phishing* yang sering digunakan oleh para pelaku. Saat terjadi kasus yang serupa dengan apa yang dijelaskan dalam sosialisasi, pihak kepolisian juga akan mengadakan konferensi pers untuk memberitahu warga mengenai situasi tersebut. Contohnya, jika ada kasus *Phishing* tertentu yang sedang marak, masyarakat akan diingatkan melalui pesan-pesan hati-hati untuk menjaga keamanan informasi pribadi mereka.

Pendekatan ini bertujuan untuk memberikan pemahaman yang lebih baik kepada masyarakat mengenai ancaman *Phishing*, serta memberikan informasi langsung ketika ada kasus aktual yang perlu dicermati. Dengan cara ini, Polda DIY berupaya untuk meningkatkan kesadaran dan kewaspadaan masyarakat terhadap risiko kejahatan *cyber*, sehingga mereka dapat mengambil langkah-langkah pencegahan yang diperlukan.

2. Bekerjasama dengan Pihak Bank

Kerjasama antara Polda Daerah Istimewa Yogyakarta dan bank menjadi sangat krusial karena tim penyidik mengandalkan sinergi ini untuk melacak para pelaku kejahatan. Pelaku seringkali membeli nomor rekening dan dompet digital dari pihak ketiga, sehingga kerjasama dengan bank memungkinkan penanganan yang lebih efektif. Pentingnya memblokir nomor rekening tersebut bertujuan agar pelaku tidak dapat melakukan transaksi yang berpotensi untuk memindahkan hasil kejahatan mereka.

Polda DIY merasa perlu untuk mencari solusi dalam menanggulangi kejahatan ini, dan salah satu strategi yang diusulkan adalah kerjasama yang lebih erat dengan bank. Dalam upaya mengetahui identitas pelaku secara lebih detail, Polda DIY merencanakan untuk membuat *Memorandum of Understanding* (MoU) sebagai dokumen perjanjian resmi antara pihak kepolisian dan bank. MoU ini diharapkan dapat memudahkan proses penyidikan yang dilakukan oleh tim Subdit V Siber Polda DIY, termasuk dalam hal penangkapan pelaku kasus *Phishing*.

Langkah ini diambil untuk meningkatkan efektivitas dan efisiensi dalam penanganan kasus *Phishing*, sambil memastikan bahwa proses penyidikan tetap sesuai dengan hukum dan prosedur yang berlaku. Dengan demikian, kerjasama antara Polda DIY dan bank diharapkan dapat menjadi langkah positif dalam memerangi kejahatan siber yang semakin kompleks.

3. Bekerjasama dengan Media Sosial dan Kominfo

Dalam menghadapi meningkatnya kasus *Phishing*, khususnya yang terjadi di media sosial seperti *Instagram*, Polda DIY diharapkan dapat menjalin kerjasama dengan *platform* media tersebut dan Kementerian Komunikasi dan Informatika (Kominfo) untuk secara efektif memberantas pelaku kejahatan ini di wilayah Daerah Istimewa Yogyakarta.

Langkah minimal yang dapat diambil oleh media sosial adalah memblokir akun pelaku, tetapi disadari bahwa pelaku seringkali mengganti akun dengan cepat, sehingga tindakan ini masih belum optimal. Oleh karena itu, disarankan agar Kominfo dapat merancang regulasi khusus bagi *platform Instagram* dan

Facebook. Regulasi tersebut dapat mengamanahkan penggunaan Nomor Induk Kependudukan (NIK), foto wajah, dan Kartu Tanda Penduduk (KTP) sebagai syarat untuk membuka toko di media sosial, mirip dengan ketentuan yang umumnya diterapkan oleh *platform e-commerce* atau perbankan.

Dengan menerapkan regulasi ini, diharapkan identitas pemilik akun lebih terjamin dan pelaku tidak dapat dengan mudah membuat identitas palsu. Upaya ini bertujuan untuk meningkatkan keamanan dan meminimalisir peluang pelaku *Phishing* untuk terus beroperasi tanpa terdeteksi. Seiring dengan itu, kerjasama lintas sektor antara Polda DIY, media sosial, dan Kominfo diharapkan dapat memberikan solusi dalam menangani ancaman *Phishing*.

4. Pengembangan Mekanisme dan Alat Untuk Pelaku

Perbaikan yang dilakukan oleh Polda DIY adalah dengan mengembangkan mekanisme dan alat yang dapat membantu para pelaku. mencakup penyediaan pelatihan tambahan, perbaikan atau pengembangan peraturan, atau pengadaan peralatan yang lebih baik untuk mendukung tugas-tugas mereka. Tujuannya adalah untuk meningkatkan efektivitas dan efisiensi dalam menjalankan tugas kepolisian serta memastikan pelayanan yang lebih baik kepada masyarakat.

4. 7 Kesimpulan Bab

Berdasarkan rumusan yang telah dianalisis oleh peneliti melalui hasil wawancara dan pembahasan, terkait Peran Polda Daerah Istimewa Yogyakarta dalam Pengungkapan Kasus *Phishing*, dapat disimpulkan bahwa tren permasalahan kasus *Phishing* di Daerah Istimewa Yogyakarta disebabkan karena

korban (*target*) terlalu mempercayai pelaku (*offender*), kurang pemahaman korban (*target*) terhadap yang digunakan, dan kurangnya kepatuhan korban (*target*) terhadap peraturan.

Sedangkan untuk modus pelaku (*offender*), mereka mengatasnamakan Merchant Terpercaya untuk mengelabui korban (*target*). Korban (*target*) diminta untuk mengisi *link* atau formulir digital, dan mengirim *email* agar pelaku (*offender*) dapat mengambil data korban (*target*). Pelaku (*offender*) bergerak baik secara individu maupun kelompok, dan korban (*target*) yang terkena penipuan bisa berasal dari kalangan muda maupun tua.

Peran Polda Daerah Istimewa Yogyakarta dalam pengungkapan kasus *Phishing* melibatkan tahapan pengaduan, penyelidikan, dan penyidikan hingga pelaku akhirnya ditangkap dan diserahkan kepada Jaksa Penuntut Umum. Namun, penelitian ini mengidentifikasi beberapa kendala, termasuk kurangnya sumber daya manusia seperti sulit mengakses pihak bank, pelaporan yang kurang memadai karena kurangnya bahan keterangan, serta kendala dalam menghadapi modus yang digunakan oleh pelaku (*offender*) sehingga sulit menemukan identitas pelaku.

BAB V

KESIMPULAN DAN SARAN

5. 1 Pengenalan Bab

Bagian ini memuat penjelasan akhir dari hasil penelitian yang telah dilakukan peneliti terkait setiap rumusan masalah yang telah diajukan pada awal penelitian. Kesimpulan yang dibuat didasarkan pada analisis yang teliti terhadap data yang telah dikumpulkan peneliti. Selanjutnya, peneliti akan memberikan rekomendasi yang ditujukan kepada peneliti berikutnya.

5. 2 Kesimpulan

Berdasarkan hasil temuan dan analisis pada bab IV mengenai penelitian berjudul "Analisis Peran Polda Daerah Istimewa Yogyakarta dalam Pengungkapan Kasus *Phishing*", peneliti dapat mengambil kesimpulan dari seluruh proses penelitian yang telah dilakukan sebagai berikut:

1. Tren kasus *Phishing* di Daerah Istimewa Yogyakarta menunjukkan peningkatan yang signifikan dalam beberapa tahun terakhir, khususnya terkait dengan UU ITE. Para pelaku *Phishing* menggunakan cara yang semakin canggih dengan menyamar sebagai pihak yang dapat dipercaya, seperti perusahaan atau lembaga resmi, untuk mengelabui orang dan mencuri informasi pribadi mereka. Mereka sering melakukan hal ini melalui *email* palsu, situs web palsu, atau pesan teks yang mengandung tautan berbahaya. Karena banyak korban tidak memahami tanda-tanda *Phishing*, risiko pencurian data semakin meningkat. Mayoritas kasus *Phishing* terjadi secara

online, terutama melalui media sosial seperti *email*, *Facebook*, dan *Instagram*, di mana informasi pribadi korban mudah tersedia. Untuk mengatasi masalah ini, diperlukan tindakan yang lebih aktif dari pihak berwenang dan peningkatan kesadaran masyarakat tentang bahaya *Phishing*.

2. Mekanisme pengungkapan kasus *Phishing* oleh Polda Daerah Istimewa Yogyakarta melalui 3 tahapan:
    a. Pengaduan dilakukan pada saat Korban melapor ke Sentra Pelayanan Kepolisian Terpadu (SPKT) Polda DIY dengan membawa identitas dan bukti terkait kasus *Phishing*. Mereka 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.
    b. 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.
    c. 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 untuk penuntutan di

pengadilan. Polisi 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.

3. Kekurangan dan kendala yang dihadapi oleh Polda Daerah Istimewa Yogyakarta dalam mengungkap kasus *Phishing* adalah bahwa meskipun telah melakukan upaya dalam mengungkap kasus *Phishing*, Polda DIY menghadapi beberapa kendala yang signifikan. Kekurangan dalam penangkapan pelaku, kurangnya pengolahan pengaduan, serta kesulitan identifikasi pelaku menjadi hambatan utama dalam proses penyidikan. Selain itu, kendala akses terhadap informasi perbankan juga menjadi tantangan serius bagi tim penyidik. Oleh karena itu, diperlukan koordinasi yang lebih baik antara pihak kepolisian, pihak perbankan, dan pihak terkait lainnya guna meningkatkan efektivitas dan efisiensi dalam pengungkapan kasus *Phishing*.
4. Perbaikan yang dilakukan oleh Polda Daerah Istimewa Yogyakarta dalam mengatasi kasus *Phishing* adalah dengan melakukan langkah-langkah strategis seperti sosialisasi kepada masyarakat, kerjasama erat dengan pihak bank, serta kolaborasi dengan media sosial dan Kementerian Komunikasi dan Informatika (Kominfo). Melalui upaya ini, Polda DIY bertujuan untuk meningkatkan kesadaran masyarakat, memperkuat penindakan terhadap pelaku kejahatan siber, dan menciptakan lingkungan yang lebih aman di ranah digital

5. 3 Implikasi Penelitian

Dari temuan penelitian ini, terdapat beberapa implikasi yang dapat disimpulkan:

1. Kepolisian Negara Republik Indonesia memiliki peran yang sangat vital dalam menjaga keamanan dan ketertiban masyarakat, menegakkan hukum, serta memberikan perlindungan dan pelayanan kepada masyarakat. Peran Polda Daerah Istimewa Yogyakarta, terutama Ditreskrimsus, menjadi kunci dalam mengungkap kasus *Phishing* yang terjadi di wilayah tersebut. Melalui upaya pengungkapan kasus *Phishing*, Polda DIY berperan aktif dalam memastikan keamanan siber masyarakat di Jogja.
2. Penelitian ini memberikan landasan bagi peningkatan kualitas Sumber Daya Manusia (SDM) di Polda DIY dengan meningkatkan jumlah personil dan meningkatkan kompetensi penyidik. Hal ini bertujuan untuk memperkuat kemampuan penyidik dalam menghadapi tantangan kejahatan siber seperti *Phishing*, sehingga dapat memberikan respons yang cepat dan efektif dalam menangani kasus tersebut.

5. 4 Keterbatasan Penelitian

Dalam penelitian ini, peneliti menyadari bahwa meskipun telah berusaha secara optimal, namun masih jauh dari kesempurnaan. Terdapat beberapa keterbatasan yang dialami selama proses penelitian. Pertama, proses wawancara memakan waktu yang cukup lama karena sulitnya menentukan jadwal yang sesuai dengan ketersediaan narasumber. Selain itu, peneliti juga tidak dapat mengakses data kasus *Phishing* karena sebagian besar data tersebut masih dalam proses penyelidikan atau penyidikan oleh pihak berwenang. Selanjutnya, 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. Sebagai contoh, penelitian tidak dapat memberikan contoh surat tahapan proses mekanisme pengungkapan kasus *Phishing* karena informasi tersebut dianggap rahasia. 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.

5. 5 Saran

5. 5. 1 Polda Daerah Istimewa Yogyakarta

Saran untuk meningkatkan kemampuan dalam pengungkapan kasus *Phishing* di wilayah Daerah Istimewa Yogyakarta adalah dengan melaksanakan pelatihan bagi penyidik di lingkup Polda Daerah Istimewa Yogyakarta. Pelatihan ini dapat dilakukan bekerja sama dengan institusi pendidikan atau lembaga pelatihan lainnya dengan tujuan untuk meningkatkan kualitas kemampuan penyidik Polda DIY. Selain itu, penting juga untuk menjalin kerjasama dengan Bidang Humas terkait untuk melakukan sosialisasi kepada masyarakat melalui konferensi pers dan himbauan langsung kepada masyarakat tentang bahaya *Phishing*.

5. 5. 2 Masyarakat

Saran Untuk menghindari ancaman *Phishing*, masyarakat dapat meningkatkan pemahaman mereka tentang metode serangan tersebut dan selalu waspada terhadap pesan yang mencurigakan. Selain itu, periksa selalu keaslian permintaan informasi sensitif sebelum memberikannya, dan pastikan untuk secara teratur memperbarui perangkat lunak keamanan. Penting juga menggunakan kata sandi yang kuat dan unik serta menjaga kewaspadaan saat berinteraksi di media sosial. Jika mencurigai adanya aktivitas *Phishing*, segera laporkan kepada pihak berwenang untuk langkah-langkah penanganan lebih lanjut. Dengan cara ini, masyarakat dapat melindungi informasi pribadi mereka dari serangan *Phishing*.

5. 5. 3 Penelitian Selanjutnya

Untuk penelitian selanjutnya, disarankan agar peneliti memperluas cakupan dengan membandingkan bagaimana kasus *Phishing* diungkapkan antara Polda Daerah Istimewa Yogyakarta dengan daerah lain. Penelitian ini dapat melibatkan lebih banyak narasumber yang berpengalaman dalam penanganan kasus *Phishing*, seperti penyidik, ahli keamanan *cyber*, dan perwakilan lembaga terkait. Dengan demikian, peneliti dapat memperoleh pemahaman yang lebih luas tentang pendekatan dan praktik terbaik dalam mengatasi kasus *Phishing* di berbagai wilayah. Selain itu, penelitian dapat fokus pada analisis faktor-faktor yang memengaruhi efektivitas pengungkapan kasus *Phishing* dan mencari solusi inovatif untuk memperkuat upaya pencegahan dan penindakan terhadap kejahatan *cyber* se*Mac*am itu.

DAFTAR PUSTAKA

Abdul Fattah Nasution. (2023a). *Metode Penelitian Kualitatif*. Harfa Creative.

Abdul Fattah Nasution. (2023b). *Metode Penelitian Kualitatif*. Harfa Creative.

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

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

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

Arianto, B. (2021). Media Sosial dan Whistleblowing. *Berkala Akuntansi Dan Keuangan Indonesia*, *6*(1), 61–80. https://doi.org/10.20473/baki.v6i1.25672

Asosiasi Penyelenggara Jasa Internet Indonesia. (2018). *Penetrasi dan Profil Perilaku Pengguna Internet Indonsia*.

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.

Creswell, J. W., & John W Creswell. (2012). Penelitian Kualitatif dan Desain Riset Memilih diantara lima pendekatan. In *Yogyakarta: Pustaka Pelajar*. Pustaka Pelajar.

Denzi, N. K. (2012). Triangulation 2.0. *Journal of MMxed Methods Research*, *6*(2), 80–88. https://doi.org/https://doi.org/10.1177/1558689812437186

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.

