JURNAL SISTEM INFORMASI GALUH ISSN 2964-7746
Volume 3, Nomor 1, Januari 2025 https://ojs.unigal.ac.id/index.php/jsig/index
(Fayza Hafiz Rahmadani)

Cybercrime: Analisis Dan Mitigasi Resiko Penipuan Tilang Online Melalui Aplikasi *WhatsApp* (WA)

Fayza Hafiz Rahmadani[*1], Hendrian Cahya Sutany[2], Mohamad Ragil Aditya[3], Muhammad Adita Fajar[4], Yesika Ulan Dari[5], Fauziyah[6]
[*1,2,3,4,5,6]Universitas Bung Karno
E-mail: [*1]fayzarahmadani@gmail.com, [2]hendriancahyasutany@gmail.com, [3]mohamadaditya479@gmail.com, [4]muhammadaditafajar@gmail.com, [5]yesikaaud@gmail.com, [6]fauziyah@ubk.ac.id

Abstract

Online ticket fraud via WhatsApp is a crime that is troubling and detrimental to society. Online ticket scams that have been rampant lately have become an increasingly serious threat in today's digital era and have caused losses to victims, one of which is financial loss due to online ticket scams. Therefore, prevention and mitigation efforts are very important to protect the public from this fraud mode. The importance of increasing public education and literacy about online fraud, increasing cyber patrols and law enforcement against online fraud perpetrators can be a solution to prevent online ticket fraud via WhatsApp. This research was conducted to increase public awareness about information security by conducting continuous analysis and education, it is hoped that online fraud can be minimized and the public can avoid losses, understand the mode of online ticket fraud via WhatsApp, and develop effective prevention strategies for online ticket fraud that is rampant. The National Cyber and Crypto Agency related to cybercrime, public complaints as many as 1,216 in 2023, it can be concluded that in Indonesia cybercrime or online fraud often occurs among the public.

Keywords : *Online Fraud, Online Traffic Fines, WhatsApp, Cybercrime, Analysis.*

Abstrak

Penipuan tilang online melalui *WhatsApp* merupakan kejahatan yang meresahkan dan merugikan masyarakat. Penipuan tilang online yang marak terjadi akhir - akhir ini menjadi ancaman yang semakin serius di era digital pada saat ini dan menimbulkan kerugian bagi korban salah satunya adalah kerugian finansial karena terjerat penipuan tilang online. Oleh karena itu, upaya pencegahan dan mitigasi menjadi sangat penting untuk melindungi masyarakat dari modus penipuan ini. Pentingnya meningkatkan edukasi dan literasi masyarakat tentang penipuan *online*, meningkatkan patroli *cyber* dan penegakan hukum terhadap pelaku penipuan *online* dapat menjadi solusi untuk mencegah terjadinya penipuan tilang *online* via *WhatsApp*. Penelitian ini dilakukan untuk meningkatkan kesadaran masyarakat tentang keamanan informasi dengan melakukan analisis dan edukasi yang berkelanjutan, diharapkan penipuan online dapat diminimalisir dan masyarakat dapat terhindar dari kerugian, memahami modus penipuan tilang online melalui WhatsApp, dan mengembangkan strategi pencegahan yang efektif penipuan tilang online yang marak terjadi. Badan Siber dan Sandi Nasional yang terkait dengan *cybercrime*, aduan masyarakat sebanyak 1.216 tahun 2023, ini dapat disimpulkan bahwa di Indonesia sering sekali terjadi *cybercrime* atau penipuan online dikalangan masyarakat.

Kata Kunci : *Penipuan Online, Tilang Online, WhatsApp, Kejahatan Siber, Analisis.*

I. PENDAHULUAN

Kemajuan teknologi informasi telah memberikan banyak manfaat bagi kehidupan masyarakat Indonesia, namun di sisi lain juga memunculkan tantangan baru bentuk berupa kejahatan siber atau *cybercrime* [1]. Menurut Badan Siber dan Sandi Negara (BSSN) pada Laporan Tahun 2023, tecatat sebanyak 403 Juta [2].

Penggunaan media sosial sebagai sarana kejahatan telah menjadi fenomena yang semakin sering terjadi di

Indonesia. Para pelaku kejahatan memanfaatkan media sosial untuk meraih keuntungan pribadi dan sering kali dengan janji keuntungan besar yang membuat korban tergiur tanpa mempertimbangkan risiko yang ada. Ketidakhadiran perjanjian formal sebelumnya membuat korban sulit menuntut pertanggungjawaban pidana terhadap pelaku [3].

Seiring terjadinya penipuan daring melalui aplikasi *WhatsApp* dari penipuan transfer pulsa, aplikasi, dan undangan pernikahan. Hingga saat ini berkembang menjadi penipuan tilang online. Penipuan tilang online via *WhatsApp* ini melibatkan penggunaan teknologi untuk memanfaatkan keahlian dan keterampilan manusia dengan tujuan memperoleh keuntungan secara tidak sah [4].

Seiring dengan semakin luasnya penggunaan media sosial dan aplikasi pesan instan para pelaku kejahatan *cyber* semakin memanfaatkan celah-celah yang ada. Pelaku kejahatan melakukan penipuan melalui pesan teks atau aplikasi seperti *WhatsApp*, dengan skema seperti mengirimkan undangan berbentuk aplikasi atau pemberitahuan yang meminta pembayaran online. Selain itu kejahatan lain di dunia maya juga terjadi, seperti mengirimkan tautan melalui pesan langsung di *platform* media sosial yang dapat digunakan oleh pelaku untuk mengambil alih akun korban. Jenis kejahatan ini sering melibatkan teknik rekayasa sosial (*social engineering*) untuk menipu korban [5].

