Unes Law Review

e-ISSN: 2622-7045 | p-ISSN: 2654-3605
Volume 8, Issue 2, Desember 2025
Available online at: https://review-unes.com

Penyidikan Tindak Pidana Pencurian Informasi Data Melalui Skimming ATM Bank BNI Cabang Padang

Muhammad Fajri Akbar Perdana[1*], Ismansyah[2], Rembrandt[3]
[1] Fakultas Hukum, Universitas Andalas, Padang, Indonesia
[2] Fakultas Hukum, Universitas Andalas, Padang, Indonesia
[3] Fakultas Hukum, Universitas Andalas, Padang, Indonesia

[*]Corresponding Author: muhammadfajriap11@gmail.com

Artikel Histori
Direvisi: 17-09-2025
Diterima: 10-10-2025
Diterbitkan: 13-12-2025

Abstrak: Kemajuan teknologi komputer, telekomunikasi, dan internet telah memicu munculnya kejahatan siber, termasuk skimming ATM yang mencuri data nasabah melalui alat pengganda informasi kartu dan PIN yang dipasang pada mesin ATM. Meskipun Pasal 30 ayat (2) Undang-Undang Nomor 19 Tahun 2016 tentang ITE telah mengatur penegakan hukum kejahatan ini, kasus skimming tetap terjadi seperti yang dialami mesin ATM Bank BNI Cabang Padang. Penelitian ini bertujuan menganalisis pengumpulan alat bukti dalam penyidikan, kendala yang dihadapi penyidik, dan upaya mengatasi kendala tersebut. Penelitian ini merupakan penelitian yuridis empiris yang bersifat deskriptif analitis dengan menggunakan data sekunder yang diperkuat dengan data primer. Data tersebut kemudian dianalisis secara kualitatif dan disajikan dalam bentuk deskriptif kualitatif. Hasil penelitian menunjukkan bahwa penyidikan kasus pencurian data ATM Bank BNI Cabang Padang melibatkan lima tahap: penangkapan, penyitaan alat bukti, pemeriksaan saksi dan tersangka, serta analisis forensik digital. Kendala utama meliputi teknologi canggih pelaku, keterbatasan alat dan SDM, birokrasi, serta kesulitan pelacakan akibat enkripsi dan server asing. Penyidik mengatasi hambatan ini melalui peningkatan kapasitas forensik, koordinasi antarlembaga, pelatihan khusus, dan sosialisasi pencegahan. Upaya terpadu ini bertujuan memaksimalkan efektivitas penyidikan dan meminimalkan kejahatan serupa di masa depan.

Kata Kunci: Skimming ATM, Penegakan Hukum ITE, Pengumpulan Alat Bukti, Forensik Digital, Kejahatan Siber

Abstract: *Advances in computer, telecommunications, and internet technology have triggered the emergence of cybercrimes, including ATM skimming that steals customer data through card and PIN information multipliers installed on ATM machines. Although Article 30 paragraph (2) of Law Number 19 of 2016 concerning ITE has regulated the enforcement of this crime, skimming cases still occur, like those experienced by the ATM machines of Bank BNI Padang Branch. This research aims to analyze evidence collection in investigations, obstacles faced by investigators, and efforts to overcome these obstacles. This research is an empirical juridical research that is descriptive and analytical using secondary data reinforced with primary data. The data is then analyzed qualitatively and presented in a qualitative descriptive form. The results show that the investigation of the ATM theft case of Bank BNI Padang Branch involves five stages: arrest, confiscation of evidence, examination of witnesses and suspects, and digital forensic analysis. The main obstacles include advanced technology of actors, limited tools and human resources, bureaucracy, and tracking difficulties due to encryption and foreign servers. Investigators overcome these barriers through forensic capacity building, interagency coordination, specialized training, and prevention socialization. This integrated effort aims to maximize the effectiveness of investigations and minimize similar crimes in the future.*

DOI: https://doi.org/10.31933/mhg1dg94

Keywords: *ATM Skimming, ITE Law Enforcement, Evidence Collection, Digital Forensics, Cybercrime*