Ginanjar, A., Widiyasono, N., & Gunawan, R. (2019). Web Phising Attack Analysis on E-Commerce Service Using Network Forensic Process Method. *Jurnal Terapan Teknologi Informasi*, *2*(2), 147–157. https://doi.org/10.21460/jutei.2018.22.111

Handoyo, S. (2016). *Pengantar Akuntansi Forensik dan Investigasi*. Ekonisia.

Latifahi, F. N., Mawardi, I., & Wardhana, B. (2022). Ancaman Pencurian Data (Phishing) Di Tengah Trend Pengguna Fintech Pada Pandemic Covid – 19 (Study Phishing Di Indonesia). *Perisai : Islamic Banking and Finance Journal*, *6*(1), 74–86. https://doi.org/10.21070/perisai.v6i1.1598

Light, D., Keller, S., & Calhoun, C. (1989). *Sociology*. Random House.

McLay, W. D. S. (2009). *Clinical Forensic Medicine*. Cambridge University Press.

Moleong, L. J. (2009). *Metodologi Penelitian Kualitatif*. PT. Remadja Rosdakarya.

Muhammad, F. E., & Harefa, B. (2023). Pengaturan Tindak Pidana Bagi Pelaku Penipuan Phisning Berbasis Web. *Jurnal USM Law Review*, *6*(1), 226. https://doi.org/10.26623/julr.v6i1.6649

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

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

Na, D. E. C., & Hipertensiva, C. (n.d.). *Framework Matrices*.

Olsen, W. K. (2004). *Triangulation in Social Research: : Qualitative and Quantitative Methods Can Really Be Mixed* (M. H. Michael Haralambos, Ed.). Causeway Press Ltd.

Pratama, B. A., & Sari, D. S. (2020). Dampak Sosial Intensitas Penggunaan Media Sosial terhadap Kesehatan Mental berupa Sikap Apatis di SMP Kabupaten Sukohajo. *GASTER*, *18*(65–75). https://doi.org/https://doi.org/10.30787/gaster.v18i1.487

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

Ramadani, R. F., Setiawati, & Natsir, M. (2020). Cerdas dan Bijak Memanfaatkan Internet melalui Komunitas Belajar. *Indonesian Journal of Adult and Community Education*, *2*(1).

Riyanto, A. D. (2019). *Indonesian Digital Report 2019*. Hootsuite. https://andi.link/hootsuite-we-are-social-indonesian-digital-report-2019/

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 Phising Baca artikel detiknews, "Gadaikan SK Ratusan Juta, PNS Ini Malah Jadi Korban Phising" selengkapnya https://news.detik.com/berita/d-6696948/gadaikan-sk-ratusan-juta-pns-ini-malah-jadi-korban-phisi*. Detik.Com. https://news.detik.com/berita/d-6696948/gadaikan-sk-ratusan-juta-pns-ini-malah-jadi-korban-phising

Saryono, A. S. (2010). *Metodologi Penelitian Kebidanan*. Nuha Medika.

Septiano, A. K., & Najicha, F. U. (2022). *Upaya Peningkatan Rasa Nasionalisme dengan Pendidikan Kewarganegaraan Kepada Generasi Muda di Era Perkembangan Teknologi*. 3.

Sugiyono. (2018). *Metode Penelitian Pendidikan Pendeketan Kuantitatif, Kualitatif, dan R&D*. Alfabeta.

Vadila, N., & Pratama, A. R. (2021). Analisis Kesadaran Keamanan Terhadap Ancaman Phishing. *Automata*, *2*(2).

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

Widodo. (2013b). *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., Puri, F. M., & Setiawan, A. (2023a). Deteksi Website Phishing Menggunakan Teknik Filter Pada Model Machine Learning. *Information System Journal*, *6*(1), 39–43. https://doi.org/10.24076/infosjournal.2023v6i01.1268

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

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

LAMPIRAN

DAFTAR LAMPIRAN

Lampiran 1 Surat Izin Penelitian

KEPOLISIAN NEGARA REPUBLIK INDONESIA
DAERAH ISTIMEWA YOGYAKARTA
BIRO SUMBER DAYA MANUSIA

NOTA DINAS
Nomor: B/ND- 1655 /X/DIK.2.6./2023/Ro SDM

Kepada : Yth. Dirreskrimsus Polda DIY

Dari : Karo SDM Polda DIY

Hal : permohonan izin penelitian mahasiswa Fakultas Bisnis dan Ekonomika Universitas Islam Indonesia.

1. Rujukan Surat Dekan Fakultas Bisnis dan Ekonomi Universitas Islam Indonesia Nomor: 1967/DEK/10/Div.URT/X/2023 tanggal 16 Oktober 2023 perihal permohonan izin penelitian.

2. Sehubungan dengan rujukan di atas, bersama ini disampaikan kepada Dir bahwa terdapat mahasiswa Fakultas Bisnis dan Ekonomi Universitas Islam Indonesia yang mengajukan izin penelitian di Polda DIY dalam rangka penyusunan karya tulis ilmiah (skripsi), adapun identitas mahasiswa sebagai berikut:
   a. nama : Maharlina Darni Purwandari;
   b. NIM : 20312410;
   c. program studi: Akuntansi;
   d. judul : "Analisis Peran Polda Daerah Istimewa Yogyakarta Dalam Pengungkapan Kasus *Phishing*";
   e. No. Telp : 087861541404.

3. Berkaitan dengan hal tersebut, dengan ini dimohon kepada Dir untuk membantu memfasilitasi permohonan penelitian mahasiswa dimaksud dengan tetap memperhatikan keamanan data informasi yang dikecualikan.

4. Demikian untuk menjadi maklum.

Yogyakarta, 20 Oktober 2023
KEPALA BIRO SUMBER DAYA MANUSIA POLDA DIY

NANANG DJUNAEDI, S.I.K., M.M.
KOMISARIS BESAR POLISI NRP 75110782

Tembusan:
1. Kapolda DIY.
2. Wakapolda DIY.
3. Dirintelkam Polda DIY.
4. Kabidpropam Polda DIY.

Lampiran 2 Transkip Wawancara : Bapak Budi Cahyono Desember

NARASUMBER 1

Nama : Bripka Cahyono Budi

Jabatan: Banit Subdit V/Siber Ditreskrimsus

Waktu : Senin, 4 Desember 2023 (09.00)

P : Pewawancara

N : Narasumber

P : kasus *Phishing* di Yogyakarta apakah ada peningkatan?

N : kalau untuk tahun 2023 ini mungkin kalau kasus *Phishing* itu mungkin kalau dibilang ada peningkatan engga, cuman masih cukup banyak juga dibandingkan tahun lalu. Kalau untuk akhir-akhir ini kasus *Phishing* lumayan. Cuman kalau dibilang meningkat itu kita harus berhubungan dengan data-data yang valid, cuman kita ya istilahnya cukup banyak dan masuk di semua kalangan. Kalangan dalam artian misalnya tingkat pendidikannya itu sudah kita kategorikan ya lumayan. ada yang SMA, sarjana, S2 dan S3.

P : kebanyakan kalau kasus *Phishing* itu rata-rata mengatasnamakan pribadi atau komplotan?

N : selama ini *case* yang pernah ditangani Polda DIY itu didalamnya ada grub, cuman kadang dia juga perannya berbeda-beda dan ada indikasi juga mereka mungkin ya melakukan kegiatan *Phishing* diluar grub atau melakukan kegiatannya sendiri.

P : di luar grub itu sendiri?

N : iya

P : bagaimana rata-rata pelaku *Phishing* itu memanfaatkan untuk mengelabui korban?

N : kalau mengelabui korbannya yang pertama itu mungkin dengan bahasa *Phishing* itu kayak bujuk rayu, jadi mereka itu menawarkan kemudahan.

Misal kita mempunyai tabungan rekening di bank tertentu. Misal bank A, bank B dan bank C nanti kalau mengeluarkan produk itu ada keringanan untuk biaya transaksinya. Yang biasanya Rp 6.000 atau Rp 10.000 mungkin jadi Rp 2.500 atau Rp 3.000 atau sebaliknya kita tetap menggunakan beban transaksi yang lama dari situlah mungkin awal mulanya. Dari awal mulainya seperti itu nanti kadang mereka mengirimkan *link* untuk mengisi biodata atau semua identitas data-data pribadi korbannya. Jadi begitu data identitas pribadi seperti nomer ATM, atau sampai kita memberikan nomor pin kita dan sebagainya. Otomatis data-data kita diketahui oleh orang lain yang tidak berkepentingan. Makanya dari situ mungkin muncul balasan kayak password OTP, begitu ada *password* OTP nanti dikirimkan balik kepada yang diduga pelaku itu tadi.

P : untuk *Phishing* tersebut apakah ada pola tersendiri yang digunakan oleh pelaku dalam menjalankan kegiatannya?

N : kalau pola itu istilahnya kayak mungkin sugesti kan mba. Jadi kayak bahasa di kita itu social engineering, jadi orang itu menganggap seperti oh saya kena mistik atau saya kena *gendam*, padahal tidak. Mungkin dari pelaku ini kan memanfaatkan hal tersebut kepada korban. Karena korban mungkin sedang tidak konsentrasi atau mungkin korban itu mendapatkan informasi tidak di klarifikasi dulu, jadi langsung percaya. Dari situlah itu masuk bujuk rayu yang mengirimkan *link* yang dia itu menjanjikan katanya bisa mendapatkan uang atau hadiah. Padahal seharusnya itu dilakukan oleh pihak bank secara resmi. Ada juga yang istilahnya dia itu permasalahan, seperti misal mba nya mau melakukan transaksi di ATM, mungkin transaksi itu ada *trouble* atau gangguan yang mungkin mba sudah transfer tapi tidak sampai ke rekening yang dituju. Mungkin karena *error*. Biasanya kan orang itu mencari *call center*. Jadi kalau *call center* di Bank-bank yang resmi itu jelas informasinya misal *call center* Bank A itu berapa. disitu kita harus jeli, mungkin ada titiknya, huruf besar, huruf kecil atau mungkin ada tambahan huruf lainnya. Kadang korban yang mencari informasi *call center* di internet itu ngga valid, itu bukan *call center* dari

bank tersebut. Nah dari situ kan korban dipandu, kalau misal menelfon nomer tersebut. Mba ada keluhan apa? ada yang dibantu? gini mba saya tadi transfer udah kepotong tapi belum masuk ke rekening tujuan. Saya bantu mba coba nanti mengirim nomer ATM nya, rekening atau PINnya berapa atau bahkan data-data lain yang pelaku butuhkan. Nanti otomatis kan korban panik, itu pasti dikasihkan tanpa berpikir panjang. Padahal kalau kode rahasia itu bersifat privasi dan tidak boleh dikasih tahu siapapun. Yang tahukan hanya bersangkutan saja. Begitupun sebaliknya kayak kode OTP/*PASSWORD* itu verifikasi hanya untuk pemegang itu sendiri. Kalau sudah beralih ke orang lain pasti sudah otomatis akun kita dipegang orang lain. Kadang orang itu kurang pemahamannya disitu. Makanya kita yang agak-agak jadi tanda tanya kita, dengan tingkat pendidikannya yang sudah cukup, rata-rata standar kita sarjana, kenapa sih orang masih kurang berpikiran yang luas. Kenapa kita gak *crosschek* dulu atau membandingkan, jadi begitu kita sudah seperti itu melakukan keputusan yang dianggap salah dan fatal

N : Jadi tanda tanya kita dengan tingkat pendidikan yang sudah cukup misal kita standar nya mungkin sarjana kenapa sih mungkin masih kurang berfikiran yang luas kok kita ngga *crosschek* dlu kok kita ngga mungkin membandingkan atau mungkin tanya yang lain jadi begitu kita apa langsung tuh kita melakukan keputusan yang itu dianggap sama

P : Kalau misal pak pihak bank di *hack* dan pelanggan itu masih belom tau pak kalau itu dihack itu bagaimana pak kan sudah ada situs resminya tapi belom tau kalau itu sedang di *hack* gimana pak

N : ngga maksudnya dari pihak bankkan nya situs bank A atau bank B atau mungkin dari pribadi nya

P : Dari pihak banknya

N : Kalo bank itu ngga maksudnya bank A bank C dia punya tim *security* sendiri

P : Iya

N : Nah tim *security* itulah yang bertanggung jawab tentang perbankan itu jadi perbedaan kalo misalnya yang diancam atau mungkin yang diganggu mungkin dari sistem *securitynya* dari pihak bank itu akan berbeda sama yang ke pribadi misalnya kaya korban nah kalo korban itukan ada kesalahan dari pribadinya

P : Iya

N : *human error* ya to, kalo misalnya dari sistem perbankannya sendiri itu kan jadi tanggung jawab penuh tuh berada di pihak bankan jadi begitu ada kerugian atau apa itu *case*nya itu akan berbeda kalau njenengan itu ngga pernah melakukan transaksi ngga apa ngga mengasih OTP ngga memberi PIN dan sebagainya itu umpama duit anda direkening bank A bank B bank C ada tabungannya misalnya ada yang hilang itu mungkin masih kita pastikan itu tanggung jawab penuh dari perbankan cuman dengan catatan orang itu harus ada investigasi dulu ini betul ngga sih duitnya mba ini dia betul betul hilang karna sistem banknya itu bermasalah atau mungkin njenengan sendiri yang melakukan human error nah nanti dari pihak *security* perbankkan itu akan bisa membuktikan nah begitu itu kesalahan dari pihak perbankkan atau mungkin kerugian mungkin istilahnya anda alami itu mungkin akan diganti cuma kalo misalnya njenengan sendiri yang melakukan human *error* atau kesalahan memberikan PIN atau OTP dan sebagainya itu pihak bank ngga mau ganti meskipun itu itungannya itu dari berapa rupiah sampek maupun belasan juta rupiah bahkan mungkin lebih itu perbedaannya

P : Soalnya pak rata rata kasus karna kesalahan beliau sendiri pak terus kaya mungkin menuntut keadilan buat tersangkanya harus gimana di amankan nya itu pak

N : Yang maksudnya gini mbak yang istilahnya setiap perbuatan ada konsekuensinya cuman kitakan serta merta mungkin bedanya menyalahkan dari korban cuman dari pihak perbankkan sendirikan ada aturannya ada SOP nya yang meningkat disitu, mangkanya ya itu tadi tingkat pendidikan dan wawasan kita pengetahuan, jangan mungkin

menggunakan mobil bagus umpama hp bagus tapi kita tidak bisa menggunakan itu malah menjadikan bencana bagi kita nah itukan harus kita hindari mangkanya dengan peradapan baru kita menyiapkan juga Itu yang berhubungan dengan teknologi, teknologi kan mau gamau begitu ini sudah era digital mau gamau kita harus belajar kalau mungkin ga bisa mungkin tanya atau *searching* ya kita pastikan *searching* itu juga harus dipastikan dulu informasinya di internetya ya kita harus memastikan bahwa itu benar,teknologi bagus tapi manusianya itu ga bisa ya itukan bermasalah nah di sisi lain kan ada yang harus tanggung jawab, tanggung jawab dari pihak perbankkan mungkin bisa mengadakan sosialisasi atau mungkin dia ada informasi yang lebih detail dan lebih jelas nah itukan biasanya perbankkan kalo dari pihak polisi kan mungkin ada tindak pidana atau mungkin di duga tindak pidana nah disitulah tanggung jawab kita nah kita mungkin juga ada himbauan atau mungkin ada laporan dari masyarakat cuman kalo misalnya njenengan mungkin ada tidak ada laporan seperti itu kitakan juga ngga tau nah kalau dari laporan masyarakat kita bisa langsung analisa dan kita *profile*. nah solusinya nanti kita bisa penegakkan hukum terus nanti kita himbauan kan himbauan kan untuk pencegahan karna rata rata pelaku yang mungkin kita amankan itu ya mungkin uang ngga ada padahal mungkin kita jejerkan dari UU ya mungkin misalkan dari UUD ITE nah kita mungkin belajar UU perbankkannya atau mungkin pencuci uangnya *case* nya dari permasalahan tersebut jadi dari pihak bank mungkin dia itu harus setidaknya ya mungkin informasi lebih jelas karna kenapa teknologi barnu upgrade nah dulu mungkin belom ada M-bangking tapi sekarang ada dulu belom ada baru mungkin sekarang ada banyak terus serinya teruskan antriannya juga mancet mancet teknologi nya yang harusnya antriannya yang model lama mungkin ngga digunakan lagi di upgrade lagi harus lebih baru atau mungkin ada *trouble* yang langsung *connect* dan ada tim *security* yang bersangkutan mungkin dari pihak pemakainya atau penggunaannya teknologi mungkin bagus istilahnya mbanya punya mobil rubicon cuman

njenengan itu ngga bisa mengemudikan padahal itu bagus cantik enak cuman kita ngga bisa ngga siap untuk memakainya itu kan malah jadi malapetaka padahal kalo kita bisa menggunakan mobil itu bisa menjadi kenyamanan untuk kita kalau saya mungkin pakainya mobil yang manual yang nyaman ya mau ngga mau kan teknologi kan harus berkembang begitu kita istilahnya ngga mengimbangngi ya mungkin siap siap kita yang jadi korban nah harus dari pihak kepolisian nah kepolisian kan penegak hukum nya atau mungkin istilahnya mencari atau menemukan pelaku cuman kan polisi bukan Superman mungkin ada keterbatasannya atau mungkin ada kendalanya kan lihat lihat dari *case* nya masing masing kan jadi seperti itu ya kalau lebih bagus itu ada pencegahan.