Sistem tilang *online* merupakan salah satu inovasi dalam penegakan hukum lalu lintas dengan memanfaatkan teknologi informasi. Digitalisasi ini diharapkan dapat membawa inovasi dalam manajemen penindakan oleh pihak kepolisian serta pembayaran denda pelanggaran lalu lintas. Tujuan pihak kepolisian membuat tilang online itu untuk mempermudah masyarakat jiak melakukan pelanggaran lalu lintas. Namun dalam praktiknya tilang online telah menjadi permasalahan baru di Indonesia, yaitu merupakan penipuan tilang *online*. Penipuan tilang online hingga saat ini adalah masalah yang jarang diteliti secara mendalam [6].

Permasalahan yang diuraikan pada penelitian ini ialah bagaimana pelaku kejahatan memanfaatkan celah – celah dalam teknologi dan media sosial untuk melakukan penipuan tilang *online*, sehingga tujuan dari penelitian ini adalah mengidentifikasi dan menganalisis sistem informasi yang terlibat dalam terjadinya penipuan tilang *online* melalui *WhatsApp* di Indonesia dan memberikan solusi dalam bentuk jurnal penelitian sebagai media informasi dan edukasi mengenai penipuan tilang online via *WhatsApp*. serta bagaimana upaya pencegahan dan penanggulangan yang

ISSN 2964-7746
https://ojs.unigal.ac.id/index.php/jsig/index

dapat dilakukan untuk mengatasi permasalahan ini.

1.1 Penelitian Relevan

Penelitian-penelitian terdahulu menjadi salah satu bahan acuan bagi peneliti ketika melakukan penelitian, sehingga peneliti dapat memperkaya teorinya dengan mempelajari penelitian-penelitian yang telah dilakukan. Berikut merupakan berupa jurnal terkait dengan penelitian yang dilakukan peneliti.

Penelitian yang dilakukan oleh Mulyadi, dkk tentang penipuan yang sebelumnya dilakukan secara konvensional kini berkembang dan dapat dilakukan melalui teknologi atau yang biasa disebut sebagai penipuan daring atau online. Penelitian ini menggunakan metode yuridis normatif. Hasil penelitian menunjukkan bahwa terdapat banyak bentuk konkret penipuan *online* yang terjadi melalui berbagai platform media sosial dan media belanja *online*, seperti *phishing, scamming*, dan rekayasa sosial. Untuk mencegah penipuan *online* diperlukan peningkatan dan perbaikan profesionalisme serta integritas aparatur penegak hukum dalam menangani kasus-kasus penipuan online yang sering terjadi di masyarakat. Langkah ini diambil untuk memastikan adanya kepastian hukum dan memberikan jaminan perlindungan bagi masyarakat [7].

Dhery, dkk melakukan penelitian mengenai penipuan melalui *smartphone* dengan menggunakan rekayasa sosial telah menjadi ancaman yang semakin serius di era digital saat ini. Penelitian ini bertujuan untuk mengeksplorasi upaya manajemen risiko yang dapat diterapkan untuk mengatasi penipuan melalui *smartphone* yang menggunakan teknik rekayasa sosial. Metode penelitian yang digunakan melibatkan analisis literatur dari berbagai sumber, seperti jurnal ilmiah, artikel, dan laporan penelitian terkait. Hasil penelitian menunjukkan bahwa manajemen risiko yang efektif melibatkan gabungan strategi teknis dan non-teknis. Strategi teknis termasuk penerapan sistem keamanan yang canggih, deteksi intrusi, dan enkripsi data, sedangkan strategi non-teknis mencakup pelatihan kesadaran keamanan bagi pengguna smartphone serta penerapan kebijakan keamanan yang ketat [8].

Penelitian yang sudah dibuat oleh Habib, dkk mengenai Perkembangan teknologi telah mengubah banyak aspek kehidupan manusia. Penggunaan internet dilakukan untuk berbagai keperluan, seperti mengakses layanan publik, media sosial, hiburan, komunikasi, permainan, berita, belanja *online*, layanan perbankan, pekerjaan, mencari informasi tentang barang serta jasa, dan lain-lain.

ISSN 2964-7746
https://ojs.unigal.ac.id/index.php/jsig/index

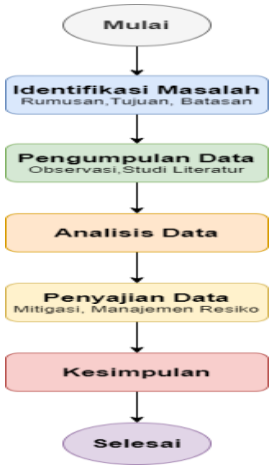
Berdasarka evaluasi sosialisasi dari hasil pengabdian yang dilakukan, dapat disimpulkan bahwa masih ada banyak anggota masyarakat yang kurang memahami tanda-tanda dari pelaku kejahatan *cyber*, sementara sejumlah warga telah mengalami kerugian finansial karena terjerat dalam tipu daya bisnis yang menawarkan keuntungan palsu. Penelitian ini menggunakan metode pelaksanaan saat melakukan kegiatan pengabdian masyarakat dengan observasi dan wawancara. Dengan betujuan bahwa masyarakat tau mengenai kejahatan *cyber* [9].

Dari beberapa sumber yang telah diuraikan, terlihat bahwa belum ada penelitian yang secara khusus meneliti tentang isu tilang online via *WhatsApp* di kalangan masyarakat Indonesia. Oleh karena itu, penelitian ini menjadi unik karena fokus pada analisis sistem informasi terkait terjadinya penipuan tilang online via *WhatsApp* serta pengembangan solusi sebagai media informasi dan edukasi bagi masyarakat untuk mengatasi permasalahan tersebut [10].