PENDAHULUAN

Perkembangan teknologi informasi dan komunikasi yang pesat telah membawa dampak signifikan terhadap berbagai aspek kehidupan masyarakat, termasuk dalam sektor perbankan.[1] Kemajuan teknologi komputer, telekomunikasi, dan internet yang didukung oleh jaringan luas berupa internet dengan kecepatan yang terus berkembang telah memudahkan manusia dalam melaksanakan aktivitas kehidupan sehari-hari.[2] Namun, di balik kemudahan yang ditawarkan, perkembangan teknologi juga membawa konsekuensi negatif berupa munculnya bentuk-bentuk kejahatan baru yang memanfaatkan teknologi digital sebagai sarana operasinya.[3]

Era *cyber* dalam dunia bisnis telah dimulai, yang ditandai dengan meningkatnya transaksi elektronik di berbagai sektor, termasuk perbankan.[4] Kejahatan *cyber* atau *cybercrime* merupakan konsekuensi dari perkembangan teknologi yang semakin canggih dan mempunyai dampak buruk bagi kehidupan manusia.[5] *Cybercrime* didefinisikan sebagai suatu bentuk penggunaan fasilitas komputer atau sistem elektronik yang digunakan untuk menyebabkan kerusakan pada sistem elektronik yang dituju oleh pelaku dengan memaksa masuk ke dalam sistem elektronik tersebut secara melawan hukum.[6]

Berbagai bentuk kejahatan siber bermunculan, seperti manipulasi data, *spionase*, *hacking*, penipuan kartu kredit (*carding*), merusak sistem (*cracking*), dan penyalinan data dari kartu ATM (*skimming* ATM).[7] Khususnya skimming ATM, merupakan modus kejahatan yang berupa penggandaan data kartu ATM nasabah dengan menggunakan alat yang ditempatkan pada *card reader*.[8]

Skimming sendiri merupakan tindakan pencurian informasi kartu debit atau kredit dengan cara mengkloning data dari *magnetic stripe* yang terdapat pada kartu milik nasabah secara *illegal*.[9] Di Indonesia, cybercrime telah diatur dalam Undang-Undang Nomor 11 Tahun 2008 yang kemudian diperbarui dengan Undang-Undang Nomor 19 Tahun 2016 tentang Informasi dan Transaksi Elektronik (ITE). Kepolisian Republik Indonesia melalui Peraturan Polri Nomor 14 Tahun 2018 Tentang Susunan Organisasi dan Tata Kerja Kepolisian Daerah mengatur Ditreskrimsus untuk memaksimalkan penegakan peraturan terhadap cyberspace, salah satunya dalam kasus skimming pada mesin ATM.[10]

Penegakan hukum terhadap tindak pidana cyber crime di bidang perbankan ternyata belum berjalan optimal, padahal ketentuan hukum yang ada sebenarnya memungkinkan pencegahan dan pemberantasan tindak pidana cyber crime di bidang perbankan[11]. Salah satu kasus yang menunjukkan kompleksitas penanganan kejahatan skimming terjadi di Satreskrim

---

[1] Gunawan, K., & Gunawan, Y. (2013). *Sekelumit Tentang Penyadapan Dalam Hukum Positif di Indonesia*. Bandung: Nuansa Aulia, p. 1.

[2] Marpaung, L. (2011). *Proses Penanganan Perkara Pidana: Penyidikan Dan Penyelidikan*. Jakarta: Sinar Grafika, p. 22.

[3] Wahid, A., & Latib, M. (2005). *Kejahatan Mayantara*. Bandung: Rafika Aditama, p. 33.

[4] Garner, B. A. (2009). *Black's Law Dictionary* (9th ed.). St. Paul: Thomson Reuters, p. 427.

[5] Arief, B. N. (2006). *Tindak Pidana Mayantara Perkembangan Kajian Cybercrime di Indonesia*. Jakarta: RajaGrafindo Persada, p. 1.

[6] Mansur, D. M. A., & Gultom, E. (2005). *Cyber Law Aspek Hukum Teknologi Informasi*. Bandung: Refika Aditama, p. 5.

[7] Suhariyanto, B. (2013). *Tindak Pidana Teknologi Informasi (Cybercrime): Urgensi Pengaturan dan Celah Hukumnya*. Jakarta: Rajawali Pers, p. 17.

[8] Ramdhan, J. G., & Sumiyati. (2019). Perlindungan Hukum Terhadap Nasabah Korban Skimming Ditinjau Dari Undang Undang Nomor 8 Tahun 1999. *Jurnal Ilmu Hukum*, 12(1), p. 78.