P : kalau kendala sendiri dari bank itu ada SOPnya, untuk lain kendala buat menangani kasus selain dari pihak yang bersangkutan kayak SOPnya mungkin kan ada yang kita perlu mengikuti aturan bank kan pak, misal datanya butuh cepat dan buru-buru terus misal kalau kita tidak mengikuti SOP dari bank sendiri gimana pak kerjasamanya kendala yang lain?

N : ya, karena gini mba di Undang-undang perbankan itukan ada untuk data pribadi ataupun nomer rekening apa itu semua ada peraturan peraturannya meskipun kita itu ada tindak pidana kita kan harus berkomunikasi, kita harus bersurat mba. Engga serta merta meskipun dia itu sudah diduga sebagai pelaku kita untuk membuka rekening dan sebagainya itu kita harus jelas dasarnya harus legal dulu, resmi. Kalau Misalkan kita ngga resmi kita juga bisa di pra peradilkan sebagai polisi jadi ya permasalahannya atau mungkin terbuka dibilang kendala, mungkin yang perlu kita tingkatkan yaitu komunikasi. Mungkin dari pihak perbankan sendiri harus mungkin berbenah. Oh mungkin untuk pembukaan rekening apa semuanya harus lebih selektif, lebih hati-hati. Dan karena ngejar profit melupakan keamanan, nah makannya sebenarnya wawancara seperti ini harusnya dari dua sisi, bisa kepolisian, bisa perbankan. Jadi informasi yang didapat mba bisa kuat. Kalau misalkan kita mungkin istilahnya mengkomentari pihak perbankan orang itu mungkin ada yang *capable*

dibidangnya. Nah begitu nanti mba crosscheck kesana nanti informasinya lebih valid.

P : mungkin kalau korbannya mau lapor ke kepolisian gimana pak tahapannya?

N : kalau lapor, mungkin kayak tadi di kriminal khusus kita ada 24 jam, maksudnya kapan mungkin disitu ada kendala yang perlu ditanyakan apa atau semua yaudah minimal korban harus membawa bukti-bukti, oh saya ada kejadian seperti ini pak karena kenapa kan tidak menuntut kemungkinan ada orang yang jujur dan gak jujur. Begitu laporan di sertai dengan dokumen yang lengkap itukan mendukung kevalidan laporan tersebut, nah cuman datanya bisa disusulkan kelengkapannya yang penting itukan langkah pertamanya yaudah dateng ke kantor untuk konsultasi ada kejadian seperti ini nanti kalau misalnya data itu kan bisa menyusul atau mungkin data itu ada di HP mau kita bantu printkan dan sebagainya, kan cepat. Jadi begitu mungkin kecepatan untuk memperoleh informasi itu mungkin ya ada kemungkinan ya untuk kita itu mengungkapkan kasus jadi lebih besar. Cuman kendalanya bukan istilahnya apa kan ini ada pihak perbankan Istilahnya pemegang data dan kepolisian kan harusnya harus sinkron. Dalam arti sinkron itu pihak bank mungkin ya harus ada upaya kalau misal ada kejadian seperti ini, upaya yang dilakukan bank bagaimana. Jadi selain mengejar profit ya harus melindungi nasabahnya karena nabung disitu kan biar dapat keuntungankan bank karena menyediakan jasa layanan. Cuman kita di tugasi oleh negara untuk menjaga ketertiban keamanan masyarakat dan penegakkan hukum.

P : dari beberapa kasus mungkin ada engga pak yang sudah selesai itu kasusnya?

N : ada, kemarin juga dari bak tertentu engga perlu saya sebutkan nama banknya, pokoknya bank yang plat merah itu kan kasus seperti itu ya istilahnya sudah kita lakukan sampai mungkin P21. Ada juga kasus yang mungkin berimbangan selerti *Phishing*, scamming itu kan hampir-hampir

sama. Cuman polanya misal scamming itu apa itu kan ada dominannya apa orang luar negeri. Kalau *Phishing* itu cenderung orang dalam negeri.

P : Rata-rata itu pak, kalau kasus *Phishing* itu dari mana? Mungkin dari perbankan atau sektor bisnis?

N : ya istilahnya begini lho mba, maksudnya *Phishing* itu berarti kita mungkin ada data yang dalam artian yang mungkin kita punya ATM, punya apa itukan ada kemungkinan besar kena *Phishing* itu sendiri. Begitu juga mungkin seperti yang sekarang menggunakan virtual account dan sebagainya itu mungkin ya kemungkinan besar ya bisa. Bahkan *platform-platform* belanja , jual beli apa semua itu tidak menuntut kemungkinan karena dia ada kode Verifikasi dan sebagainya. Jadi bukan di perbankan saja mungkin dari *platform-platform* jual beli , atau mungkin *platform-platform* yang digunakan untuk transaksi pembayaran itu kita kadang sering mungkin ada OTP , password, atau mungkin pin itukan harus hati-hati. Intinya gini mba maksudnya anda kan cenderung ke akuntansi sebenarnya, jadi kan kalau seperti ini cuman untuk sebagai pengertian saja kecuali mungkin mahasiswa hukum. Kalau hukum nanti ranahnya kan seperti itu, mungkin kalau nanti anda bekerja istilahnya auditor forensik atau berhubungan dengan pembukuan biar paham oh kasus ini seperti ini. Bisa juga nanti mungkin dengan bekerja diperbankan apa itu semua ranahnya kan itu ada tim fraudnya, mungkin akan cenderung ke arah seperti itu. Jadi kalau misalnya kayak ilmu hukumnya sebenarnya sedikit aja. Sebenarnya penekanannya itu cuman untuk sekedar wawasan untuk bahwasanya fenomenanya seperti ini, dampaknya dapat menyebabkan seperti ini. Dampaknya dapat melibatkan dari pihak perbankan, dari pihak kepolisian bahkan dari masyarakat. Yang menjadi PR kita, catatan kita itu ya itu tadi mba. Maksudnya masyarakat di era sekarang itu kan kadang bahasa jawanya gumunan, jadi mudah percaya. Terus istilahnya kagetan dalam arti kita dapat uang hadiah, dapat ini langsung Mengkait-kaitkan gitu, oh betul aku kemarin habis Shopee wajar kalau saya dapat keuntungan seperti ini sering Mengkait-kaitkan. Harusnya kita bener bener

check, pastikan apa semua hadiah itu diberikan sama siapa, password itu diberikan sama siapa itukan kita harus betul-betul waspada. Hati-hati kalau kita ke ATM disuruh misalnya ketik pinnya mba silahkan ganti. Maka dari itu, jika disisi lain mengejar keuntungan ya security dari nasabah itu harus diimbangi, karena disitu kan dapat profit dapat keuntungan , terus kalau misalnya nanti sistem security nya kurang bagus nanti kalau misalnya tidak ada kepercayaan dari nasabah berartikan nasabah dapat beralih ke *platform* A, *platform* B atau bank A, bank C . Konsekuensinya nanti bisa menurunkan kredibilitas dari perusahaan itu. Makannya fungsinya keamanan itu sangat penting apalagi mungkin yang bekerja di instansi manapun yang berhubungan dengan data, ataupun istilahnya dengan kode kode rahasia itu harus bener di upgrade jadi jangan mentang mentang sistem udah bagus pasti aman, ya tidak bisa. Karena apa penjahat itu pasti mencari celah dari itu semua. Jadi antara dari teknologi dan kejahatan akan bekejar-kejaran. Contoh kemarin baru iPhone berapa atau samsung berapa engga sampai satu tahun dia akan keluar baru seri baru. Begitu kita tidak upgrade teknologi itu mungkin kita akan terkena dampaknya. Makanya yang dibutuhkan itu ya tadi kita harus cepat tanggap, peka dan harus ber update. Update dalam arti di bidang kita apa, bermasyarakat, atau HP ya teknologi apa semuanya kita harus hati-hati, harus teliti. Kalau kita ada pekerjaan yang berhubungan jangan kita sambi, harus jeli dalam artian kalau misalnya kita cari browsing di google itu misalnya antara bank A dan semuanya mungkin password nya bagaimana, *email*nya apa, terus mungkin webnya apa, huruf besar kecil titiknya dimana, itu kita harus betul-betul pastikan. Karena apa cek-cek crosscheck final check. Jangan hanya sekilas. Karena apa , ketika itu semua sudah terjadi yasudah kita ga tahu. kalau misalnya yang input langsung tahu. Tapi kalau di dunia maya larinya akan kemana kita belum tahu.Apalagi diimbangi dengan data-data yang tidak valid. Contoh kayak data *Facebook*, ig dan lainnya kalau kita membuat akun itu harus valid kalau engga akan menyulitkan juga. Bukan seperti kayak akun fake,

makannya yang dibutuhkan disamping itu kecerdasan, yaitu moral.Yang pertama itu mental dulu , kalau moralnya itu sudah bagus kalau kamu di kasih kepercayaan apapun itu akan bisa menjaganya. Sepintar apapun dia kalau moralnya kurang baik itu riskan. Karena apa, saya pinter diteknologi mungkin di bujuk sama pelaku , kamu saya bayar sekian buat membobol itu. Jadi pesan moral kita seperti itu, bagi generasi z seperti mba itu ya penekanannya moral, etika, attitude nah itu yang sangat penting. Karena kenapa, kita mengkritik itu boleh tapi etikanya bagaimana. Bukannya gaboleh demo atau gimana, tapikan ada etikanya, attitudenya. Semua kritis ya boleh, emang seharusnya seperti itu karena kenapa setiap sistem itu engga ada kontrolnya, engga ada yang mengkritik atau apa dia bisa membelok mba.

Lampiran 3 Transkip Wawancara : Bapak Muhammad Robani Desember

NARASUMBER 2

Nama : Brigadir Muhammad Robani S.H.
Jabatan: Unit 3/Subdit V Ditreskrimsus
Waktu : Senin, 18 Desember 2023 (08.45)
P : Pewawancara
N : Narasumber
K : Korban

P : Bagaimana tren kasus *Phishing* di Yogyakarta selama tahun 2023?

N : Tren *Phishing* dengan mengatasnamakan (suatu merchant, person, *platform* digital) sebuah instansi dengan maksud mencari kelengahan korban yang membutuhkan/menggunakan layanannya.

P : Tempat/aplikasi apa yang paling sering menjadi *target* serangan *Phishing* di Yogyakarta?

N : *Facebook* dan ig. *Phishing* juga ada yang menggunakan *Email*, Whatsapp. Pelaku *Phishing* sering menggunakan *email* sebagai sarana karena *email* merupakan salah satu komunikasi daring yang umum digunakan dan tersebar luas. *Instagram* itu *platform* berbagi foto dan video yang populer, di mana banyak pengguna membagikan momen pribadi dan informasi secara visual. Pelaku *Phishing* dapat memanfaatkan fitur ini untuk membuat penipuan yang menarik, seperti akun palsu yang meniru selebriti atau perusahaan, guna menarik perhatian pengguna dan mendapatkan informasi pribadi. *Facebook*, media sosial besar dengan jumlah pengguna yang sangat besar. Pelaku *Phishing* menggunakan *Facebook* karena di *platform* ini terdapat beragam informasi pribadi pengguna, mulai dari detail personal hingga hubungan sosial. Dengan memanfaatkan fitur pesan atau membuat halaman palsu, pelaku *Phishing*

dapat menyebarkan penipuan dan mencuri informasi sensitif dari pengguna *Facebook* yang kurang waspada.

P : Bagaimana respons masyarakat terhadap serangan *Phishing* di Yogyakarta, terutama terkait dengan tingkat kesadaran dan pencegahan?

N : kesadaran perlu ditingkatkan, karena masyarakat DIY cenderung belum memahami karakteristik dan fungsi medsos yang digunakan sehingga ada ketidakpahaman tersebut seringkali digunakan sebagai celah oleh para pelaku tindak pidana. Terkendala, masyarakat masih pasif. Karena mereka sendiri tidak peduli dan hanya media untuk komunikasi.

P : Adakah peningkatan kasus *Phishing* yang terkait sektor bisnis tertentu di yogyakarta?

N : Maksudnya gimana?

P : mungkin dari sektor perbankan, manufaktur begitu pak

N : itu data yaa, mungkin maksud kamu modus yang sering digunakan *Phishing* itu sering kali mengatas namakan apa gitu. Kalau kebanyakan pasti merchant, terkait belanja *online* biasanya, nanti selebihnya biar dijawab berdasarkan data sama mas ben nanti.

P : Bagaimana cara pelaku memanfaatkan faktor-faktor sosial atau budaya khususnya di yogyakarta untuk mencapai tujuan mereka?

N : Faktor yang dimaksud seperti apa?