II. METODE PENELITIAN

2.1 Tahapan Penelitian

Tahapan Metode pada penelitian ini diantaranya dapat dilihat pada Gambar 1 berikut.



Gambar 1. Tahapan Penelitian Analisis Sistem Informasi Terjadinya Penipuan Tilang Online Melalui *WhatsApp*

2.2 Identifikasi Masalah

1. Rumusan
   a. Bagaimana modus operandi penipuan tilang online melalui *WhatsApp*?
   b. Apa saja faktor-faktor yang mempengaruhi kerentanan masyarakat terhadap penipuan tilang online?
   c. Bagaimana peran sistem informasi dalam memfasilitasi atau mencegah penipuan tilang online melalui *WhatsApp*?
2. Tujuan
   a. Mengidentifikasi dan menganalisis pola-pola penipuan tilang online yang terjadi melalui *WhatsApp*.
   b. Mengevaluasi faktor-faktor yang berkontribusi terhadap keberhasilan penipuan tilang online.

c. Mengkaji peran sistem informasi dalam konteks penipuan tilang online dan merumuskan rekomendasi untuk meningkatkan keamanan sistem.

3. Batasan
   a. Penelitian fokus pada kasus penipuan tilang online yang terjadi melalui aplikasi *WhatsApp*.
   b. Periode analisis dibatasi dari tahun 2019 hingga 2024.

2.3 Pengumpulan Data

Teknik yang digunakan untuk mengumpulkan data dalam penelitian ini dengan metode kuantitatif. Teknik pengumpulan data ini dimulai dari keresahan tim peneliti atas terjadinya penipuan tilang online, selanjutnya tim peneliti melakukan pemetaan data yang didapat dari media sosial dan laporan BSSN tahun 2023. Dilanjutkan dengan tahap melakukan observasi dan studi literatur untuk mendapatkan hasil.

1. Observasi

   Observasi adalah teknik pengumpulan data di mana peneliti mengamati dan mencatat fenomena yang sedang diteliti. Observasi merupakan kegiatan ilmiah yang bersifat empiris, faktual, dan didasarkan pada kenyataan. Peneliti juga dapat memperoleh wawasan dari sebuah platform yang bernama tiktok, dengan video – video yang sesuai dengan subjek penelitian yaitu penipuan tilang online via *WhatsApp* [11].

2. Studi Literatur

   Studi literatur adalah rangkuman tertulis dari berbagai artikel jurnal, buku, dan dokumen lainnya yang menjelaskan informasi sebelumnya mengenai penelitian dan topiknya. Tahapan studi literatur tersebut dilakukan untuk mengetahui penelitian terlebih dahulu mengenai penipuan tilang online via *WhatsApp* serta dampak dari file aplikasi yang dikirimkan oleh pelaku tindak kejahatan melalui pesan percakapan *WhatsApp* terhadap perangkat korban [12].

2.4 Analisis Data

Analisis data adalah proses pengolahan data untuk membuatnya lebih mudah dibaca dan diinterpretasikan [13]. maka analisis data adalah upaya untuk mengumpulkan data secara akurat yang dilakukan melalui observasi dan studi literatur untuk menemukan hasil dari permasalahan yang diteliti. Sedangkan teknik analisis data kuantitatif yaitu data dalam bentuk jumlah yang digunakan untuk memberikan penjelasan tentang kejelasan angka-angka atau untuk membandingkan beberapa gambaran untuk mendapatkan gambaran baru. Setelah itu, data diberikan kembali dalam bentuk kalimat atau penjelasan [13]. Tim peneliti memberikan

ISSN 2964-7746
https://ojs.unigal.ac.id/index.php/jsig/index

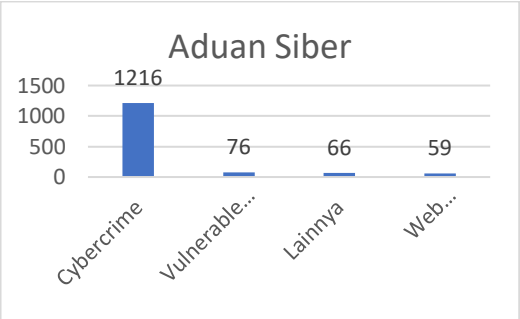
penjelasan menyeluruh tentang proses analisis data. Pada umumnya, deskripsi tentang teknik penghitungan statistik dan software yang digunakan juga ditampilkan pada bagian hasil dan pembahasan [14].

2.5 Penyajian Data

Penyajian data adalah proses mengorganisir data dengan menghubungkan satu kelompok data dengan kelompok data lainnya. Dengan menampilkan data, akan lebih mudah untuk memahami situasi yang ada dan merencanakan langkah berikutnya berdasarkan pemahaman tersebut. Penyajian data spesifik dipaparkan melalui hasil dan pembahasan [15].

III. HASIL DAN PEMBAHASAN

Diketahui bahwa di Indonesia banyak sekali penipuan online atau *cybercrime*. Pada tahun 2023 menurut Badan Siber dan Sandi Nasional yang terkait dengan *cybercrime*, aduan masyarakat sebanyak 1.216 yang dapat dilihat dari grafik pada gambar 2 berikut ini.