[9] Gabriel, A., Pinasang, D. R., & Bawole, H. Y. A. (2024). Penegakan Hukum Terhadap Kejahatan Skimming Atm Berdasarkan Undang-Undang Nomor 19 Tahun 2016.*Lex Privatum*, 13(5), pp. 2-3.

[10] *Ibid.,* p. 5.

Polresta Padang, yaitu Laporan Polisi Nomor: LP/569/A/X/2020/Resta-SPKT Unit III, tanggal 22 Oktober 2020, yang melibatkan tindak pidana illegal akses atau pembobolan data pada mesin ATM Bank BNI.

Kasus ini melibatkan empat pelaku utama yang bekerja secara terorganisir di bawah koordinasi seorang bos di Malaysia. Modus operandi yang digunakan sangat canggih, dimulai dengan pemasangan alat skimming berupa kamera kecil untuk merekam PIN nasabah dan alat pembaca data di slot kartu ATM. Data yang berhasil dikumpulkan kemudian diolah menggunakan laptop dan dikirimkan melalui aplikasi *Team Viewer* ke jaringan internasional. Dalam menganalisis kasus ini, teori sistem peradilan pidana (*criminal justice system*) menjadi sangat relevan. Romli Atmasasmita menjelaskan bahwa sistem peradilan pidana menekankan pada koordinasi dan sinkronisasi komponen peradilan pidana, pengawasan dan pengendalian penggunaan kekuasaan, efektivitas sistem penanggulangan kejahatan, dan penggunaan hukum sebagai instrumen untuk memantapkan "*the administration of justice*."[11] Sejalan dengan hal tersebut, pendekatan *Crime Control Model* oleh Herbert Packer sangat relevan dalam konteks kejahatan skimming, di mana pemberantasan kejahatan merupakan fungsi terpenting yang harus diwujudkan dengan titik tekan pada efektivitas, kecepatan, dan kepastian.[12]

Selanjutnya, untuk melengkapi analisis teoretis, teori penegakan hukum menurut Soerjono Soekanto menjadi landasan dalam mengevaluasi efektivitas penanganan kasus ini. Soekanto mengidentifikasi lima faktor yang mempengaruhi efektivitas penegakan hukum: faktor hukum atau peraturan itu sendiri, faktor penegak hukum, faktor sarana atau fasilitas pendukung, faktor masyarakat, dan faktor kebudayaan.[13] Dalam praktiknya, keterbatasan dalam aspek-aspek tersebut justru menjadi kendala utama dalam penyidikan kasus skimming ATM, sehingga diperlukan evaluasi menyeluruh terhadap setiap komponen sistem peradilan pidana untuk meningkatkan efektivitas penanganan kejahatan sejenis di masa mendatang.

Berdasarkan latar belakang tersebut, penelitian ini fokus pada tiga permasalahan utama: Bagaimana pengumpulan alat bukti dalam penyidikan tindak pidana pencurian informasi data mesin ATM Bank BNI Cabang Padang di Satreskrim Polresta Padang? Apa kendala yang dihadapi penyidik Satreskrim Polresta Padang dalam pengumpulan alat bukti tersebut? Bagaimana upaya penyidik dalam mengatasi kendala pengumpulan alat bukti dalam penyidikan tindak pidana ini?

METODE PENELITIAN

Penelitian ini menggunakan pendekatan yuridis empiris dengan sifat deskriptif analitis.[14] Pendekatan yuridis empiris adalah penelitian hukum mengenai implementasi ketentuan hukum normatif secara in action pada setiap peristiwa hukum tertentu yang terjadi dalam masyarakat.[15] Metode ini dipilih karena penelitian ini bertujuan menganalisis implementasi peraturan perundang-undangan dalam praktik penyidikan kasus skimming ATM.

Sumber data terdiri dari data primer dan data sekunder. Data primer diperoleh melalui wawancara mendalam dengan penyidik Satreskrim Polresta Padang, khususnya penyidik yang menangani kasus pencurian data ATM Bank BNI Cabang Padang. Data sekunder terdiri dari bahan hukum primer berupa peraturan perundang-undangan terkait (UUD 1945, KUHP, KUHAP, UU Kepolisian, UU ITE, dan peraturan pelaksanaannya), bahan hukum sekunder

[11] Atmasasmita, R. (1996). *Sistem Peradilan Pidana (Criminal Justice System) Perspektif Ekstensialisme dan Abolisionisme*. Bandung: Bina Cipta, p. 9.