P : Misalkan kayak orang jawa ini segan gitu pak, misal ditanyain tentang hal-hal yang mungkin pribadi dengan orang asing atau bahkan dengan nomer yang tidak dikenal yang mengaku bahwa atmnya ketinggalan atau gimana gitu. Asal dikasih kode otp atau sandinya gitu pak

N : Biasanya para pelaku itu kalau terkait dengan *Illegal acces* itu , yang ini mungkin *illegal acces*. Karena nanti jika saya mengatakan yang tren nanti kamu fokus ke *illegal acces*, kan nanti ada banyak kayak penipuan, itu tindakan untuk menipu atau memanipulasi orang untuk memperoleh keuntungan. pornografi itu materi atau gambar yang secara eksplisit menampilkan konten seksual, terus pencemaran nama baik yang dapat merugikan dan menyesat untuk merusak reputasi orang. pengancaman,

mulai dari ancaman fisik, psikologis orang sampai keamanan seseorang. *illegal acces*, menyerupai suatu media sosial yang secara tidk sah masuk ke akun orang untuk mencuri data atau sandi. Ntar kamu masuk ke *illegal acces*. Kalau terkait *illegal acces* dengan modus *Phishing* nanti biasanya pelaku itu menggunakan form pendaftaran. Meminta korban untuk mendaftarkan akun instragam atau bahkan media sosialnya sebagai syarat penggunaan layanan merchant. Contoh, misal di instragam saya mau menggunakan layanan centang biru, saya harus masukan akun instragam saya karena pelaku mengirimkan formulir digital. Disitu saya harus mencantumkan nama akun saya, karena saya mau menggunakan centang biru ini sebagai suatu contoh penggunaan instragam ya. Saya harus mencantumkan akun media saya, *email* ,*email* pemulihan, nomer pemulihan, setelah data-data saya masukan, pelaku akan mencoba mengakses dengan alasan nanti untuk mendaftarkan layanan centang biru tadi. Saya diminta untuk konfirmasi menggunakan nomer yang ada ditempat saya, itu cara lama. Atau dengan cara baru, biasanya pelaku ini akan mengambil alih akun *email* kita setelah itu pelaku akan merubah sandi, password, akun pemulihan, nomer pemulihan akan dirubah semua dan akhirnya akan digunakan oleh pelaku untuk menggunakan beberapa media sosial kita yang menggunakan *email* sebagai data awal. Jadi ada dua cara, langsung pada saat menggunakan dengan data yang kita punya untuk mengambil salah satu media sosial kita atau dengan menggunakan *email* yang kita cantumkan disitu yang kemudian meminta kode OTP pemulihan yang sebetulnya itu diambil alih dan berlanjut ke pengambilalihan media sosial lainnya seperti itu.

P : apa langkah-langkah yang diambil oleh pemerintah setempat untuk meningkatkan kesadaran dan perlindungan terhadap serangan *Phishing* di yogyakarta?

N : kalau polda DIY sendiri sudah membuat himbauan. Himbauan itu pasti ada media-media sosialnya Polda DIY terutama terus setiap ada rilis dengan penanganan kasus kita pasti akan membuat himbauan juga secara

langsung melalui konferensi pers. Selain itu nanti dari korban kita akan memberikan juga himbauan, panduan dan juga pembelajaran terkait tindak pidana yang sering terjadi terkait media sosial. Kalau yang dari pemerintah sendiri saya kurang tahu, kalau pemerintah nanti ini konteksnya terlalu luas, apakah kemungkinan kominfo atau pemda atau pemerintah secara presiden itu kita belum bisa menyampaikan karena ranahnya terlalu luas. Tapi kalau polda DIY seperti itu tadi konferensi pers maupun media sosial polda DIY semua sudah disampaikan terus kita juga ada layanan dari ditreskrimsus. Nomor kontak yang selalu kita stand by kan 1 x 24 jam untuk layanan konsultasi maupun pelaporan di nomor 081995200008. Ada kontak person dari siber langsung, nanti bisa ditanyakan. Tapi kalu siber sebetulnya di bareskrim nanti ada nomornya sendiri, namanya siberpolri.go.id. Itu isinya layanan terkait aduan maupun laporan sama juga dan himbauan-himbauan terkait tindakan pidana ITE.

P : bagaimana mekanisme pengungkapan polda DIY terhadap kasus dengan modus *Phishing* di wilayah DIY?

N : Prosedur awal korban menyampaikan keluhan dalam bentuk laporan maupun aduan dengan beberapa cara. Satu melalui SPKT polda DIY dan diarahkan ke ditreskrimsus, piket ditreskrimsus terus piket ditreskrimsus diarahkan ke piket Siber, 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 yang tadi. 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 (screenshot percakapan,website yang digunakan oleh pelaku maupun akun dari pelaku, dll)

P : apakah ada biaya yang harus ditanggung korban dalam mengajukan laporan atau melibatkan polda dalam menangani kasus *Phishing*?

N : nggak ada secara umum kita

P : apa saja biaya operasional yang dikeluarkan polda DIY?

N : Secara langsung yang melibatkan korban itu engga ada biaya, tidak ada biaya yang melibatkan korban. Seluruh biaya lidik,sidik sudah terdapat pagu anggarannya.

P : estimasi waktu yang dibutuhkan?

N : tidak terbatas, memaksimalkan masa kadaluarsa tindak pidana. Jadi batas waktu penangananya sampai batas waktu kadaluarsanya. Namanya tindak pidana itu kadaluarsanya dalam masa 10 tahun setelah dilaporkan. Umpamanya, nanti masa penyelidikan kita itu maksimal 10 tahun tapi untuk batasan penanganan dalam suatu perkara tidak ada batasan. Kita itu hanya memaksimalkan masa kadaluarsa.

P : langkah awal polda DIY setelah menerima laporan korban ?

N : melakukan gelar awal untuk menentukan tindak pidana yang dilanggar oleh pelaku. Kemudian meminta keterangan dari korban berdasarkan kronologi. Meminta petunjuk-petunjuk atau alat bukti yang ditinggalkan oleh pelaku.

P : Bagaimana Polda DIY melakukan penyelidikan dan pengumpulan informasi terhadap pelaku *Phishing*?

N : proses penyelidikannya menelusuri semua petunjuk dan alur yang dilakukan oleh pelaku dalam proses tindak pidana. memastikan identitas pelaku, kronologi melakukan tindak pidana, bukti dan alat yang digunakan oleh pelaku dalam melakukan tindak pidana. Setelah penyelidikan selesai, penyelidik akan melakukan gelar perkara untuk menentukan tindak pidana yang kemudian hasil gelar perkara tersebut dituangkan dalam SP2HP yang diserahkan kepada korban atau pelapor. Untuk tindak lanjut penanganan (menghentikan penyelidikan atau melanjutkan ke tahap penyidikan)

P : apa sanksi atau peraturan yang dapat dikenakan kepada pelaku *Phishing* setelah hasil diungkap oleh Polda DIY ?

N : sanksi berdasarkan dugaan tindak pidana yang dilanggar (KUHP UU ITE maupun UU lainnya)

P : proses koordinasi antara Polda DIY dengan pihak lain seperti lembaga keuangan dan instansi terkait kasus *Phishing*?

N : diatur dalam PERKAP nomor 10 tahun 2022, sebentar mba (ada korban yang melapor adanya tindak penipuan) sini, pindah kesini sekalian mbanya sambil belajar. Jadi gimana ceritanya, ini contoh ya mba kasus.

K : saya kenal media sosial aplikasi pertemanan kencan

N : itu dimana ? Di playstore ada?

K : ada, terus intinya saya dikenalkan main trading crypto terus diajak

N : anda kenal dengan aplikasi itu terus dikenalkan dengan seseorang?

K : engga dia main disitu terus saya diajak dan dikenalkan

N : bisa diperlihatkan aplikasinya?

K : (korban memperlihatkan applikasi yang digunakan)

K : terus intinya saya dikenalin dengan trading crypto.

N : dikenalkan dengan seseorang?

K : engga, dia main itu. Dia ngajak saya. Langsung di ajak main di applikasi itu

N : boleh dilihat aplikasinya?

K : (menunjukkan aplikasinya)

N : boleh saya lihat pas anda kenalan dengan pelaku ini?

K : (menunjukkan bukti chat) karena saya diperkenalkan dengan website ini tadi.

N : website itu tadi dikenalkan lewat wa

K : setelah saya kenalan dengan segala macam.

N : namanya siapa?

K : (sensor nama pelaku)

N : setelah tukeran nomor wa itu kalian yang dibahas pertama kali apa?

K : yang dibahas ya kenalan aja, kamu bekerja dimana, ya biasa saling kenal aja. terus suatu saat dia minta tolong mainin akun trading dia.

N : mainin akun trading ini dalam rangka apa? Maksudnya anda disuruh masukan uang kesitu?

K : engga, jadi ceritanya dia xxx. Dia gaboleh main trading. karena aturannya di kantor itu orang internal tidak boleh main itu. Tapi *platform* yang dipakai bukan indodax, yang dipakai main. Karena dia gabisa main di hpnya, karena IP-nya nanti bakal ke detected kantor, saya diminta untuk mainin dan saya disitu udah ngerasa sudah ga enak. saya udah nolak pak sebenarnya tapi karena terus besoknya engga saya mainin. yaudahlah lagian dia juga gak minta uang ke saya, jadi dia itu suruh saya login terus ngechat di adminya di website ini, terus nanti disuruh bilang saya mau topup. Saya login pakai akun dia, *email* dia, password dia. Saya mau topup terus adminnya ngasih info nomer rekening, nah nomer rekeningnya itu.

N : chatnya ada engga?

K : yang chat dia, di akunnya dia belum saya *screenshot*, saya harus login lagi. Sebenernya ada historinya, kalau saya bisa buka dan passwordnya belum di ganti. Terus nomer rekening tadi saya informasikan ke dia harus transfer ke sini, terus dia ngirim saya bukti transfer , saya kirimkan ke admin, terus adminnya menyetujui, okey topup. Terus setelah itu, setelah dia berhasil topup saya masuk ke walletnya dia, di cek saldonya dia, udah nambah. Terus setelah di wallet, saya masuk ke menu ini untuk membeli crypto tadi, saya dah gabisa, akun saya dah dibekukan untuk beli koin tadi. Untuk beli koin, kelihatan berhasil ada untungnya.

N : kamu tertarik?

K : sebenarnya saya engga tertarik juga, cuman saya gimana ya diajak main. Kamu juga main dong, ini juga uang untuk ibaratnya kita gitu lho. Sebenarnya saya gakmau dan gak tertarik sebenarnya. Saya disuruh buat akun sendiri akhirnya. akun sendiri, saya daftar sendiri terus saya melakukan hal yang sama chat admin segala macam dan topup.

N : intinya kamu tertarik engga?

K : sebenernya dalam hati engga tertarik tapi karena disarankan.

N : yasudah intinya kamu melakukan

K : iya saya melakukan, saya awalnya topup cuman 500rb, terus saya main seperti yang ditunjukkan dia dan bener ada untungnya tapi kan saya gatau

pak itu beneran atau engga. Soalnya di website ini seolah-olah untung. Terus seiring berjalannya waktu, ceritanya gini, dia itu ngakunya data analis. Dia tahu kapan pasarnya bagus dan jelek gitukan. Setiap dia main disarankan saya juga main supaya untung. Pada akhirnya saya main. Seiring berjalannya waktu saya ngerasa orang ini emang fiks engga benerkan, saya coba cut off, kita udahan. Terus saya ingin meng withdraw deposit saya. Pas saya nge with draw gabisa. Saya complain ke admin, katanya akun saya dibekukan karena melakukan istilahnya aktivitas ilegal. Saya ga paham, saya gak pernah melakukan apa-apa tapi akunnya jawabannya formalitas.

N : websitenya namanya apa mas?

K : (sensor nama website)

N : ini ada dua, kamu mau laporan yang mana? Kerugian kamu di aplikasi trading berapa?

K : 20.500 JT

N : kamu mau ngelaporin aplikasi trading ini atau kamu mau ngelaporin orang yang kmau chat?

K : Iya dua-duanya pak, pinginnya sih supaya uangnya kembali ya

N : tidak bisa , kita tidak bisa memastikan uangmu kembali.

K : kepinginnya sih begitu, nah pinginya terungkap orang ini siapa. Tapi yang di tekankan itu karena saya main di aplikasi itu dan deposit saya berupa uang di crypto tadi tidak bisa ditarik.

N : dia bisa memastikan engga, kalau kamu main itu untung?

K : dia memastikan,

N : ada engga bukti chatnya kalau kamu untung?

K : ada

N : coba saya lihat

K : (memberikan bukti percakapan)

N : ini merupakan salah satu metode *Phishing*, jadi dia mengaku mengatas namakan seseorang. Menawarkan sebuah *platform* trading kemudian

dalam *platform* trading itu dia dalam proses penawaran itu menjanjikan. kalau *platform* trading itu dibawah naungan kemendag .

P : kemendag pak?

N : iya, jadi ada beberapa *platform* yang bisa digunakan kalau kita menyampaikan masalah *platform* ya, atas nama *platform*. Kalau *platform* Fintech dibawah ojk, *platform* trading itu dibawah Bappebti. Bappebti itu ada di kementerian perdagangan. Subnya itu di Bappebti.

Kalau *platform* perdagangan itu karena ekonomi global jadi kementerian perdagangan tidak mengatur secara khusus. Shopee itu masuk di kementerian perdagangan tetapi kayak Arizona , Amazon itu tidak masuk ke Bappebti. Saya jelaskan lagi runtutan tentang pelaporan ya.

P : baik pak

N : Dari awal korban melaporkan kejadian, ada dua cara melaporkannya. Yang pertama, Melalui SPKT. Yang kedua, lapor siaga Piket Ditreskrimsus. Ini saya menjelaskan yang laporan di SPKT ya. SPKT membuat laporan polisi. Korban membawa dokumen berupa apa saja yang menjadi petunjuk mislanya: isi percakapan, website yang digunakan pelaku, akun pelaku, dll. Laporan itu kemudian diteruskan kepada penyidik, yang memiliki kewajiban melakukan penyelidikan. Penyelidikan bertujuan untuk menentukan apakah ada indikasi pidana atau tidak. Jika ada, penyelidikan bisa ditingkatkan ke penyidikan, dengan pembuatan gelar penyidikan dan kemungkinan dilibatkannya sidik atau penyilidikan. Penyidikan dilakukan untuk mengumpulkan bukti lebih lanjut, menentukan tersangka, dan mencari kejelasan terhadap peristiwa dengan cara melakukan analisa profil dan melecak keberadaan pelaku. Setelah selesai, hasil penyidikan bersama barang bukti atau tersangka diserahkan ke JPU (Jaksa Penuntut Umum). Peran jaksa adalah menuntut di persidangan. Dengan demikian, tugas polisi melibatkan menerima laporan, melakukan penyelidikan, dan selesai sampai pada tahap penyidikan, sedangkan tugas jaksa dimulai dari situ untuk menuntut di pengadilan. Itu

udah ada mas risky, dilanjut sama mas Risky kalau mau lihat proses ini silahkan.

P : baik pak

Lampiran 4 Transkip Wawancara : Bapak Riski Praditya Putra Desember

NARASUMBER 3

Nama : Bripda Riski Praditya Putra
Jabatan: Banum Subdit V/Siber Ditreskrimsus
Waktu : Senin, 18 Desember 2023 (09.58)
P : Pewawancara
N : Narasumber

P : Mekanisme pengungkapan kasus *Phishing* itu bagaimana ya pak? Urutannya jika korban ingin melaporkan ke kepolisian. Mulai dari mana ya?