Gambar 2. Kategori Aduan Siber

(Sumber: Lanskap Kemanan Siber Indonesia pada Tahun 2023)

Dari gambar diatas dapat mengetahui bahwa pada tahun 2023 banyak sekali terjadi aduan *cybercrime* yang diterima oleh Badan Siber dan Sandi Nasional, ini dapat disimpulkan bahwa di Indonesia sering sekali terjadi *cybercrime* atau penipuan online dikalangan masyarakat. Perlunya mengetahui bahwa penipu tersebut memiliki beberapa cara untuk melakukan modus penipuan online terutama terkait tilang online. Maka dengan ini kami menganalisis teknik yang digunakan oleh pelaku penipuan sebagai berikut:

3.1 Teknik Penipuan Tilang Online melalui *WhatsApp*

3.1.1 Analisis teknik yang digunakan oleh pelaku penipuan.

a. Phishing

Phishing adalah teknik penipuan yang paling umum digunakan dalam kasus tilang online. Pelaku penipuan mengirimkan pesan *WhatsApp* yang tampak resmi dari instansi penegak hukum, seperti kepolisian atau dinas perhubungan, dengan tujuan untuk menipu korban agar memberikan informasi pribadi atau melakukan pembayaran, serta hal yang biasanya pelaku lakukan saat melakukan penipuan:

a) Pesan Palsu: Pelaku mengirimkan pesan yang berisi informasi bahwa korban telah melakukan pelanggaran

ISSN 2964-7746
https://ojs.unigal.ac.id/index.php/jsig/index

lalu lintas dan harus membayar denda.

b) Lampiran Berbahaya: Pesan seringkali menyertakan tautan atau lampiran yang mengarahkan korban ke situs web palsu yang mirip dengan situs resmi. Korban diminta untuk memasukkan informasi pribadi atau detail kartu kredit di situs palsu tersebut.

c) Tekanan Waktu: Pesan biasanya menciptakan rasa urgensi dengan menyatakan bahwa denda harus dibayar dalam waktu tertentu untuk menghindari konsekuensi lebih lanjut, seperti penahanan atau denda tambahan.

b. Spoofing

Spoofing adalah teknik di mana pelaku penipuan memalsukan identitas pengirim pesan sehingga pesan tersebut tampak seolah-olah berasal dari sumber yang tepercaya. Seperti berikut ini yang digunakan oleh pelaku yaitu:

a) Nomor Telepon Palsu: Pelaku menggunakan aplikasi atau layanan tertentu untuk mengirim pesan dari nomor yang mirip atau sama dengan nomor resmi instansi penegak hukum.

b) Nama Pengguna yang Dipalsukan: Dalam beberapa kasus, pelaku juga memalsukan nama pengguna di aplikasi *WhatsApp* untuk menyerupai nama resmi dari instansi yang berwenang.

c. Malware

Malware digunakan untuk menginfeksi perangkat korban dengan tujuan mencuri informasi pribadi atau memantau aktivitas korban dengan cara

a) Lampiran Berbahaya: Pelaku menyertakan lampiran dalam pesan *WhatsApp* yang jika dibuka, akan mengunduh dan menginstal malware di perangkat korban.

b) Tautan ke Situs Berbahaya: Pelaku menyertakan tautan yang mengarahkan korban ke situs web berbahaya yang akan mengunduh *malware* secara otomatis.

3.1.2 Identifikasi Kerentanan Teknologi

Identifikasi Kerentanan Teknologi yang Dieksploitasi oleh Pelaku Penipuan saat melakukan penipuan terutama penipuan tilang online via *WhatsApp* dapat disebabkan karna ada kerentanan teknologi yang bisa dieksploitasikan atau disalah gunakan sebagai berikut:

1) Kepercayaan pada Pesan yang Diterima

Banyak pengguna masih mudah percaya pada pesan yang diterima melalui *WhatsApp*, terutama jika pesan tersebut tampak berasal dari sumber yang tepercaya. Kerentanan ini dieksploitasi oleh pelaku penipuan untuk menyebarkan informasi palsu.

ISSN 2964-7746
https://ojs.unigal.ac.id/index.php/jsig/index

2) Kurangnya Edukasi mengenai *Phishing* dan *Spoofing*

Banyak pengguna yang belum sepenuhnya mengerti tentang teknik phishing dan spoofing, serta cara mengidentifikasi dan menghindari pesan penipuan. Kurangnya edukasi ini membuat pengguna rentan terhadap serangan.

3) Kemudahan Membuat Situs Palsu

Pelaku penipuan memanfaatkan kemudahan dalam membuat situs web palsu yang mirip dengan situs resmi. Teknologi ini dieksploitasi untuk menipu korban agar memberikan informasi pribadi atau melakukan pembayaran di situs palsu tersebut.

4) Kelemahan pada Protokol Keamanan

WhatsApp menggunakan enkripsi *end-to-end* untuk melindungi pesan, tetapi protokol keamanan ini masih memiliki kelemahan. Misalnya, jika pelaku penipuan berhasil memasang malware pada perangkat korban, mereka dapat mengakses pesan yang dienkripsi.

5) Peniruan Identitas

Kemampuan untuk meniru nomor telepon atau nama pengguna di *WhatsApp* memberikan kesempatan bagi pelaku penipuan untuk menyamar sebagai instansi resmi. Hal ini memanfaatkan kerentanan dalam sistem identifikasi pengguna.

3.1.3 Jejak Digital dan Bukti Elektronik

Jejak digital merupakan informasi yang ditinggalkan oleh pelaku saat menggunakan perangkat dan layanan digital. Dalam kasus penipuan tilang online melalui *WhatsApp*, berbagai bentuk jejak digital dapat ditinggalkan oleh pelaku yang melakukan penipuan tersebut.