[12] Lamintang, P. A. F. (1996). *Kriminologi dan Sistem Peradilan Pidana*. Jakarta: Pusat Pelayanan Keadilan dan Pengabdian Hukum UI, p. 21.

[13] Soekanto, S. (2021). *Faktor-Faktor Yang Mempengaruhi Penegakan Hukum*. Jakarta: Rajawali Press, pp. 8-9.

[14] Atmasasmita, R. (1996). *Sistem Peradilan Pidana (Criminal Justice System) Perspektif Ekstensialisme dan Abolisionisme*. Bandung: Bina Cipta, p. 9.

[15] *Ibid.*

berupa literatur, jurnal, dan hasil penelitian terdahulu, serta bahan hukum tersier berupa kamus hukum dan ensiklopedia.[16] Teknik pengumpulan data dilakukan melalui studi dokumen dan wawancara mendalam. Studi dokumen dilakukan untuk mengumpulkan data sekunder melalui penelitian kepustakaan yang relevan dengan topik penelitian.[17] Wawancara mendalam dilakukan dengan narasumber kunci, yaitu Kanit Tipiter Satreskrim Polresta Padang yang memiliki pengalaman langsung dalam menangani kasus *skimming* ATM.

Data yang terkumpul kemudian diolah dan dianalisis menggunakan metode kualitatif deskriptif. Analisis dilakukan dengan mengkategorikan data berdasarkan rumusan masalah, kemudian mengaitkannya dengan teori hukum yang relevan.[18] Pendekatan ini bertujuan menghasilkan gambaran yang komprehensif tentang proses penyidikan, kendala yang dihadapi, dan upaya penanggulangan dalam kasus pencurian data ATM.

PEMBAHASAN

Tinjauan Umum Penyidikan dan Tindak Pidana Pencurian Data

Penyidikan merupakan serangkaian tindakan penyidik dalam hal dan menurut cara yang diatur dalam undang-undang untuk mencari serta mengumpulkan bukti yang dengan bukti itu membuat terang tentang tindak pidana yang terjadi dan guna menemukan tersangkanya.[19] Menurut R. Wiyono, perbedaan mencolok antara penyelidikan dengan penyidikan adalah jika dalam penyelidikan arahnya untuk menentukan ada atau tidaknya peristiwa yang diduga merupakan perbuatan pidana, sedangkan dalam penyidikan arahnya untuk menentukan siapa tersangka yang dapat diduga melakukan perbuatan pidana tersebut.[20]

Tindak pidana adalah terjemahan dari Strafbaarfeit yang secara umum identik dengan kejahatan.[21] Moeljatno menyatakan bahwa tindak pidana adalah perbuatan yang dilarang oleh suatu aturan hukum larangan mana disertai ancaman (sanksi) yang berupa pidana tertentu, bagi barangsiapa yang melanggar larangan tersebut.[22] Dalam konteks pencurian informasi data melalui ATM, hal ini berkaitan dengan kejahatan *cyber* yang merupakan perbuatan melawan hukum yang dilakukan secara pribadi maupun kelompok dengan memanfaatkan komputer atau jaringan komputer sebagai sarana dalam melakukan suatu kejahatan untuk memperoleh keuntungan dengan merugikan pihak lain.[23]

Skimming ATM adalah tindakan pencurian data yang merugikan nasabah bank dengan mencuri informasi data dari ATM melalui penggandaan data nasabah lewat magnetic strip pada kartu ATM, dengan cara menempelkan alat yang disebut skimmer pada slot kartu di mesin ATM.[24] Kejahatan skimming ATM diatur dalam Pasal 30 ayat (2) Undang-Undang Nomor 19 Tahun 2016 yang berbunyi:

> "Setiap Orang dengan sengaja dan tanpa hak atau melawan hukum mengakses Komputer dan/atau Sistem Elektronik dengan cara apa pun dengan tujuan untuk memperoleh Informasi Elektronik dan/atau Dokumen Elektronik."

---

[16] Marzuki, P. M. (2011). *Penelitian Hukum*. Jakarta: Prenadamedia, pp. 141-142.

[17] Sugiyono. (2016). *Metodologi Penelitian Kuantitatif, Kualitatif Dan R&D*. Bandung: CV. Alfabeta, p.247.