N : Berarti dari awal itu kan korban merasakan bahwa mendapatkan tindak pidana, setelah itu korban melakukan pengaduan di kepolisian. setelah itu, pada korban membuat laporan awal ke SPKT depan dan memberikan surat rekomendasi gelar awal. disini pihak kepolisian akan memberikan tanggapan atau masukan terhadap kasus korban, jika terjadi tindak pidana korban harus seperti apa. setelah itu 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. Setelah itu, korban nanti menceritakan kronologinya seperti apa terus kapan,dimana pokoknya semua itu diceritakan nanti yang piket ini biasanya kalau tindak pidana itu memenuhi unsur itu langsung dibuatkan surat laporan. Jadi, mengisi kertas pink, kertas pengaduan nanti itu kronologi disitu diisi seperti hari, tanggal, unsur pidananya apa setelah itu nanti kembali lagi ke SPKT untuk dibuatkan Surat Pengaduan. Setelah dari sana nanti mendapatkan Surat Pengaduan terus dibawa lagi ke sini mba (Krimsus) dengan membawa kertas pink tersebut. kita akan membuat SPTL (surat tanda penerimaan laporan) agar nanti korban ingin mengetahui pekembangan kasusnya wajib membawa

SPTL. Setelah disini nanti mulai untuk BAP, dimintai keterangan. Setelah BAP selesai menunggu perkembangannya seperti apa, karena kan dari kami surat pengaduan itu akan naik ke pimpinan. Pimpinan nanti di disposisikan ke mana, diturunkannya kemana, sebenarnya kalau UU ITE itu nanti ke Siber. Jadi, masuk ke Siber pengaduannya, setelah itu disposisikan lagi oleh kabsudit ke penyidik yang menangani. yang kedua adalah naik ke tahap penyelidikan, disini kami mencari bukti adanya tindak pidana. yang pertama kami lakukan itu menyusun surat perintah tugas, surat perintah penyelidikan dan membuat SP2HP A1 yang dilakukan oleh penyidik. Lalu setelah kami membuat surat tersebut kami melakukan pemeriksaan kepasa saksi, disini kami meminta keterangan tentang kejadian yang dialami korban dan memeriksa, ada tindakan pindana yang dilakukan. Setelah itu menganalisa bukti yang didapat dari korban, kita pilah-pilih lagi mba, apakah ada kaitannya dengan tindak pidana. seperti nomor telfon, dompet digital, rekening, *link* yang menjadi alat bukti korban pada saat terjadinya kasus *Phishing*. jika kita menemukan adanya tindak pidana yang diterima oleh korban kami akan membuat laporan hasil penyelidikan. Laporan hasil penyelidikan ini adalah temuan-temuan yang dilakukan penyidik. mulai dari informasi korban, waktunya, lokasinya kapan dan pelakunya. 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. Nanti biasanya kalau kasus yang paling susah diungkap itu kasus penipuan *online*, Illegal Acces itu susah karena pembuktiannya itu sulit mba. Setelah itu nanti naik ke tahap Penyelidikan, jadi kita penyelidikan dulu nanti kalau bukti-bukti yang kita dapat itu bisa menunjukkan ke pelaku itu biasanya kita akan melakukan Penindakan. Tidak semua pengaduan di proses karena kita lihat apakah kasus ada unsur tindak pidananya. Kalau tidak bisa secara bukti nanti itu kita akan gelarkan seperti apa, mencari solusinya bagaimana, terus biasanya kita sampaikan ke pelapor kendalanya seperti apa kita sampaikan mba,

karenakan mengungkap kasus tindak pidana penipun *online*, illegal Acces itu engga mudah juga. Karena pelaku-pelaku sekarang itu sudah pintar mba, misal nomernya dibuanglah. pada saat kita mengidentifikasi pelaku juga makin sulit salah satunya dengan pelaku membuang nomernya itu, lalu kalau pakai *email*/media sosial itu pakai akun dari hasil beli, bukan akun yang asli. kita memproses kasus tersebut juga lumayan mba karena kita butuh informasi yang relevan. Setelah naik tahap penyelidikan nanti kalau memenuhi unsur dan pelakunya jelas nanti akan ke tahap Penyidikan. Nah pada tahap penyidikan itu bisa melakukan upaya paksa penangkapan ke pelaku.

P : butuh waktu berapa lama kira-kira kalau paling cepat untuk kasus penipuan *online*, illegal acces, *Phishing*?

N : kalau paling cepet itu tergantung buket,tergantung apa yang kita dapat dari pelapor misalkan buket awal itu nanti kita olah sampai menemukan pelaku. Jadi apa ya mba, penyidik itu kadang kesusahan ketika buket awalnnya itu minim gitu. Jadi semakin banyak buket yang diberikan oleh pelapor seperti misalnya: nomer telfonnya, ATM nya apa, terus transaksinya dimana, Instragamnnya apa, social medianya apa itu malah mempermudah penyidik untuk menganalisa mengolah data itu.

P : terus kalau setelah dari tahap penyelidik itu tahapannya apa lagi pak?

N : setelah dari penyelidikan naik ke penyidikan, penyidikan ini kita melakukan investigasi lebih mendalam untuk mengungkapkan fakta yang didapatkan. 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. 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. pada saat memeriksa saksi-saksi kami juga melakukan analisa pro*file* untuk melihat latar belakang pelaku ini, seperti apa dia di

kehidupan sehari-hari. setelah kami dapatkan latar belakangnya, kami melacak pelaku tersebut, posisi terakhirnya dimana, pelaku sedang melakukan apa dan nanti kita akan koordinasi. setelah itu kami akan melakukan gelar perkara pelaku untuk mengetahui apakah itu benar-benar pelaku. dengan mengumpulkan bukti-bukti yang mengarahkan kepada pelaku. kalau sudah mengetahui pelakunya siapa, 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. Kami juga melakukan penggeledahan dan penyitaan barang bukti pelaku. penggeledahannya terhadap barang ya mba, alat buktinya itu semisal seperti telfon, buku tabungan yang biasanya digunakan pelaku untuk melakukan kejahatan tersebut. 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. Membuat berkas seperti itu mba, berkasnya warna merah. yang isinya seperti berita acara,analisa penyelidik. Jadi setelah berkasnya jadi kita geser 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, dilampirkan mba. Kita nanti melengkapi itu, setelah itu kita melengkapinya, 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.

P : habis dari tahap 2 kejaksaan, apa tahapan selanjutnya?

N : Jadi setelah tahap 2 itu nanti ada persidangan, sidang untuk menentukan berapa lama hukuman yang di dapatkan pelaku. Jadi anti biasanya kami mendapatkan surat dari kejaksaan untuk sidang.

P : Kalau kendalanya dan kekurangannya apa saja pak?

N : Kendala dan kekurangan apa mba?

P : Untuk mengukapkan kasus, misal dari kurangnya bukti terus apa lagi yang biasanya sering dihadapi?

N : kalau kekurangan itu karena ada beberapa hal yang tidak cukup mba, bisa jadi dari keterangan,barang bukti dan lainnya. biasanya kekurangan dari pelapor sih mba, yang komunikasinya ke kami itu kurang. kurangnya bahan -bahan awal untuk melaporkan kasus itu juga kendala.pelaku sekarang juga pinter ya mba, seiring berjalannya dan berkembangnya teknologi, itu juga kendala bagi kami. halangan atau rintangan itu pasti ada mba pada saat pelaksanaan. itu jadi pr buat kami saat melakukan tugas.

P : ada koordinasi tidak? Misalnya pelapor itu kenanya dengan suatu lembaga. Apakah ada koordinasi antara lembaga dengan pihak kepolisian?

N : Maksudnya gimana ya mba?

P : misal saya kena kasus dengan lembaga perbankan. Apakah ada koordinasi antara perbankan dengan kepolisian?

N : kalau koordinasi itu pasti, soalnya kan memiliki ranah, Ranah itu juga di dunia perbankan juga, bank-bank itu juga punya ranah. Jadi kita gak asal langsung masuk ke lembaga gitu. Istilahnya kita permisilah. Koordinasi itu wajib.

P : Bagaimana langkah perbaikan buat polda untuk kasus *Phishing*? Untuk meningkatkanefektifitas polda dalam pengungkapan kasus?

N : untuk langkah-langkah perbaikan itu sebenarnya dari penyidik, untuk mengungkap kasus memang butuh waktu. dari melakukan analisa awal itu pasti sama. dari sdm kami sendiri dalam proses penyelidikan, Soalnya kan harus ada buket awal dulu. buket awal yang lengkap menjadi kunci untuk memahami kasus, namun jika tidak dapat dibuktikan oleh korban bbisa menyebabkan kendala. oleh karena itu mba, fokusnya diberikan pengembangan keterampilan penyidik dalam mengumpulkan bukti yang kuat. itu langkah-langkah perbaikannya. Jadi ketika buket awalnya itu

lengkap dapat membantu, tapi ketika buketnya dari awal itu sudah gak bisa dibuktikan oleh korban itu kami kesulitan juga mba. Alat bukti juga diperlukan, karena dengan adanya barang bukti bisa mendapatkan keterangan saksi dan sebagai bahan pembuktian. Kita juga melakukan kerjasama dengan beberapa lembaga masyrakat dan Sosialisasi dengan menghimbau masyarakat untuk lebih hati-hati, biasanya kami akan menggelar konferensi pers.

P : rata-rata untuk kasus *Phishing* itu kena UU ITE pasal berapa pak?

N : *Phishing* itu akan masuk ke Illegal Acces juga, pasal 30 ayat 1 UU ITE.

Lampiran 5 Transkip Wawancara : Bapak Riski Praditya Putra Januari

NARASUMBER 4

Nama : Bripda Riski Praditya Putra
Jabatan: Banum Subdit V/Siber Ditreskrimsus
Waktu : Kamis, 11 Januari 2024 (10.25)
P : Pewawancara
N : Narasumber

P : Bapak apakah *Phishing* ada jenisnya? Atau hanya modus yang menggunakan beberapa cara untuk melakukannya? Bagaimana penanganannya?

N : jadi untuk penanganannya nanti masuk ke *illegal acces* dengan modus *Phishing* itu modelnya berupa *link*. Jadi ketika korban memencet *link* nanti ada muncul misalnya modusnya dari ATM A,B,C menyerupai entitas terpercaya. Yang terakhir kemarin ada yang mencet *link* muncul tampilan seperti aplikasi dompet digital kayak Dana. Dari dana itu, ngisi kode-kode. Biasanya kode OTP nah dari situ pelaku bisa monitor karena yang buat tampilan aplikasi itu Pelaku melalui *link* Tersebut. Jadi OTPnya terbaca oleh pelaku, setelah itu digunakan masuk ke akun dompet digital oleh pelaku. Pada saat itu akun dompet digital tersebut ada saldo. Saldonya diambil alih ke pelaku.

P : apa cuman hanya *link* saja?

N : kebanyakan *link* sih mba, kalau pdf, undangan itu jarang. Karena mungkin dari kami sudah mengedukasi lewat *platform Instagram*. Kalau ada undangan yang berbentuk pdf, *link* dan seterusnya itu jangan sampai dibuka. Apalagi sama orang yang dikenal mba.

P : jadi rata-rata memang kasusnya itu modusnya menggunakan *link* ya?

N : iya betul, kalau *Phishing* kebanyakan dari *link*.

P : kalau yang dalam bentuk foto, video pak?

N : kalau bentuk foto dan video, untuk *Phishing* dengan modus menggunakan foto atau video itu sementara belum ada laporannya dan prediksi dari kami kemuning kedepannya bakal ada foto dan video itu disisipin Malware untuk modus *Phishing*.

P : kalau kendala sendiri yang dihadapi dengan modus pelaku yang bermacam-macam ini apa ya pak? Misalnya kayak nomer hp fiktif gitu pak.

N : kebanyakan kendalanya dari nomer rekening. Jadi nomer rekening pelaku itu menggunakan rekening tampungan. Dan rekening tampungan itu di jual belikan dalam artian pelaku itu mencari rekening random namanya. Intinya pelaku ini beli ke orang, kebanyakan rekening ini dari Jawa Barat. Jadi pelaku ini beli dulu rekeningnya lalu rekening itu dibuat misalnya 5 rekening itu dibuat untuk uang tampungan dari modus *Phishing* tersebut. Itu rekeningnya ada yang ATM bisa jadi juga mobile banking.

P : jadi tiba-tiba ada yang ngisi saldo gitu pak dari orang yang tidak dikenali?

N : nah jadi setelah terjadi pengambil Alihan, misalnya dari dompet digital tadi itu diambil alih terus di transfer ke rekening tampungan. Kalau tidak rekening tampungan ya dompet digital tampungan. Setelah dari situ, ada pelaku yg transfer lagu ke ATM tampungan lagi habis itu ke nomor rekeningnya sendiri. Jadi alurnya seperti itu

P : selain dari nomer rekening ada lagi gak pak?

N : selain nomer rekening itu dompet digital mba, kadang juga mereka mainnya dari dana ke dana

P : kemarin ada kasus pak, ada orang yang tiba-tiba mentransfer sejumlah uang dengan nominal yang cukup besar dari rekening yang tidak diketahui. Padahal orang tersebut merasa sedang tidak melakukan transaksi apapun. Setelah itu orang yg ditransfer uang tersebut di laporkan kepada pihak yg transfer uang tersebut.

N : jadi misalnya mba dapat transfer dari orang yg tidak dikenal 60 jt dan orang yg mentransfer itu laporan. Kalau itu kemungkinan salah transfer, kalaupun mba menerima pasti mba merasa bahwa uang tersebut bukan

milik mba dan punya niatan untuk mengembalikan. Kemungkinan salah transfer dan belum ada modus tersebut.

P : jadi kasusnya masih rata-rata menggunakan *link* ya?

N : betul mba, rata-rata kasus memang dari *link*, laporan yang kami dapat dari *link*

P : apa mungkin pak sudah ada yang kena modus yang dari undangan atau pdf itu tapi tidak dilanjut lapor kepolisian?

N : kalau itu tergantung dari korban sih mba, biasanya kalau korban sudah mengalami kerugian gitu baru bisa dilaporkan. Kalau korban tidak ada kerugian tidak bisa dilaporkan.

P : untuk kerugian apa harus berupa uang saja, misal kalau data yang dicuri?

N : itu bisa mba nanti masuknya ke manipulasi data, biasanya digunakan untuk pinjol. Kalau kebanyakan *Phishing* itu datanya aman-aman saja mba, mereka soalnya fokusnya ke uang.

P : kalau *Phishing* ada kelompoknya sendiri engga pak?

N : kalau *Phishing* itu ada kelompoknya, ada jaringannya

P : apakah Polda pernah meringkus jaringan tersebut?

N : jadi modelnya itu tetep perorangan, mengoperasikan itu tetep perorangan. Kita masih menyelidikinya, jaringannya kerjasama sama siapa. Koordinasi mereka pasti satu wilayah. Dan itu biasanya daerah Sumatra sana

P : menurut bapak langkah perbaikan apa yang perlu dilakukan? seperti misalnya bekerjasama dengan media sosialnya, sosialisasi dengan masyarakat.

N : Untuk perbaikan, sosialisasi dengan masyarakat itu juga pasti. tujuannya agar masyarakat mempunyai pemahaman dan kesadaran tentang bahayanya kasus tersebut. tindakan apa yang dilakukan masyarakat jika kasus seperti itu terjadi. bekerjasama dengan lembaga bank, media sosial atau kominfo. untuk bank sendiri kita kerjasama untuk mengatur kerangka kerjanya seperti apa atau etiknya seperti apa dan tata caranyanya bagaimana terkait dengan pertukaran informasi biar makin efektif. untuk mendeteksi, mencegah kasus yang sama terjadi lagi, kerja sama yang

dilakukan dengan media sosial/kominfo ini agar melindungi masyarakat dari upaya penipuan *online* dan ancaman keamanan siber.

P : Pembobolan akun itu apa saja ya pak jenis atau modus yang digunakan oleh para pelaku?

N : banyak mba. misalnya kayak mengisi kredensial itu pelaku menggunakan nama pengguna dan kata sandi yang didapat dari pelanggaran yang sebelumnya. malware, perangkat yang biasanya disisipkan untuk mencuri atau mengakses. melakukan pencatatan kunci dengan merekam setiap pengguna perangkat lunak untuk informasi masuknya atau login. pelaku menyusup ke komunikasi antara dua pihak untuk mengakses atau mencuri informasi yang sedang dipertukarkan. pokoknya yang berbau kata sandi juga mudah terjadi *Phishing* mba. cuman, kasus yang sering polda tangani itu kasus *Phishing* mba.