Berikut adalah analisis dari beberapa jejak digital utama yang ditinggalkan oleh pelaku penipuan:

a. Analisis Jejak Digital yang Ditinggalkan oleh Pelaku Penipuan

a) Alamat IP *(Internet Protocol)*

Alamat IP adalah salah satu jejak digital paling signifikan yang dapat digunakan untuk melacak lokasi perangkat yang digunakan oleh pelaku penipuan. Setiap kali pelaku mengakses internet, alamat IP perangkatnya akan tercatat dalam log server penyedia layanan internet atau situs web yang diakses. Seperti berikut penjelasannya:

i) Log Server

Ketika pelaku mengakses situs web atau layanan online, alamat IP mereka dicatat dalam *log server*. Data ini mencakup informasi waktu akses, alamat IP, dan aktivitas yang dilakukan.

ii) Header Email dan Pesan

Jika pelaku mengirim email atau pesan melalui layanan tertentu,

ISSN 2964-7746
https://ojs.unigal.ac.id/index.php/jsig/index

alamat IP pengirim dapat ditemukan dalam header pesan. Informasi ini membantu melacak lokasi geografis pelaku.

b) Nomor Telepon

Nomor telepon yang digunakan oleh pelaku untuk mengirim pesan penipuan melalui *WhatsApp* atau melakukan panggilan telepon juga merupakan jejak digital yang penting.

i) Rekam Jejak Komunikasi

Operator telekomunikasi atau provider layanan telepon menyimpan log komunikasi yang mencakup nomor telepon yang digunakan, waktu dan durasi panggilan, serta pesan yang dikirim.

ii) Aplikasi Pihak Ketiga

Jika pelaku menggunakan aplikasi pihak ketiga untuk menyembunyikan nomor telepon mereka, analisis lebih lanjut terhadap aplikasi tersebut dapat mengungkapkan nomor asli pelaku.

c) Akun Palsu

Pelaku seringkali membuat akun palsu untuk menipu korban. Akun palsu ini dapat ditemukan di berbagai platform media sosial atau aplikasi pesan instan.

i) Data Registrasi

Informasi yang diberikan saat mendaftar akun, seperti email, nomor telepon, dan nama pengguna, dapat digunakan untuk melacak pelaku.

ii) Aktivitas Akun

Riwayat aktivitas akun, termasuk pesan yang dikirim, postingan, dan interaksi dengan pengguna lain dapat memberikan petunjuk tentang identitas pelaku.

b. Identifikasi Bukti Elektronik yang Dapat Digunakan dalam Penyelidikan dan Penuntutan.

Bukti elektronik adalah setiap informasi yang dihasilkan, disimpan, atau dikirim dalam bentuk digital yang dapat digunakan dalam penyelidikan dan penuntutan kasus penipuan. Berikut adalah beberapa jenis bukti elektronik yang dapat digunakan:

a) Log Server dan Data Jaringan

Data yang dicatat dalam log server dan data jaringan dapat menjadi bukti yang kuat dalam penyelidikan.

i. Log Akses

Catatan akses ke situs web atau layanan online yang menunjukkan alamat IP, waktu akses, dan aktivitas yang dilakukan oleh pelaku.

ii. Metadata Pesan

Metadata dari email atau pesan, termasuk alamat IP pengirim, waktu pengiriman, dan rute jaringan yang dilalui.

ISSN 2964-7746
https://ojs.unigal.ac.id/index.php/jsig/index

b) Bukti dari Perangkat Pelaku

Perangkat yang digunakan oleh pelaku, seperti komputer, smartphone, atau tablet, menyimpan banyak bukti elektronik yang relevan. Agar dapat mengetahui bahwa hal apa saja yang tertinggal jika pelaku sedang melakukan penipuan:

i. Riwayat *Browser*

Riwayat *browsing* dapat menunjukkan situs web yang diakses oleh pelaku, termasuk situs palsu yang digunakan untuk penipuan.

ii. File dan Dokumen

File yang disimpan di perangkat pelaku, termasuk dokumen yang berkaitan dengan penipuan, dapat menjadi bukti penting.

iii. Aplikasi Terinstal

Daftar aplikasi yang terinstal dan log aktivitas aplikasi dapat memberikan petunjuk tentang metode yang digunakan oleh pelaku.

c) Rekam Jejak Komunikasi

Rekam jejak komunikasi dari operator telekomunikasi dan penyedia layanan internet dapat digunakan untuk melacak aktivitas pelaku. Maka pihak dari operator komunikasi dapat menampilkan log panggilan atau pesan dan data lokasi terakhir pelaku melakukan aktivitas tersebut. Berikut adalah penjelasannya:

i. Log Panggilan dan Pesan

Catatan panggilan dan pesan yang mencakup nomor telepon, waktu, dan durasi komunikasi.

ii. Data Lokasi

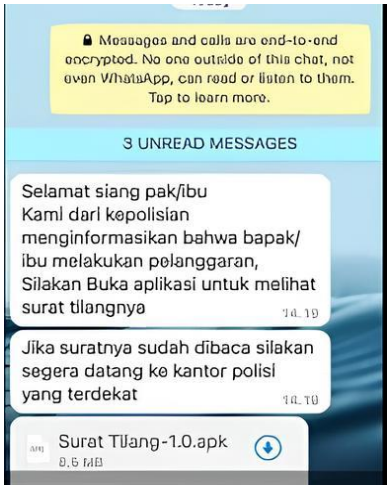
informasi lokasi yang dikumpulkan oleh operator telekomunikasi saat perangkat terhubung ke jaringan.

d) Bukti dari Platform *Online*

Platform online seperti media sosial dan aplikasi pesan instan menyimpan data yang dapat digunakan sebagai bukti. Pelaku akan meninggalkan bukti juga pada korban yang terkena penipuan online tilang online via *WhatsApp*, contohnya dan penjelasannya sebagai berikut:

i. Riwayat Chat

Riwayat chat yang mencakup pesan yang dikirim dan diterima, termasuk tautan dan lampiran yang dibagikan. Contoh pelaku sedang melakukan penipuan tilang online via *WhatsApp* dapat dilihat pada gambar 3.