[18] Muhammad, A. K. (2004). *Hukum dan Penelitian Hukum*. Bandung: Citra Aditya Bakti, p. 126.

[19] Effendi, Tolib. (2014). *Dasar-Dasar Hukum Acara Pidana*. Malang: Setara Press, p. 82.

[20] Wiyono, R. (2006). *Pengadilan Hak Asasi Manusia di Indonesia*. Jakarta: Kencana, p. 36.

[21] Chazawi, Adami. (2005). *Pelajaran Hukum Pidana I.* Jakarta: RajaGrafindo Persada, p. 69.

[22] Moeljatno. (2000). *Asas-Asas Hukum Pidana*. Jakarta: Rineka Cipta, pp. 54-55.

[23] Arifah, Dista Amalia. (2011). Kasus Cybercrime di Indonesia. *Jurnal Bisnis dan Ekonomi*, 18 (2), p. 186.

[24] Gabriel, A., Pinasang, D. R., & Bawole, H. Y. A. *Loc.Cit.*

Pengumpulan Alat Bukti dalam Penyidikan Tindak Pidana Pencurian Informasi Data Mesin ATM Bank BNI Cabang Padang

Penyidikan tindak pidana pencurian informasi data melalui skimming pada mesin ATM Bank BNI Cabang Padang yang dilakukan oleh Satreskrim Polresta Padang merupakan contoh kompleksitas penanganan kejahatan teknologi di era digital. Kasus ini melibatkan empat pelaku utama yang bekerja secara terorganisir: Sakban Daulay (Pgl Ben), Jamal Alamsyah Sagala (Pgl Jamal), Mangiring Laia (Pgl Firman), dan Roland Reza Lubis (Pgl Reza), yang beroperasi di bawah koordinasi seorang bos di Malaysia.

Pengumpulan alat bukti dalam kasus ini dilakukan melalui lima tahap sistematis yang mencerminkan penerapan teori sistem peradilan pidana. Tahap pertama adalah penangkapan dan penahanan. Penangkapan dilakukan pada 21 Oktober 2020 berdasarkan Surat Perintah Penangkapan Nomor SP.Kap/171/X/2020/Reskrim dan SP.Kap/170/X/2020/Reskrim. Proses ini menunjukkan kepatuhan terhadap prinsip *due process of law* sebagaimana diatur dalam KUHAP, di mana setiap tindakan penangkapan harus berdasarkan surat perintah yang sah.[25]

Modus operandi pelaku dimulai pada tanggal 11-15 Oktober 2020, di mana Jamal dan Ben mencari lokasi ATM Bank BNI yang ramai dan strategis. Pada tanggal 20 Oktober 2020, sekitar pukul 16.00 WIB, Jamal dan Firman memasang alat skimming berupa kamera kecil (mata) di atas tombol angka untuk merekam PIN nasabah dan alat pembaca data (kepala) di slot kartu ATM. Setelah pemasangan, mereka mengamati dari warung sekitar yang berjarak 15 meter dari ATM, sementara Ben dan Reza membantu memantau. Tahap selanjutnya, adalah penyitaan barang bukti berdasarkan Surat Perintah Penyitaan Nomor Sp.Sita/140/X/2020/Reskrim tanggal 22 Oktober 2020. Barang bukti yang disita sangat lengkap dan mencerminkan tingkat kecanggihan operasi, termasuk 3 set "mata" (perangkat perekam PIN), 5 set "kepala" (pembaca data kartu), 1 unit laptop HP, 1 set WiFi TP-Link, 5 unit ponsel, 3 kartu memori, serta peralatan pendukung seperti cat semprot, lem, amplas, dan kuas untuk menyamarkan perangkat. Penyitaan juga mencakup 2 unit kendaraan (Honda Scoopy dan Honda Vario) serta uang tunai Rp5.000.000 yang diduga hasil kejahatan.

Pengumpulan alat bukti dalam penyidikan dilanjutkan dengan pemeriksaan saksi, dimana pada kasus ini melibatkan delapan orang, termasuk perwakilan Bank BNI (Asdiyanto dan Hendro), karyawan hotel (Hafiz Zikri Mardi dan Mega Mustika), serta anggota kepolisian (Dian Wihendro Ratno, Aulia Purwanto, dan Albert Firman). Keterangan saksi dari Bank BNI mengungkapkan bahwa pihak bank segera mengambil tindakan pencegahan dengan memaksa nasabah mengganti PIN (force PIN) begitu terdeteksi indikasi skimming. Sementara itu, karyawan hotel mengungkapkan aktivitas mencurigakan para pelaku selama menginap, seperti sering keluar-masuk kamar sambil membawa tas besar.