Lampiran 6 Peraturan-Peraturan Terkait

PERATURAN KEPALA KEPOLISIAN NEGARA REPUBLIK INDONESIA

NOMOR 12 TAHUN 2009

TENTANG

PENGAWASAN DAN PENGENDALIAN PENANGANAN PERKARA PIDANA DI LINGKUNGAN KEPOLISIAN NEGARA REPUBLIK INDONESIA

DENGAN RAHMAT TUHAN YANG MAHA ESA

KEPALA KEPOLISIAN NEGARA REPUBLIK INDONESIA,

Menimbang : a. bahwa tugas dan wewenang penanganan perkara pidana yang merupakan pelaksanaan dari peran kepolisian di bidang penyidikan yang diemban oleh satuan fungsi reserse dalam pelaksanaannya sangat rawan terjadi penyimpangan yang dapat menimbulkan pelanggaran hak asasi manusia;

b. bahwa untuk menjamin kelancaran pelaksanaan penyidikan dan untuk menghindari terjadinya penyimpangan atau penyalahgunaan penggunaan kewenangan oleh aparat Kepolisian Negara Republik Indonesia selaku penyidik dan penyelidik dari Markas Besar Kepolisian Negara Republik Indonesia sampai kesatuan wilayah terdepan, harus dilakukan pengawasan dan pengendalian yang efektif;

c. bahwa untuk meningkatkan fungsi pengawasan dan pengendalian serta pertanggungjawaban pelaksanaan tugas dan kewenangan di bidang penyidikan perlu disusun aturan yang jelas sebagai pedoman pelaksanaan pengendalian dan pelaksanaan penyidikan;

d. bahwa berdasarkan pertimbangan sebagaimana dimaksud dalam huruf a, huruf b dan huruf c, perlu menetapkan Peraturan Kepala Kepolisian Negara Republik Indonesia tentang Pengawasan dan Pengendalian Penanganan Perkara Pidana di Lingkungan Kepolisian Negara Republik Indonesia;

Mengingat : 1. Undang-Undang Nomor 8 Tahun 1981 tentang Hukum Acara Pidana (Lembaran Negara Republik Indonesia Tahun 1981 Nomor 76, Tambahan Lembaran Negara Republik Indonesia Nomor 3209);

2. Undang-Undang .....

www.lorrytutu.com

PERATURAN KEPALA KEPOLISIAN NEGARA REPUBLIK INDONESIA

NOMOR 14 TAHUN 2012

TENTANG

MANAJEMEN PENYIDIKAN TINDAK PIDANA

DENGAN RAHMAT TUHAN YANG MAHA ESA

KEPALA KEPOLISIAN NEGARA REPUBLIK INDONESIA,

Menimbang :

a. bahwa Kepolisian Negara Republik Indonesia merupakan alat negara yang berperan dalam memelihara keamanan dan ketertiban, menegakkan hukum, memberikan perlindungan, pengayoman dan pelayanan kepada masyarakat dalam rangka memelihara keamanan dalam negeri;

b. bahwa dalam melaksanakan tugas penegakan hukum, penyidik Kepolisian Negara Republik Indonesia mempunyai tugas, fungsi, dan wewenang di bidang penyidikan tindak pidana, yang dilaksanakan secara profesional, transparan, dan akuntabel terhadap setiap perkara pidana guna terwujudnya supremasi hukum yang mencerminkan rasa keadilan;

c. bahwa berdasarkan pertimbangan sebagaimana dimaksud dalam huruf a dan huruf b, perlu menetapkan Peraturan Kepala Kepolisian Negara Republik Indonesia tentang Manejemen Penyidikan Tindak Pidana;

Mengingat :

1. Undang-Undang Nomor 8 Tahun 1981 tentang Hukum Acara Pidana (Lembaran Negara Republik Indonesia Tahun 1981 Nomor 76, Tambahan Lembaran Negara Republik Indonesia Nomor 3209);

2. Undang-Undang Nomor 2 Tahun 2002 tentang Kepolisian Negara Republik Indonesia (Lembaran Negara Republik Indonesia Tahun 2002 Nomor 2, Tambahan Lembaran Negara Republik Indonesia Nomor 4168);

3. Peraturan Presiden Nomor 52 Tahun 2010 tentang Susunan Organisasi dan Tata Kerja Kepolisian Negara Republik Indonesia;

MEMUTUSKAN:

Menetapkan : **PERATURAN KEPALA KEPOLISIAN NEGARA REPUBLIK INDONESIA TENTANG MANAJEMEN PENYIDIKAN TINDAK PIDANA.**

BAB ...

PERATURAN KEPALA KEPOLISIAN NEGARA REPUBLIK INDONESIA

NOMOR 22 TAHUN 2010

TENTANG

SUSUNAN ORGANISASI DAN TATA KERJA PADA TINGKAT KEPOLISIAN DAERAH

DENGAN RAHMAT TUHAN YANG MAHA ESA

KEPALA KEPOLISIAN NEGARA REPUBLIK INDONESIA,

Menimbang : bahwa untuk melaksanakan ketentuan Pasal 35 Peraturan Presiden Nomor 52 Tahun 2010 tentang Susunan Organisasi dan Tata Kerja Kepolisian Negara Republik Indonesia, perlu menetapkan Peraturan Kepala Kepolisian Negara Republik Indonesia tentang Susunan Organisasi dan Tata Kerja Pada Tingkat Kepolisian Daerah;

Mengingat :

1. Undang-Undang Nomor 2 Tahun 2002 tentang Kepolisian Negara Republik Indonesia (Lembaran Negara Republik Indonesia Tahun 2002 Nomor 2, Tambahan Lembaran Negara Republik Indonesia Nomor 4168);

2. Peraturan Presiden Nomor 52 Tahun 2010 tentang Susunan Organisasi dan Tata Kerja Kepolisian Negara Republik Indonesia;

MEMUTUSKAN

Menetapkan : **PERATURAN KEPALA KEPOLISIAN NEGARA REPUBLIK INDONESIA TENTANG SUSUNAN ORGANISASI DAN TATA KERJA PADA TINGKAT KEPOLISIAN DAERAH**

BAB I

KETENTUAN UMUM

Pasal 1

Dalam Peraturan ini yang dimaksud dengan:

1. Kepolisian …..

PERATURAN PEMERINTAH REPUBLIK INDONESIA
NOMOR 23 TAHUN 2007

TENTANG
DAERAH HUKUM KEPOLISIAN NEGARA REPUBLIK INDONESIA

DENGAN RAHMAT TUHAN YANG MAHA ESA

PRESIDEN REPUBLIK INDONESIA,

Menimbang : bahwa untuk melaksanakan ketentuan Pasal 6 ayat (3) Undang-Undang Nomor 2 Tahun 2002 tentang Kepolisian Negara Republik Indonesia, perlu menetapkan Peraturan Pemerintah tentang Daerah Hukum Kepolisian Negara Republik Indonesia;

Mengingat :
1. Pasal 5 ayat (2) Undang-Undang Dasar Negara Republik Indonesia Tahun 1945;
2. Undang-Undang Nomor 2 Tahun 2002 tentang Kepolisian Negara Republik Indonesia (Lembaran Negara Republik Indonesia Tahun 2002 Nomor 2, Tambahan Lembaran Negara Republik Indonesia Nomor 4168);

MEMUTUSKAN:

Menetapkan : PERATURAN PEMERINTAH TENTANG DAERAH HUKUM KEPOLISIAN NEGARA REPUBLIK INDONESIA.

BAB I ...

SALINAN

PRESIDEN
REPUBLIK INDONESIA

UNDANG-UNDANG REPUBLIK INDONESIA

NOMOR 19 TAHUN 2016

TENTANG

PERUBAHAN ATAS UNDANG-UNDANG

NOMOR 11 TAHUN 2008

TENTANG INFORMASI DAN TRANSAKSI ELEKTRONIK

DENGAN RAHMAT TUHAN YANG MAHA ESA

PRESIDEN REPUBLIK INDONESIA,

Menimbang : a. bahwa untuk menjamin pengakuan serta penghormatan atas hak dan kebebasan orang lain dan untuk memenuhi tuntutan yang adil sesuai dengan pertimbangan keamanan dan ketertiban umum dalam suatu masyarakat yang demokratis perlu dilakukan perubahan terhadap Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik agar terwujud keadilan, ketertiban umum, dan kepastian hukum;

b. bahwa berdasarkan pertimbangan sebagaimana dimaksud dalam huruf a, perlu membentuk Undang-Undang tentang Perubahan atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik;

Mengingat : 1. Pasal 5 ayat (1), Pasal 20, Pasal 25A, Pasal 28D ayat (1), Pasal 28E ayat (2), Pasal 28E ayat (3), Pasal 28F, Pasal 28G ayat (1), Pasal 28J ayat (2), dan Pasal 33 ayat (2) Undang-Undang Dasar Negara Republik Indonesia Tahun 1945;

2. Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (Lembaran Negara Republik Indonesia Tahun 2008 Nomor 58, Tambahan Lembaran Negara Republik Indonesia Nomor 4843);

Dengan . . .

KITAB UNDANG-UNDANG

HUKUM ACARA PIDANA (KUHAP)

Undang-Undang Nomor 8 Tahun 1981

Bab I Ketentuan Umum
Bab II Ruang Lingkup Berlakunya Undang-undang
Bab III Dasar Peradilan
Bab IV Penyidik dan Penuntut Umum Bagian Kesatu : Penyelidik dan Penyidik
Bab IV Penyidik dan Penuntut Umum Bagian Kedua : Penyidik Pembantu
Bab IV Penyidik dan Penuntut Umum Bagian Ketiga : Penuntut Umum
Bab V Penangkapan, Penahanan, Penggeledahan Badan, Pemasukan Rumah, Penyitaan Dan Pemeriksaan Surat Bagian Kesatu :Penangkapan
Bab V Penangkapan, Penahanan, Penggeledahan Badan, Pemasukan Rumah, Penyitaan Dan Pemeriksaan Surat Bagian Kedua : Penahanan
Bab V Penangkapan, Penahanan, Penggeledahan Badan, Pemasukan Rumah, Penyitaan Dan Pemeriksaan Surat Bagian Ketiga : Penggeledahan
Bab V Penangkapan, Penahanan, Penggeledahan Badan, Pemasukan Rumah, Penyitaan Dan Pemeriksaan Surat Bagian Keempat : Penyitaan
Bab V Penangkapan, Penahanan, Penggeledahan Badan, Pemasukan Rumah, Penyitaan Dan Pemeriksaan Surat Bagian Kelima : Pemeriksaan Surat
Bab VI Tersangka dan Terdakwa
Bab VII Bantuan Hukum
Bab VIII Berita Acara
Bab IX Sumpah atau Janji
Bab X Wewenang Pengadilan Untuk Mengadili Bagian Kesatu : Praperadilan
Bab X Wewenang Pengadilan Untuk Mengadili Bagian Kedua : Pengadilan Negeri
Bab X Wewenang Pengadilan Untuk Mengadili Bagian Ketiga : Pengadilan Tinggi
Bab X Wewenang Pengadilan Untuk Mengadili Bagian Keempat : Mahkamah Agung
Bab XI Koneksitas
Bab XII Ganti Kerugian dan Rehabilitasi Bagian Kesatu : Ganti Kerugian
Bab XII Ganti Kerugian dan Rehabilitasi Bagian Kedua : Rehabilitasi
Bab XIII Penggabungan Perkara Gugatan Ganti Kerugian
Bab XIV Penyidikan Bagian Kesatu : Penyelidikan
Bab XIV Penyidikan Bagian Kedua : Penyidikan
Bab XV Penuntutan
Bab XVI Pemeriksaan di Sidang Pengadilan Bagian Kesatu : Panggilan dan Dakwaan
Bab XVI Pemeriksaan di Sidang Pengadilan Bagian Kedua : Memutus Sengketa Mengenai Wewenang Mengadili
Bab XVI Pemeriksaan di Sidang Pengadilan Bagian Ketiga : Acara Pemeriksaan Biasa
Bab XVI Pemeriksaan di Sidang Pengadilan Bagian Keempat : Pembuktian dan Putusan Dalam Acara Pemeriksaan Biasa
Bab XVI Pemeriksaan di Sidang Pengadilan Bagian Kelima : Acara Pemeriksaan Biasa
Bab XVI Pemeriksaan di Sidang Pengadilan Bagian Keenam : Acara Pemeriksaan Cepat
Bab XVI Pemeriksaan di Sidang Pengadilan Bagian Ketujuh : Pelbagai Ketentuan
Bab XVII Upaya Hukum Bagian Kesatu : Pemeriksaan Tingkat Banding
Bab XVII Upaya Hukum Bagian Kedua : Pemeriksaan Untuk Kasasi

PRESIDEN
REPUBLIK INDONESIA

UNDANG-UNDANG REPUBLIK INDONESIA
NOMOR 2 TAHUN 2002
TENTANG
KEPOLISIAN NEGARA REPUBLIK INDONESIA

DENGAN RAHMAT TUHAN YANG MAHA ESA

PRESIDEN REPUBLIK INDONESIA,

Menimbang :

a. bahwa keamanan dalam negeri merupakan syarat utama mendukung terwujudnya masyarakat madani yang adil, makmur, dan beradab berdasarkan Pancasila dan Undang-Undang Dasar Negara Republik Indonesia Tahun 1945;

b. bahwa pemeliharaan keamanan dalam negeri melalui upaya penyelenggaraan fungsi kepolisian yang meliputi pemeliharaan keamanan dan ketertiban masyarakat, penegakan hukum, perlindungan, pengayoman, dan pelayanan kepada masyarakat dilakukan oleh Kepolisian Negara Republik Indonesia selaku alat negara yang dibantu oleh masyarakat dengan menjunjung tinggi hak asasi manusia;

c. bahwa telah terjadi perubahan paradigma dalam sistem ketatanegaraan yang menegaskan pemisahan kelembagaan Tentara Nasional Indonesia dan Kepolisian Negara Republik Indonesia sesuai dengan peran dan fungsi masing-masing;

d. bahwa Undang-Undang Nomor 28 Tahun 1997 tentang Kepolisian Negara Republik Indonesia sudah tidak memadai dan perlu diganti untuk disesuaikan dengan pertumbuhan dan perkembangan hukum serta ketatanegaraan Republik Indonesia;

e. sebagaimana dimaksud dalam huruf a, b, c, dan d, perlu dibentuk Undang-Undang tentang Kepolisian Negara Republik Indonesia;

Mengingat :

1. Pasal 5 ayat (1), Pasal 20, dan Pasal 30 Undang-Undang Dasar Negara Republik Indonesia Tahun 1945;

2. Ketetapan Majelis Permusyawaratan Rakyat Nomor VI/MPR/2000 tentang Pemisahan Tentara Nasional Indonesia dan Kepolisian Negara Republik Indonesia;

3. Ketetapan Majelis Permusyawaratan Rakyat Nomor VII/MPR/2000 tentang Peran Tentara Nasional Indonesia dan Peran Kepolisian Negara Republik Indonesia;

4. Undang-Undang Nomor 8 Tahun 1974 tentang Pokok-Pokok Kepegawaian sebagaimana telah diubah dengan Undang-Undang Nomor 43 Tahun 1999 (Lembaran Negara Tahun 1999 Nomor 169, Tambahan Lembaran Negara Nomor 3890);

Dengan...

Lampiran 7 *Framework* Matrices Tren Permasalahan *Phishing* POLDA DIY

	A : Tren Permasalahan	B : A. Jenis Kejahatan Siber	C : 1. Pembobolan Akun	D : a. *Phishing*	E : 2. Pencemaran Nama Baik	F : 3. Pornografi	G : 4. Pengancaman	H : 5. Penipuan
1 : Cahyono Budi. 04-12-2023		Siber Ditreskrimsus		kalau untuk tahun 2023 ini mungkin kalau kasus *Phishing* itu mungkin kalau dibilang ada peningkatan engga, cuman masih cukup banyak juga dibandingkan tahun lalu. Kalau untuk akhir-akhir ini kasus *Phishing* lumayan.				