Gambar 3. Contoh Pesan Penipuan Tilang Online
(Sumber Gambar detikOto Jumat, 17 Maret 2023)

ii. Profil Pengguna
Informasi profil pengguna, termasuk nama pengguna, email, dan nomor telepon yang terdaftar.

3.2 Analisis Jaringan Pelaku Penipuan

Identifikasi jaringan pelaku penipuan menggunakan analisis jaringan sosial. Analisis pola komunikasi dan struktur jaringan untuk mengungkap operasi penipuan. Maka kami menyimpulkan bahwa penipuan tilang online via *WhatsApp* ini bisa bergerak dari beberapa kelompok, yaitu:

a. Kelompok Pengirim Pesan.
Bertanggung jawab untuk mengirimkan pesan penipuan kepada korban.
b. Kelompok Penyedia Data.
Menyediakan data korban, seperti nomor telepon dan informasi pribadi kepada kelompok pengirim pesan.
c. Kelompok Malware.
Mengembangkan malware yang disebar melalui tautan atau file APK dalam pesan penipuan.
d. Kelompok Pencuci Uang.
Menguras rekening bank korban dan mentransfer uang hasil penipuan.

3.3 Analisis pola komunikasi dan struktur jaringan untuk mengungkap operasi penipuan.

Pola komunikasi dalam jaringan menunjukkan bahwa pelaku menggunakan berbagai strategi untuk memanipulasi korban. Ini akan menyebabkan korban akan sangat percaya karena sudah dimanipulasi oleh pelaku yang seolah – olah menjadi pihak dari terkait dan dapat dipercaya oleh korban, dengan seperti:

a. Menyamar sebagai petugas kepolisian
Pelaku menggunakan nama dan foto profil yang menyerupai petugas kepolisian untuk membangun kepercayaan korban.
b. Menciptakan rasa urgensi
Pelaku mendesak korban untuk segera menyelesaikan pembayaran denda tilang dengan alasan akan dikenakan sanksi jika terlambat.

ISSN 2964-7746
https://ojs.unigal.ac.id/index.php/jsig/index

c. Menawarkan solusi mudah

Pelaku menyediakan tautan atau file APK yang diklaim dapat digunakan untuk melihat bukti pelanggaran dan melakukan pembayaran denda.

3.4 Pencegahan dan Mitigasi Penipuan Tilang *Online*.

Penipuan tilang online melalui *WhatsApp* merupakan kejahatan yang meresahkan dan merugikan masyarakat. Oleh karena itu, upaya pencegahan dan mitigasi menjadi sangat penting untuk melindungi masyarakat dari modus penipuan ini.

a) Strategi pencegahan menggunakan teknologi.

i) Autentikasi Multi-Faktor (MFA).

Penerapan MFA pada platform *WhatsApp*, sistem pembayaran tilang online, dan layanan publik lainnya dapat meningkatkan keamanan akun dan mempersulit pelaku penipuan untuk mengaksesnya.

ii) Pemfilteran Konten.

Penerapan sistem pemfilteran konten pada platform *WhatsApp* dan media sosial lainnya dapat membantu mendeteksi dan memblokir pesan penipuan sebelum menjangkau korban.

iii) Kecerdasan Buatan (AI).

Penggunaan AI dapat membantu mengidentifikasi pola komunikasi dan aktivitas yang mencurigakan dalam platform online, sehingga dapat mendeteksi potensi penipuan dan mengambil tindakan pencegahan.

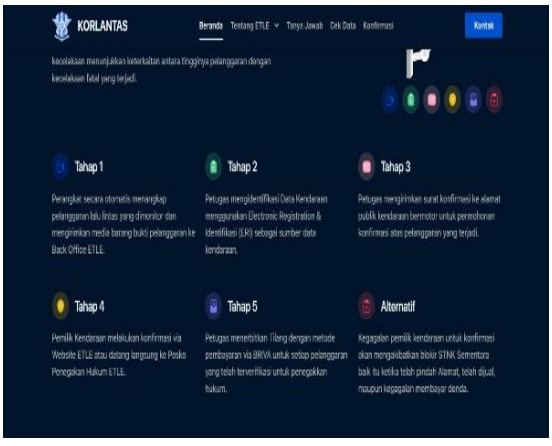
b) Mitigasi Risiko.

i) Peningkatan keamanan sistem pembayaran tilang online:

Menyediakan berbagai metode pembayaran tilang online yang mudah diakses dan aman, seperti melalui ATM, bank, atau aplikasi mobile banking. Meneraptkan sistem enkripsi data saat melakukan transaksi.

ii) Kerjasama antara pihak terkait:

Kerjasama antara pihak kepolisian, Kementerian Komunikasi dan Informatika (Kominfo), dan operator telekomunikasi untuk melacak dan memblokir nomor telepon yang digunakan untuk penipuan tilang online. Dapat melihat dari pihak kepolisan pada gambar 4 berikut.



Gambar 4. Tahap terjadi tilang elektronik dan langkah langkah dalam pengecekan serta pembayaran denda

ISSN 2964-7746
https://ojs.unigal.ac.id/index.php/jsig/index

untuk pelanggar (sumber: *Website* Korlantas Polri)

iii) Pentingnya peran aktif masyarakat:

Melaporkan kepada pihak berwajib jika menerima pesan penipuan tilang online dan tidak membuka file APK yang mencurigakan dalam pesan tilang online.