Selanjutnya, berdasarkan keterangan saksi tersebut, penyidik kemudian melakukan pemeriksaan terhadap para tersangka. Para pelaku secara terbuka mengakui keterlibatan mereka dalam operasi terorganisir ini. Setiap anggota memiliki peran spesifik: Pgl Ben sebagai koordinator, Pgl Jamal dan Pgl Firman bertugas memasang dan mencopot alat skimming, sementara Pgl Reza memantau lokasi. Para tersangka mengaku bekerja di bawah komando "Pgl Mas" di Malaysia dengan sistem pembayaran Rp2.000.000 untuk setiap 500 data nasabah yang berhasil dicuri, plus uang harian Rp100.000.

Pada tahap terakhir, penyidik akan melakukan analisis terhadap alat bukti yang dikategorikan menjadi empat jenis: alat bukti fisik (perangkat *skimming*, laptop, ponsel), alat bukti digital (rekaman CCTV ATM, aplikasi *Team Viewer*, pesan *WhatsApp* grup "Boss Group"), alat bukti dokumen (surat pengiriman DHL, paspor, catatan transaksi), dan keterangan saksi serta tersangka[37]. Keberagaman bukti ini mencerminkan prinsip *integrated*

[25] Harahap, M. Y. (2007). *Pembahasan Dan Penerapan KUHAP Penyidikan Dan Penuntutan*. Jakarta: Sinar Grafika, p. 160.

criminal justice system yang memadukan berbagai disiplin ilmu, termasuk digital forensik untuk analisis data dan forensik tradisional untuk barang bukti fisik.

Penggunaan landasan hukum dalam kasus ini merujuk pada Pasal 46 ayat (1) juncto Pasal 30 Undang-Undang ITE. Pasal 30 UU ITE mengatur larangan terhadap tindakan akses secara tidak sah (unauthorized access) terhadap sistem elektronik, sementara Pasal 46 ayat (1) memberikan dasar penerapan sanksi pidana dengan ancaman pidana penjara dan/atau denda. Selain itu, penyidikan juga merujuk pada Pasal 55 dan Pasal 56 KUHP sebagai landasan pertanggungjawaban pidana bagi pihak yang terlibat secara tidak langsung.

Data yang berhasil dikumpulkan menunjukkan bahwa dari aksi skimming selama sekitar tiga jam, pelaku berhasil mencuri data 81 nasabah. Data tersebut diolah menggunakan laptop dan dikirimkan melalui aplikasi *Team Viewer* ke jaringan bos mereka di Malaysia. Temuan bukti pengiriman peralatan *skimming* dari Malaysia melalui DHL Express mengindikasikan keterlibatan jaringan kejahatan transnasional yang memerlukan koordinasi lintas yurisdiksi.

Proses pengumpulan alat bukti ini menunjukkan penerapan *Crime Control Model* dalam teori sistem peradilan pidana, di mana kepolisian bertindak cepat untuk mencegah pelaku melarikan diri atau menghilangkan bukti.[26] Namun, pendekatan ini diimbangi dengan Due Process Model yang memastikan prosedur hukum diikuti secara ketat, tercermin dalam penerbitan surat perintah penyitaan dan penangkapan yang sesuai ketentuan KUHAP.

Kendala yang Dihadapi Penyidik dalam Pengumpulan Alat Bukti

Penyidikan kasus skimming ATM menghadapi berbagai kendala yang kompleks, yang dapat dianalisis menggunakan teori efektivitas hukum Soerjono Soekanto. Kendala pertama adalah kompleksitas teknologi dan modus operandi pelaku yang semakin canggih. Pelaku menggunakan peralatan skimming yang dirancang khusus untuk menyatu dengan desain mesin ATM, sehingga hampir tidak terdeteksi oleh mata awam. Selain itu, penggunaan aplikasi Team Viewer memungkinkan pengiriman data secara *real-time* ke server luar negeri dengan jejak digital yang dapat terhapus seketika.