	A : Tren Permasalahan	B : A. Jenis Kejahatan Siber	C : 1. Pembobolan Akun	D : a. *Phishing*	E : 2. Pencemaran Nama Baik	F : 3. Pornografi	G : 4. Pengancaman	H : 5. Penipuan
2 : Muhammad Robani. 18-12-2023	Tren *Phishing* dengan mengatasnamakan (suatu *merchant*, person, *platform* digital) sebuah instansi dengan maksud mencari kelengahan korban yang membutuhkan/menggunakan layanannya.		Biasanya para pelaku itu kalau terkait dengan *Illegal acces* itu Karena nanti jika saya mengatakan yang tren nanti kamu fokus ke *illegal acces, illegal acces*, menyerupai suatu media sosial yang secara tidk sah masuk ke akun orang untuk mencuri data atau sandi. Ntar kamu masuk ke *illegal acces*. Kalau terkait *illegal acces* dengan modus *Phishing* nanti biasanya pelaku itu menggunakan form pendaftaran.	Kalau terkait *illegal acces* dengan modus *Phishing*	terus pencemaran nama baik yang dapat merugikan dan menyesat untuk merusak reputasi orang.	pornografi itu materi atau gambar yang secara eksplisit menampilkan konten seksual	pengancaman, mulai dari ancaman fisik, psikologis orang sampai keamanan seseorang.	kan nanti ada banyak kayak penipuan, itu tindakan untuk menipu atau memanipulasi orang untuk memperoleh keuntungan

	A : Tren Permasalahan	B : A. Jenis Kejahatan Siber	C : 1. Pembobolan Akun	D : a. *Phishing*	E : 2. Pencemaran Nama Baik	F : 3. Pornografi	G : 4. Pengancaman	H : 5. Penipuan
3 : Riski Praditya Putra. 11-01-2024				pokoknya yang berbau kata sandi juga mudah terjadi *Phishing* mba.				
4 : Riski Praditya Putra. 18-12-2023				*Phishing* itu akan masuk ke *Illegal Acces* juga, pasal 30 ayat 1 UU ITE.				

	A : B. *Crime* Triangle	B : 1. *Offender* (Pelaku)	C : a. Faktor Pendorong	D : 1). Eksploitasi Perangkat	E : 2). Ketidaktaatan dan keengganan pengguna	F : b. Modus	G : 1). Mengatasnamakan Merchant yang Terpercaya
1 : Cahyono Budi. 04-12-2023		selama ini *case* yang pernah ditangani Polda DIY itu didalamnya ada grup, cuman kadang dia juga perannya berbeda-beda dan ada indikasi juga mereka mungkin ya melakukan kegiatan *Phishing* diluar grub atau melakukan kegiatannya sendiri.	Mungkin dari pelaku ini kan memanfaatkan hal tersebut kepada korban.	Ada juga yang istilahnya dia itu permasalahan, seperti misal mba nya mau melakukan transaksi di ATM, mungkin transaksi itu ada *trouble* atau gangguan yang mungkin mba sudah transfer tapi tidak sampai ke rekening yang dituju. Mungkin karena error. pihak bank di *hack* dan pelanggan itu masih belom	Saya bantu mba coba nanti mengirim nomer ATM nya, rekening atau PINnya berapa atau bahkan datadata lain yang pelaku butuhkan. Nanti otomatis kan korban panik, itu pasti dikasihkan tanpa berpikir panjang. Padahal kalau kode rahasia itu bersifat privasi dan tidak boleh dikasih tahu siapapun. Yang tahukan hanya bersangkutan saja. Begitupun sebaliknya kayak kode OTP/PASSWORD itu verifikasi hanya untuk pemegang itu sendiri. Kalau sudah beralih ke orang lain pasti sudah otomatis akun kita dipegang orang lain. mungkin kerugian mungkin istilahnya anda alami itu mungkin akan diganti cuma kalo misalnya njenengan sendiri yang melakukan human error atau kesalahan memberikan PIN atau OTP		

2 : Muhammad Robani. 18-12-2023						itu data yaa, mungkin maksud kamu modus yang sering digunakan *Phishing*	modus yang sering digunakan *Phishing* itu sering kali mengatas namakan apa gitu. Kalau kebanyakan pasti *merchant*, terkait belanja *online* biasanya,
3 : Riski Praditya Putra. 11-01-2024		jadi modelnya itu tetep perorangan, mengoperasikan itu tetep perorangan. Kita masih menyelidikinya, jaringannya kerjasama sama siapa. Koordinasi mereka pasti satu wilayah. Dan itu biasanya daerah Sumatra sana					
4 : Riski Praditya Putra. 18-12-2023							

H : 2). Meminta untuk mengisi Formulir Digital	I : 3). Menggunakan *Email* untuk Mengambil Data	J : c. Karakteristik	K : 1). Sebagai Entitas Terpercaya	L : 2. *Target* (korban)	M : a. Kurang Pemahaman	N : b. Mudah Percaya
		apakah ada pola tersendiri yang digunakan oleh pelaku	Padahal seharusnya itu dilakukan oleh pihak bank secara resmi .		Kalau sudah beralih ke orang lain pasti sudah otomatis akun kita dipegang orang lain. Kadang orang itu kurang pemahamannya disitu.	kalau mengelabui korbannya yang pertama itu mungkin dengan bahasa *Phishing* itu kayak bujuk rayu, jadi mereka itu menawarkan kemudahan. Karena korban mungkin sedang tidak konsentrasi atau mungkin korban itu mendapatkan informasi tidak di klarifikasi dulu, jadi langsung percaya .

Meminta korban untuk mendaftarkan akun instragam atau bahkan media sosialnya sebagai syarat penggunaan layanan merchant. Contoh, misal di instragam saya mau menggunakan layanan centang biru, saya harus masukan akun instragam saya karena pelaku mengirimkan formulir digital.	Atau dengan cara baru, biasanya pelaku ini akan mengambil alih akun *email* kita setelah itu pelaku akan merubah sandi, akun pemulihan, nomer pemulihan akan dirubah semua dan akhirnya akan digunakan oleh pelaku untuk menggunakan beberapa media sosial kita yang menggunakan *email* sebagai data awal	karakteristik	Tren *Phishing* dengan mengatasnamakan (suatu merchant, person, *platform* digital) sebuah instansi dengan maksud mencari kelengahan korban yang membutuhkan/menggunakan layanannya		kesadaran perlu ditingkatkan, karena masyarakat DIY cenderung belum memahami karakteristik dan fungsi medsos yang digunakan sehingga ada ketidakpahaman tersebut seringkali digunakan sebagai celah oleh para pelaku tindak pidana. Terkendala, masyarakat masih pasif. Karena mereka sendiri tidak peduli dan hanya media untuk komunikasi.	

Lampiran 8 *Framework* Matrices Mekanisme Pengungkapan Kasus *Phishing* POLDA DIY

	A : Mekanisme Pengungkapan Kasus *Phishing*	B : A. Pengaduan	C : 1. SPKT (Sentra Pelayanan Kepolisian Terpadu)	D : 2. Subdit V Siber	E : B. Penyelidikan	F : 1. Surat Perintah	G : 2. Memeriksa Saksi	H : 3. Menganalisis Bahan Keterangan	I : 4. Laporan Hasil Penyelidikan	J : 5. Layak Tidaknya ke Penyidikan
1 : Cahyono Budi. 04-12-2023										
2 : Muhammad Robani. 18-12-2023			Prosedur awal korban menyampaikan keluhan dalam bentuk laporan maupun aduan dengan beberapa cara. Satu melalui SPKT polda DIY dan diarahkan ke ditreskrimsus. Dokumen atau alat bukti harus disertakan oleh korban ketika membuat laporan kasus *Phishing*. Apa dokumennya							Untuk tindak lanjut penanganan (menghentikan penyelidikan atau melanjutkan ke tahap penyidikan)

	A : Mekanisme Pengungkapan Kasus *Phishing*	B : A. Pengaduan	C : 1. SPKT (Sentra Pelayanan Kepolisian Terpadu)	D : 2. Subdit V Siber	E : B. Penyelidikan	F : 1. Surat Perintah	G : 2. Memeriksa Saksi	H : 3. Menganalisis Bahan Keterangan	I : 4. Laporan Hasil Penyelidikan	J : 5. Layak Tidaknya ke Penyidikan
			yaitu semua dokumen atau alat bukti yang berhubungan dengan dugaan tindak pidana yang dilakukan oleh pelaku, yang bisa menjadi petunjuk (*screenshot* percakapan,*website* yang digunakan oleh pelaku maupun akun dari pelaku, dll)							
3 : Riski Praditya Putra. 18-12-2023	Mekanisme pengungkapan kasus *Phishing*	Berarti dari awal itu kan korban merasakan bahwa mendapatkan tindak pidana, setelah itu korban melakukan	setelah itu, pada korban membuat laporan awal ke SPKT depan. memberikan surat rekomendasi gelar awal. disini pihak kepolisian akan memberikan tanggapan atau masukan terhadap	setelah itu korban akan konsultasi dengan pihak siber tentang kasusnya, kalau memenuhi unsur pidana ITE lalu diarahkan ke	yang kedua adalah naik ke tahap penyelidikan, disini kami mencari bukti adanya tindak pidana	yang pertama kami lakukan itu menyusun surat perintah tugas, surat perintah penyelidikan dan	Lalu setelah kami membuat surat tersebut kami melakukan pemeriksaan kepasa saksi, disini kami meminta	seperti nomor telfon, dompet digital, rekening, *link* yang menjadi alat bukti korban pada saat terjadinya kasus *Phishing*. jika kita	Laporan hasil penyelidikan ini adalah temuan-temuan yang dilakukan penyidik. mulai dari informasi korban, waktunya,	Disitu para penyidik dapat menentukan, sebenarnya kasus ini bisa masuk ke tahap penyidikan tidak. nanti pelapor biasanya

	A : Mekanisme Pengungkapan Kasus *Phishing*	B : A. Pengaduan	C : 1. SPKT (Sentra Pelayanan Kepolisian Terpadu)	D : 2. Subdit V Siber	E : B. Penyelidikan	F : 1. Surat Perintah	G : 2. Memeriksa Saksi	H : 3. Menganalisis Bahan Keterangan	I : 4. Laporan Hasil Penyelidikan	J : 5. Layak Tidaknya ke Penyidikan
		pengaduan di kepolisian.	kasus korban, jika terjadi tindak pidana korban harus seperti apa.	Krimsus (Kriminal Khusus) yang menangani dari Direktorat Reserse Kriminal Khusus unit Siber. Setelah itu, korban nanti menceritakan kronologinya seperti apa terus kapan,dimana pokoknya semua itu diceritakan nanti yang piket ini biasanya kalau tindak pidana itu memenuhi		membuat SP2HP A1 yang dilakukan oleh penyidik	keterangan tentang kejadian yang dialami korban dan memeriksa, ada tindakan pindana yang dilakukan.	menemukan adanya tindak pidana yang diterima oleh korban kami akan membuat laporan hasil penyelidikan.	lokasinya kapan dan pelakunya. Disitu para penyidik dapat menentukan, sebenarnya kasus ini bisa masuk ke tahap penyidikan tidak	komunikasi dengan penyidik untuk menanyakan perkembangan perkaranya gimana

	A : Mekanisme Pengungkapan Kasus *Phishing*	B : A. Pengaduan	C : 1. SPKT (Sentra Pelayanan Kepolisian Terpadu)	D : 2. Subdit V Siber	E : B. Penyelidikan	F : 1. Surat Perintah	G : 2. Memeriksa Saksi	H : 3. Menganalisis Bahan Keterangan	I : 4. Laporan Hasil Penyelidikan	J : 5. Layak Tidaknya ke Penyidikan
				unsur itu langsung dibuatkan surat laporan. Jadi, mengisi kertas pink, kertas pengaduan nanti itu kronologi disitu diisi seperti hari, tanggal, unsur pidananya apa setelah itu nanti kembali lagi ke SPKT untuk dibuatkan Surat Pengaduan.						
4 : Riski Praditya Putra. 11-01-2024										

K : C. Penyidikan	L : 1. Surat Perintah	M : 2. Memeriksa Saksi dan Identifikasi Pelaku	N : a. Analisa Pro*file*	O : b. Melacak Pelaku	P : 3. Penangkapan	Q : 4. Penahanan	R : 5. Penggeledahan dan Penyitaan	S : 6. Berkasan Hasil Diperiksa	T : 7. Berkas Diajukan ke JPU	U : 8. Menyerahkan Tersangka dan Barang Bukti ke JPU
bisa ditingkatkan ke penyidikan		Penyidikan dilakukan untuk kumpulkan bukti lebih lanjut, menentukan tersangka, dan mencari kejelasan terhadap peristiwa	Penyidikan dilakukan untuk mengumpulkan bukti lebih lanjut, menentukan tersangka, dan mencari kejelasan terhadap peristiwa dengan cara melakukan analisa profil							Setelah selesai, hasil penyidikan bersama barang bukti atau tersangka diserahkan ke JPU (Jaksa Penuntut Umum). Peran jaksa adalah menuntut di persidangan. Dengan demikian, tugas polisi melibatkan menerima

										laporan, melakukan penyelidikan, dan selesai sampai pada tahap penyidikan, sedangkan tugas jaksa dimulai dari situ untuk menuntut di pengadilan.
setelah dari penyelidikan naik ke penyidikan, penyidikan ini kita melakukan investigasi lebih mendalam untuk mengungkap fakta yang didapatkan	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	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	pada saat memeriksa saksi-saksi kami juga melakukan analisa pro*file* untuk melihat latar belakang pelaku ini, seperti apa dia di kehidupan sehari-hari.	setelah kami dapatkan latar belakang, kami melacak pelaku tersebut, posisi terakhirnya dimana, pelaku sedang melakukan apa dan nanti kita akan koordinasi.	setelah itu kami akan melakukan gelar perkara pelaku untuk mengetahui apakah itu benar-benar pelaku. dengan mengumpulkan bukti-bukti yang mengarahkan kepada pelaku. kalau sudah mengetahui pelakunya siapa, kalau di penyidikan itu bisa upaya paksa untuk penangkapan itu bisa. Kalau	Setelah pelaku tertangkap nanti kita masukan sel (penahanan), kami melakukan penahanan berdasar bukti dan surat ya mba. jadi tidak asal menahan orang seperti ada etikanya.	Kami juga melakukan penggeledahan dan penyitaan barang bukti pelaku. penggeledahannya terhadap barang ya mba, alat buktinya itu semisal seperti telfon, buku tabungan yang biasanya digunakan pelaku untuk melakukan kejahatan tersebut.	Membuat berkas seperti itu mba, berkasnya warna merah. yang isinya seperti berita acara analisa penyelidik	Jadi setelah berkasnya jadi kita geser 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	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

		pengakuan bahwa telah terjadi tindak pidana yang terungkap dalam percakapan *online* surat tersebut			pelakunya ketangkap itu berdasarkan sprinkep, springledah itu ada , sprinkes, sprinlidik itu pasti wajib kita bawa sebagai dasar kami.	disamping itu kami juga akan mengolah berkasnya. Penahanan dilakukan 1x24 jam dan harus segera tetapkan apakah pelaku ditahan atau tidak			berisi tentang kurangnya apa, nanti ditulis di surat itu, dilampirkan mba. Kita nanti melengkapi itu, setelah itu kita melengkapinya ,	berkas perkara dan barang bukti.