3.5 Tantangan dan Rekomendasi dalam Menghadapi Penipuan Tilang Online

a. Tantangan dalam Investigasi Forensik Digital dan Identifikasi Pelaku Penipuan

Investigasi forensik digital dalam kasus penipuan tilang online melalui *WhatsApp* memiliki beberapa tantangan, di antaranya:

a) Sifat anonim platform online

Pelaku penipuan seringkali menggunakan identitas palsu dan akun anonim di platform online, sehingga sulit untuk melacak dan mengidentifikasi mereka.

b) Kecepatan pertukaran informasi

Platform online seperti *WhatsApp* memungkinkan pertukaran informasi yang cepat dan mudah, sehingga pelaku penipuan dapat dengan mudah menghapus bukti atau mengubah identitas mereka.

c) Keterbatasan data forensik

Data yang tersedia pada platform online mungkin tidak lengkap atau terfragmentasi, sehingga sulit untuk merekonstruksi kejadian secara akurat.

d) Keterampilan dan pengetahuan teknis

Investigasi forensik digital membutuhkan keterampilan dan pengetahuan teknis yang mumpuni, yang mungkin tidak dimiliki oleh semua penyidik.

b. Rekomendasi untuk Kolaborasi antara Instansi Pemerintah, Penyedia Layanan, dan Lembaga Keamanan Siber.

Untuk mengatasi tantangan-tantangan tersebut diperlukan kolaborasi yang kuat antara berbagai pihak, di antaranya:

a) Instansi pemerintah

Polri, Kementerian Komunikasi dan Informatika (Kominfo), dan Badan Siber dan Sandi Negara (BSSN) dapat bekerja sama untuk mengembangkan strategi investigasi forensik digital yang efektif, meningkatkan kapasitas penyidik, dan memperkuat regulasi terkait keamanan siber.

b) Penyedia layanan

Platform online seperti *WhatsApp*, Facebook, dan Google dapat bekerja sama dengan penegak hukum untuk menyediakan akses data yang diperlukan untuk investigasi, meningkatkan mekanisme pelaporan penipuan, dan mengembangkan teknologi

ISSN 2964-7746
https://ojs.unigal.ac.id/index.php/jsig/index

untuk mendeteksi dan mencegah penipuan online.

c) Lembaga keamanan siber

Lembaga keamanan siber seperti *National Cyber Security Agency* (NCSA) dan Indonesia Internet Defense and Security Institute (IIDS) dapat memberikan pelatihan dan edukasi kepada penyidik dan masyarakat tentang keamanan siber, membantu menganalisis data forensik digital, dan mengembangkan teknologi untuk melawan *cybercrime*.

c. Pentingnya Edukasi Masyarakat tentang Keamanan Siber dan Pengenalan Penipuan Online.

Edukasi dan literasi digital bagi masyarakat sangat penting untuk mencegah penipuan tilang online. Berupaya untuk dapat memahami apa saja yang harus dilakukan ketika pelaku melakukan atau sedang menipu masyarakat, yaitu:

a) Mengetahui modus penipuan online yang umum terjadi

Masyarakat perlu dibekali pengetahuan tentang modus penipuan online yang sering digunakan, seperti penipuan tilang online, penipuan phishing, dan penipuan berkedok giveaway.

b) Berhati-hati dengan informasi yang diterima di internet

Masyarakat harus kritis terhadap informasi yang diterima di internet, terutama jika informasi tersebut datang dari sumber yang tidak dikenal atau mencurigakan.

c) Menjaga keamanan akun *online.*

Masyarakat perlu menjaga keamanan akun online mereka dengan menggunakan password yang kuat, mengaktifkan autentikasi multi-faktor, dan berhati-hati saat mengklik tautan atau membuka file attachment.

d) Melaporkan penipuan *online* kepada pihak berwajib.

Jika masyarakat menemukan atau mengalami penipuan online, mereka harus segera melaporkannya kepada pihak berwajib, seperti Polri atau BSSN.

IV. KESIMPULAN

Penipuan tilang online yang marak terjadi akhir - akhir ini menjadi ancaman yang semakin serius di era digital pada saat ini dan menimbulkan kerugian bagi korban salah satunya adalah kerugian finansial karena terjerat penipuan tilang *online*. Hal ini dapat terjadi kerena kurangnya pemahaman masyarakat mengenai penipuan *online* via *WhatsApp*, pentingnya meningkatkan edukasi dan literasi masyarakat tentang penipuan *online*, meningkatkan patroli *cyber* dan penegakan hukum terhadap pelaku penipuan *online* dapat menjadi solusi untuk mencegah terjadinya

ISSN 2964-7746
https://ojs.unigal.ac.id/index.php/jsig/index

penipuan tilang *online* via *WhatsApp*. Dalam penelitian ini tim peneliti melakukan penelitian menggunakan metode deskriptif kualitatif yang merupakan pendekatan penelitian yang berfokus pada pemahaman mendalam dan menyeluruh terhadap suatu fenomena atau situasi sosial untuk menginvestigasi dan mengevaluasi masalah yang dihadapi dengan menggunakan data sekunder.

V. SARAN

Saran-saran untuk untuk penelitian lebih lanjut untuk menutup kekurangan penelitian. Tidak memuat saran-saran diluar untuk penelitian lanjut. Kesulitan dalam mengidentifikasi dan melacak pelaku. Penggunaan teknologi seperti nomor telepon dan akun media sosial palsu semakin mempersulit proses penegakan hukum. Maka perlunya mengembangkan teknologi dalam mengidentifikasi pelaku dan melacak pelaku. Kurangnya koordinasi antara instansi dapat menghambat proses investigasi dan tindak lanjut untuk pelaku. Penegakan hukum Indonesia yang lemah maka perlu regulasi tegas dalam penjerat pelaku penipuan tilang online ini.