Permasalahan mendasar dalam penyidikan *cyber crime* dimulai dari keterbatasan alat dan keahlian forensik digital. Tidak semua penyidik memiliki kompetensi dalam menganalisis perangkat elektronik yang disita, mengingat forensik digital adalah bidang khusus yang membutuhkan pelatihan intensif. Penyidik sering bergantung pada bantuan pihak ketiga atau lembaga khusus yang memiliki ahli forensik digital, yang dapat menghambat penyelesaian kasus. Permasalahan semakin kompleks ketika menghadapi data yang telah dienkripsi atau dihapus oleh pelaku, yang memerlukan teknologi canggih seperti perangkat *decryption* atau alat data *recovery* tingkat tinggi.

Bersamaan dengan keterbatasan teknologi, koordinasi dengan lembaga lain menjadi tantangan tersendiri, terutama dalam kasus yang melibatkan lintas yurisdiksi. Kerja sama dengan Interpol atau pihak berwenang di Malaysia menghadapi kendala birokrasi yang rumit dan memakan waktu lama. Di tingkat lokal, kerja sama dengan Bank BNI dalam mengakses data transaksi dan rekaman CCTV juga terkendala oleh prosedur internal bank yang ketat terkait kerahasiaan nasabah. Perbedaan sistem hukum dan kebijakan antara Indonesia dan Malaysia juga menjadi penghambat dalam koordinasi, terutama dalam proses ekstradisi pelaku.

Selain masalah koordinasi, keterbatasan sumber daya manusia dan logistik turut memperburuk situasi. Jumlah personel penyidik yang terbatas tidak sebanding dengan tingginya beban kerja, sehingga memengaruhi kedalaman dan kualitas penyelidikan. Kurangnya alat pendukung seperti perangkat lunak analisis data dan sarana transportasi operasional juga menghambat efektivitas penyidikan. Minimnya personel dan alat pendukung membuat upaya patroli atau sosialisasi menjadi kurang optimal.

[26] Lamintang, P. A. F. *Loc.Cit.*

Tantangan lain yang tidak kalah signifikan berkaitan dengan dinamika pelaku dan perlindungan data. Pelaku sering mengubah modus operandi dan menggunakan identitas palsu atau nama samaran untuk menghindari deteksi. Penggunaan platform komunikasi dengan fitur enkripsi *end-to-end* dan penghapusan riwayat percakapan setelah transaksi menyulitkan penyidik dalam mengumpulkan bukti digital. Selain itu, penyidik harus memproses data korban tanpa melanggar hak privasi mereka, sesuai dengan Undang-Undang Perlindungan Data Pribadi.

Dari segi hukum dan pembuktian, kompleksitas meningkat karena pembuktian unsur pidana dalam kasus *cyber crime* memerlukan alat bukti elektronik yang sah secara hukum. Berbeda dengan kasus konvensional, bukti digital harus memenuhi standar hukum agar dapat diakui di pengadilan, yang melibatkan konversi data digital ke dalam bentuk yang dapat diterima secara hukum. Validasi bukti elektronik memerlukan peran ahli forensik digital yang tersertifikasi, namun ketersediaan ahli tersebut masih terbatas.

Masalah dalam proses penyidikan juga muncul dari peran saksi dan keterangan yang tidak konsisten. Saksi sering memberikan keterangan yang tidak lengkap atau tidak konsisten karena berbagai faktor seperti ketakutan, tekanan psikologis, atau kurangnya pemahaman tentang hukum. Dalam kasus ini, Satria Wibowo awalnya menyangkal keterlibatannya sebelum akhirnya mengaku, yang menunjukkan dinamika perubahan keterangan saksi. Ketidakkonsistenan ini menimbulkan tantangan besar bagi penyidik dalam memverifikasi setiap pernyataan dan membandingkannya dengan bukti lain.

Pengelolaan barang bukti fisik menambah kompleksitas dalam proses penyidikan. Barang bukti yang sangat banyak dan beragam jenisnya memerlukan penanganan khusus untuk mencegah kerusakan atau kehilangan. Barang bukti elektronik sangat rentan terhadap kerusakan jika tidak ditangani sesuai prosedur yang benar, seperti paparan medan magnet, suhu ekstrem, atau kesalahan teknis. Tanpa sistem pencatatan yang baik, barang bukti bisa tertukar, tertinggal, atau bahkan dicuri.