Lampiran 9 *Framework* Matrices Kekurangan yang dihadapi Polda DIY terhadap Kasus *Phishing* di wilayah Daerah Istimewa Yogyakarta

	A : Kekurangan	B : 1. Pelaku Sulit Ditangkap	C : 2. Tidak Semua Pengaduan diproses	D : 3. Identifikasi Pelaku
1 : Cahyono Budi. 04-12-2023				
2 : Muhammad Robani. 18-12-2023				
3 : Riski Praditya Putra. 18-12-2023	kalau kekurangan itu karena ada beberapa hal yang tidak cukup mba, bisa jadi dari keterangan barang bukti dan lainnya	kurangnya bahan -bahan awal untuk melaporkan kasus itu juga kendala pelaku sekarang juga pinter ya mba, seiring berjalannya dan berkembangnya teknologi, itu juga kendala bagi kami. halangan atau rintangan itu pasti ada mba pada saat pelaksanaan. itu jadi pr buat kami saat melakukan tugas.	Tidak semua pengaduan di proses karena kita lihat apakah kasus ada unsur tindak pidananya. Kalau tidak bisa secara bukti nanti itu kita akan gelarkan seperti apa, mencari solusinya bagaimana, terus biasanya kita sampaikan ke pelapor kendalanya seperti apa kita sampaikan mba, karenakan mengungkap kasus tindak pidana penipun *online*, *illegal Acces* itu engga mudah juga.	pada saat kita mengidentifikasi pelaku juga makin sulit salah satunya dengan pelaku membuang nomernya itu, lalu kalau pakai *email*/media sosial itu pakai akun dari hasil beli, bukan akun yang asli. kita memproses kasus tersebut juga lumayan mba karena kita butuh informasi yang relevan.
4 : Riski Praditya Putra. 11-01-2024				

Lampiran 10 *Framework* Matrices Kendala yang dihadapi Polda DIY terhadap Kasus *Phishing* di wilayah Daerah Istimewa Yogyakarta

	A : Kendala	B : 1. Pelaporan Kurang Memadai	C : a. Kurangnya Bahan Keterangan	D : b. Kurangnya Alat Bukti	E : 2. Modus Pelaku	F : a. Rekening Simpanan	G : b. Dompet Digital Simpanan	H : 3. Sulitnya Akses ke Pihak Bank
1 : Cahyono Budi. 04-12-2023								ya, karena gini mba di Undang-undang perbankan itukan ada untuk data pribadi ataupun nomer rekening apa itu semua ada peraturan peraturannya meskipun kita itu ada tindak pidana kita kan harus berkomunikasi, kita harus bersurat mba. Engga serta merta meskipun dia itu sudah diduga sebagai pelaku kita untuk membuka rekening dan sebagainya itu kita harus jelas dasarnya harus legal dulu, resmi.
2 : Muhammad Robani. 18-								

	A : Kendala	B : 1. Pelaporan Kurang Memadai	C : a. Kurangnya Bahan Keterangan	D : b. Kurangnya Alat Bukti	E : 2. Modus Pelaku	F : a. Rekening Simpanan	G : b. Dompet Digital Simpanan	H : 3. Sulitnya Akses ke Pihak Bank
12-2023								
3 : Riski Praditya Putra. 18-12-2023	itu juga kendala bagi kami. halangan atau rintangan itu pasti ada mba pada saat pelaksanaan. itu jadi pr buat kami saat melakukan tugas.	kalau paling cepet itu tergantung buket,tergantung apa yang kita dapat dari pelapor misalkan buket awal itu nanti kita olah sampai menemukan pelaku. Jadi apa ya mba, penyidik itu kadang kesusahan ketika buket awalnnya itu minim gitu. Jadi semakin banyak buket yang diberikan oleh pelapor seperti misalnya: nomer telfonnya, ATM nya apa, terus transaksinya dimana, Instragamnnya apa, social medianya apa itu malah mempermudah penyidik untuk menganalisa mengolah	biasanya kekurangan dari pelapor sih mba, yang komunikasinya ke kami itu kurang. kurangnya bahan - bahan awal untuk melaporkan kasus itu juga kendala. Jadi ketika buket awalnya itu lengkap dapat membantu, tapi ketika buketnya dari awal itu sudah gak bisa dibuktikan oleh korban itu kami kesulitan juga mba.	Alat bukti juga diperlukan, karena dengan adanya barang bukti bisa mendapatkan keterangan saksi dan sebagai bahan pembuktian	pelaku sekarang juga pinter ya mba, seiring berjalannya dan berkembangnya teknologi, itu juga kendala bagi kami. halangan atau rintangan itu pasti ada mba pada saat pelaksanaan. itu jadi pr buat kami saat melakukan tugas.			kalau koordinasi itu pasti, soalnya kan memiliki ranah, Ranah itu juga di dunia perbankan juga, bank-bank itu juga punya ranah. Jadi kita gak asal langsung masuk ke lembaga gitu. Istilahnya kita permisilah. Koordinasi itu wajib.

	A : Kendala	B : 1. Pelaporan Kurang Memadai	C : a. Kurangnya Bahan Keterangan	D : b. Kurangnya Alat Bukti	E : 2. Modus Pelaku	F : a. Rekening Simpanan	G : b. Dompet Digital Simpanan	H : 3. Sulitnya Akses ke Pihak Bank
		data itu. biasanya kekurangan dari pelapor sih mba, yang komunikasinya ke kami itu kurang. kurangnya bahan - bahan awal untuk melaporkan kasus itu juga kendala.						
4 : Riski Praditya Putra. 11-01-2024						Jadi nomer rekening pelaku itu menggunakan rekening tampungan. Dan rekening tampungan itu di jual belikan dalam artian pelaku itu mencari rekening random namanya. Intinya pelaku ini beli ke orang, kebanyakan rekening ini dari Jawa Barat. Jadi pelaku ini beli dulu rekeningnya lalu rekening itu dibuat	Kalau tidak rekening tampungan ya dompet digital tampungan. Setelah dari situ, ada pelaku yang transfer lagu ke ATM tampungan lagi habis itu ke nomor rekeningnya sendiri.selain nomer rekening itu dompet digital mba, kadang juga mereka mainnya dari dana ke dana	

	A : Kendala	B : 1. Pelaporan Kurang Memadai	C : a. Kurangnya Bahan Keterangan	D : b. Kurangnya Alat Bukti	E : 2. Modus Pelaku	F : a. Rekening Simpanan	G : b. Dompet Digital Simpanan	H : 3. Sulitnya Akses ke Pihak Bank
						misalnya 5 rekening itu dibuat untuk uang tampungan dari modus *Phishing* tersebut.nah jadi setelah terjadi pengambil Alihan, misalnya dari dompet digital tadi itu diambil alih terus di transfer ke rekening tampungan		

Lampiran 11 *Framework* Matrices Perbaikan yang dilakukan Oleh Polda DIY terhadap Kasus *Phishing* di wilayah Daerah Istimewa Yogyakarta

	A : Perbaikan	B : 1. Sosialisai	C : a. Himbauan kepada Masyarakat	D : 2. Bekerjasama Dengan Pihak Bank	E : 3. Bekerjasama Dengan Media Sosial dan Kominfo	F : 4. Pengembangan Mekanisme dan Alat untuk pelaku
1 : Cahyono Budi. 04-12-2023			kalo dari pihak polisi kan mungkin ada tindak pidana atau mungkin di duga tindak pidana nah disitulah tanggung jawab kita nah kita mungkin juga ada himbauan			
2 : Muhammad Robani. 18-12-2023			kalau polda DIY sendiri sudah membuat himbauan. Himbauan itu pasti ada media-media sosialnya Polda DIY terutama terus setiap ada rilis dengan penanganan kasus kita pasti akan membuat himbauan juga secara langsung melalui konferensi pers.			
3 : Riski Praditya Putra. 18-12-2023	Untuk langkah-langkah perbaikan.	Kita juga melakukan kerjasama dengan beberapa lembaga masyrakat. osialisasi dengan menghimbau masyarakat untuk lebih hati-hati, biasanya				langkah-langkah perbaikan itu sebenarnya dari penyidik, untuk mengungkap kasus memang butuh waktu. dari melakukan analisa awal itu pasti sama. dari sdm kami sendiri dalam proses penyelidikan, Soalnya kan harus ada buket awal

	A : Perbaikan	B : 1. Sosialisai	C : a. Himbauan kepada Masyarakat	D : 2. Bekerjasama Dengan Pihak Bank	E : 3. Bekerjasama Dengan Media Sosial dan Kominfo	F : 4. Pengembangan Mekanisme dan Alat untuk pelaku
		kami akan menggelar konferensi pers.				dulu. buket awal yang lengkap menjadi kunci untuk memahami kasus, namun jika tidak dapat dibuktikan oleh korban bbisa menyebabkan kendala. oleh karena itu mba, fokusnya diberikan pengembangan keterampilan penyidik dalam mengumpulkan bukti yang kuat. itu langkah-langkah perbaikannya.
4 : Riski Praditya Putra. 11-01-2024			sosialisasi dengan masyarakat itu juga pasti. tujuannya agar masyarakat mempunyai pemahaman dan kesadaran tentang bahayanya kasus tersebut. tindakan apa yang dilakukan masyarakat jika kasus seperti itu terjadi.	bekerjasama dengan lembaga bank, media sosial atau kominfo. untuk bank sendiri kita kerjasama untuk mengatur kerangka kerjanya seperti apa atau etiknya seperti apa dan tata caranyanya bagaimana terkait dengan pertukaran informasi biar makin efektif.	untuk mendeteksi, mencegah kasus yang sama terjadi lagi, kerja sama yang dilakukan dengan media sosial/kominfo ini agar melindungi masyarakat dari upaya penipuan *online* dan ancaman keamanan siber.	

Lampiran 12 Pedoman Wawancara Tidak Terstruktur (Polda DIY)

PEDOMAN WAWANCARA TIDAK TERSTRUKTUR (POLDA DIY)

NAMA :

Jabatan/Posisi :

Rumusan Masalah 1 : Bagaimana tren permasalahan *Phishing* di wilayah daerah istimewa yogyakarta?

1. Bagaimana tren kasus *Phishing* di Yogyakarta selama tahun 2023?
2. Apa saja sebaran jenis serangan *Phishing* yang paling umum terjadi di Yogyakarta pada kuartal pertama tahun ini?
3. Berapakah persentase kenaikan jumlah serangan *Phishing* di Yogyakarta dibandingkan dengan periode sebelumnya?
4. *Platform online* apa yang paling sering menjadi *target* serangan *Phishing* di Yogyakarta?
5. Bagaimana tingkat keberhasilan penanganan kasus *Phishing* oleh pihak berwenang di Yogyakarta?
6. Apakah terdapat pola atau karakteristik khusus dari serangan *Phishing* yang terjadi di wilayah ini?
7. Bagaimana respons masyarakat terhadap serangan *Phishing* di Yogyakarta, terutama terkait dengan tingkat kesadaran dan pencegahan?
8. Adakah peningkatan kasus *Phishing* yang terkait dengan sektor bisnis tertentu di Yogyakarta?
9. Bagaimana cara para pelaku *Phishing* memanfaatkan faktor-faktor sosial atau budaya khusus di Yogyakarta untuk mencapai tujuan mereka?
10. Apa langkah-langkah yang telah diambil oleh pemerintah setempat untuk meningkatkan kesadaran dan perlindungan terhadap serangan *Phishing* di Yogyakarta?

Rumusan Masalah II : Bagaimana mekanisme pengungkapan Polda DIY terhadap kasus *Phishing* di wilayah Daerah Istimewa Yogyakarta?

1. Bagaimana prosedur awal ketika seorang korban melaporkan kasus *Phishing* kepada Polda?
2. Apa dokumen atau bukti yang harus disertakan oleh korban ketika membuat laporan kasus *Phishing*?
3. Apakah ada biaya yang harus ditanggung oleh korban saat mengajukan laporan atau melibatkan Polda dalam menangani kasus *Phishing*?
4. Apa saja biaya operasional yang harus dikeluarkan oleh Polda DIY dalam menyelesaikan kasus *Phishing* yang melibatkan korban?
5. Berapa estimasi waktu yang dibutuhkan oleh Polda DIY untuk menyelesaikan satu kasus *Phishing*?
6. Apa jenis pertanyaan yang diajukan oleh Polda DIY kepada korban kasus *Phishing* selama proses penanganan?
7. Bagaimana langkah-langkah awal yang diambil oleh Polda DIY setelah menerima laporan dari korban kasus *Phishing*?
8. Bagaimana Polda DIY melakukan penyelidikan dan mengumpulkan informasi terkait pelaku dalam kasus *Phishing*?
9. Apa bukti atau laporan yang perlu dikumpulkan oleh Polda DIY untuk mendukung pengambilan keputusan dalam mengungkap kasus *Phishing*?
10. Apa jenis pertanyaan yang diajukan oleh Polda DIY kepada pelaku *Phishing* ketika sudah ditangkap?
11. Setelah tahap penyelidikan selesai, bagaimana Polda DIY berkomunikasi dengan korban dan pelaku mengenai hasil investigasi?
12. Apa sanksi atau peraturan yang dapat dikenakan kepada pelaku kasus *Phishing* setelah berhasil diungkap oleh Polda DIY?
13. Bagaimana proses koordinasi antara Polda DIY dengan pihak lain, seperti lembaga keuangan atau instansi terkait, dalam menangani kasus *Phishing*?
14. Apakah Polda DIY memberikan informasi atau edukasi kepada korban mengenai langkah-langkah pencegahan setelah menyelesaikan kasus?
15. Bagaimana Polda DIY mendukung korban dalam pemulihan dan pencegahan agar tidak menjadi korban *Phishing* lagi di masa mendatang?

Rumusan Masalah III : Apa kendala yang dihadapi oleh Polda DIY dalam pengungkapan kasus *Phishing* di wilayah Daerah Istimewa Yogyakarta?

1. Apa hambatan utama yang dihadapi oleh korban ketika menyiapkan laporan dan bukti terkait kasus *Phishing*?
2. Apa kendala yang sering dihadapi oleh Polda DIY dalam mencari informasi mengenai keberadaan pelaku kasus *Phishing*?
3. Bagaimana pembiayaan menjadi kendala dalam penyelesaian kasus *Phishing* yang melibatkan Polda DIY?
4. Apa tantangan terbesar yang dihadapi oleh Polda DIY dalam mengumpulkan bukti-bukti terkait kasus *Phishing*?
5. Apa faktor-faktor yang sering menjadi hambatan dalam pengumuman keputusan Polda DIY kepada korban dan pelaku pada tahap terakhir penyelesaian kasus *Phishing*?
6. Bagaimana koordinasi antara Polda DIY dan lembaga atau instansi terkait bisa menjadi kendala dalam mengungkapkan kasus *Phishing*?

Rumusan Masalah IV : Perbaikan apa yang dapat dilakukan Polda DIY dalam pengungkapan kasus *Phishing* di wilayah Daerah Istimewa Yogyakarta?

1. Apa langkah-langkah perbaikan yang dilakukan Polda DIY untuk meningkatkan efektivitas dalam merumuskan strategi mengungkap kasus *Phishing*?
2. Bagaimana Polda DIY memperbaiki komunikasi dan edukasi kepada korban serta masyarakat secara umum guna mencegah terjadinya kasus *Phishing*?
3. Apa inisiatif perbaikan yang diambil oleh Polda DIY dalam meningkatkan kerja sama dengan lembaga atau instansi terkait untuk lebih efisien mengungkap kasus *Phishing*?

Mekanisme pengungkapan Polda DIY terhadap kasus *Phishing* di wilayah DIY?

1. data laporan yang masuk dan laporan yg selesai.
2. Data tentang jumlah yg melaporkan.
3. Surat izin penelitian
4. Berkas Surat perintah penyidikan, dll