DAFTAR PUSTAKA

[1] R. Kuswulandari, A. W. I. Jowanka, T. N. P. Riyanto, dan T. Listiani, “Analisis Manajemen Risiko Ancaman Kejahatan Siber (Cyber Crime) Dalam Aplikasi Whatsapp,” *Prosiding Seminar Nasional Teknologi Informasi dan Bisnis (SENATIB)*, 2023.

[2] Badan Siber dan Sandi Negara, “LANSKAP KEAMANAN SIBER INDONESIA 2023,” Jakarta Selatan, 2023. [Daring]. Tersedia pada: https://www.bssn.go.id/wp-content/uploads/2024/03/Lanskap-Keamanan-Siber-Indonesia-2023.pdf

[3] M. Adaninggar, F. Andhika Perkasa, dan A. U. Hosnah, “TANGGUNG JAWAB HUKUM DAN KONSEKUENSI BAGI PELAKU PENIPUAN DENGAN MODUS ARISAN MELALUI PLATFORM MEDIA SOSIAL,” *Civilia : Jurnal Kajian Hukum dan Pendidikan Kewarganegaraan*, vol. 3, hlm. 63–71, 2024, [Daring]. Tersedia pada: http://jurnal.anfa.co.id

[4] L. Firdausiah Ersa, G. Aningsih, T. Hidayat, dan A. Febri Sonni, “Analisis Jaringan Komunikasi Penipuan Daring Melalui Media Sosial Whatsapp Messenger,” *Jurnal Netnografi Komunikasi*, vol. 2, no. 2, hlm. 73–90, 2024, [Daring]. Tersedia pada: http://netnografiikom.org/index.php/netnografi

[5] S. Sunardi, A. Fadlil, dan N. M. P. Kusuma, “Implementasi Data Mining dengan Algoritma Naïve Bayes untuk Profiling Korban Penipuan Online di Indonesia,” *JURNAL MEDIA INFORMATIKA BUDIDARMA*, vol. 6, no. 3, hlm. 1562, Jul 2022, doi: 10.30865/mib.v6i3.3999.

ISSN 2964-7746
https://ojs.unigal.ac.id/index.php/jsig/index

[6] L. Z. Apriliana dan N. S. P. Jaya, "EFEKTIVITAS PENGGUNAAN E–TILANG TERHADAP PELANGGARAN LALU LINTAS DI POLRES MAGELANG," vol. 5, no. 2, 2019.

[7] M. Mulyadi *dkk.*, "Analisis Penipuan Online Melalui Media Sosial Dalam Perspektif Kriminologi," *Media Hukum Indonesia (MHI)*, vol. 2, no. 2, hlm. 74, 2024, doi: 10.5281/zenodo.11183088.

[8] D. Fajariandono, W. Wilman Sitorus, E. Desianto, F. Aer, A. Rahim, dan Y. Andy Pramata, "Upaya Risk Management Dalam Mengatasi Penipuan Modus Social Engineering Melalui Smartphone," *EKOMA: Jurnal Ekonomi, Manajemen, Akuntansi*, vol. 3, no. 3, 2024.

[9] H. Nurfaizal, A. Efendi, dan D. Eko Prasetyo, "Sosialisasi Fenomena Kejahatan Cyber dan Langkah Penanggulangan Sebagai Bentuk Antisipasi," *APPA: Jurnal Pengabdian kepada Masyarakat*, vol. 1, no. 5, 2024, [Daring]. Tersedia pada: https://jurnalmahasiswa.com/index.php/appa

[10] N. Fassa, D. I. Aryani, dan E. Wianto, "Perancangan Animasi sebagai Media Edukasi Kesadaran Masyarakat terhadap Kasus Penipuan File APK," *Jurnal Penelitian Mahasiswa Desain*, vol. 03, no. 02, hlm. 204–221, 2023, [Daring]. Tersedia pada: https://ojs.unikom.ac.id/index.php/divagatra

[11] R. Riskuna dan L. Uce, "STUDI ANALISIS PENGARUH GAME ONLINE TERHADAP MINAT BELAJAR SISWA," *JURNAL PENDIDIAKANNUSANTARA*, vol. 1, no. 1, 2024.

[12] F. Ananda, W. Ramadhan, L. Rohana, E. Wahyuningsih, dan H. A. Falah, "PENIPUAN KARTU KREDIT DI INDONESIA," *JISOSEPOL: JURNAL ILMU SOSIAL EKONOMI DAN POLITIK*, vol. 2, no. 2, 2024, [Daring]. Tersedia pada: https://samudrapublisher.com/index.php/JISOSEPOL

[13] M. I. Syahroni, "ANALISIS DATA KUANTITATIF," *Jurnal Al-Musthafa STIT Al-Aziziyah Lombok Barat*, vol. 1, no. 3, 2023.

[14] M. M. Ali, T. Hariyati, M. Y. Pratiwi, dan S. Afifah, "Metodologi Penelitian Kuantitatif Dan Penerapan Nya Dalam Penelitian," *Education Journal*, vol. 2, no. 2, 2022.

[15] Y. Prayuti, A. T. Parulian, I. Parulian, D. A. Jeremy, dan J. Fire, "PERLINDUNGAN KONSUMEN DALAM TRANSAKSI PRODUK KESEHATAN ONLINE: ANALISIS REGULASI DAN PRAKTIK," *JOURNAL SYNTAX IDEA*, vol. 3, no. 6, hlm. 1247, Jun 2021, doi: 10.36418/syntax-idea.v3i6.1227.

[16] Firdaus, E. A., Maulani, S. (2023). Perencanaan Kerangka Kerja Menggunakan The Open Group Architecture Framework-Architecture Development Method (TOGAF-ADM) pada Puskesmas Sukatani. Jurnal Sistem Informasi Galuh, 32-37.