Akhirnya, faktor eksternal berupa tekanan waktu dan publikasi media turut mempersulit proses penyidikan. Penyidik sering menghadapi tekanan untuk menyelesaikan kasus dengan cepat, yang dapat memaksa mereka mengambil langkah instan tanpa mempertimbangkan kelengkapan investigasi. Pemberitaan media yang intensif dapat menciptakan tekanan psikologis pada penyidik dan berpotensi memberikan informasi kepada pelaku untuk menghancurkan atau memanipulasi bukti.

Upaya Mengatasi Kendala Pengumpulan Alat Bukti

Dalam mengatasi berbagai kendala yang dihadapi, penyidik Satreskrim Polresta Padang telah melakukan sejumlah upaya strategis yang dapat dianalisis berdasarkan teori penegakan hukum. Upaya pertama adalah peningkatan kapasitas forensik digital melalui pelatihan intensif bagi personel dalam teknik analisis perangkat elektronik, pemulihan data yang terenkripsi, dan penggunaan alat *decryption* serta data *recovery*. Penyidik juga berkoordinasi dengan laboratorium forensik digital pusat yang memiliki ahli dan peralatan canggih untuk memastikan proses analisis bukti digital dapat dilakukan lebih cepat dan akurat. Selain pelatihan, dilakukan pengadaan alat forensik digital yang mutakhir melalui kerja sama dengan pemerintah pusat dan pemangku kepentingan terkait. Perangkat lunak dan perangkat keras yang diperlukan, seperti alat untuk melacak jejak digital atau memecahkan enkripsi, dianggarkan untuk meningkatkan kemandirian penyidik dalam menangani kasus kejahatan siber.

Selanjutnya, diperlukan optimalisasi koordinasi dengan lembaga lain menjadi prioritas utama, terutama dalam kasus yang melibatkan lintas yurisdiksi. Penyidik memperkuat kerja sama dengan Interpol dan otoritas Malaysia melalui saluran resmi seperti permintaan bantuan hukum timbal balik (*Mutual Legal Assistance*). Untuk mempercepat proses, semua dokumen permohonan disiapkan secara lengkap dan sesuai prosedur untuk menghindari kendala

birokrasi. Di tingkat lokal, penyidik menjalin komunikasi intensif dengan Bank BNI untuk mengakses data transaksi dan rekaman CCTV, dengan pendekatan persuasif dan pemahaman terhadap regulasi perlindungan data, penyidik berhasil mempercepat proses verifikasi permintaan data. Kerja sama dengan akademisi dan industri teknologi juga ditingkatkan untuk mendapatkan wawasan terbaru tentang perkembangan kejahatan siber.

Seiring dengan peningkatan koordinasi, pemanfaatan teknologi untuk pengumpulan dan analisis bukti menjadi fokus penting berikutnya. Penyidik menggunakan perangkat lunak analisis data untuk melacak pola transaksi mencurigakan atau aliran dana ilegal. Alat pelacakan alamat IP dan VPN digunakan untuk mengidentifikasi pelaku yang bersembunyi di balik jaringan anonim. Sistem *backup* digital untuk barang bukti elektronik juga dikembangkan untuk mencegah kerusakan atau kehilangan data. Berkaitan dengan pengelolaan bukti, peningkatan pengelolaan barang bukti fisik dilakukan melalui penerapan sistem manajemen yang ketat.

Setiap barang bukti didokumentasikan dengan detail, diberi label, dan disimpan dalam lingkungan terkendali. Teknologi seperti *barcode* atau *QR code* digunakan untuk memudahkan pelacakan, sementara kerja sama dengan laboratorium forensik memastikan barang bukti elektronik diperiksa dengan prosedur yang benar. Dalam aspek penanganan saksi, pelatihan khusus diterapkan untuk menangani saksi dan keterangan yang tidak konsisten. Penyidik dilatih dalam teknik interogasi dan wawancara yang efektif, termasuk pendekatan psikologis untuk mengurangi ketakutan atau tekanan pada saksi. Rekaman CCTV atau bukti digital digunakan untuk memverifikasi keterangan saksi sehingga dapat membangun kronologi kejadian yang akurat.

Untuk mengatasi faktor eksternal, penanganan tekanan media dan waktu menjadi perhatian khusus. Penyidik menerapkan prinsip transparansi terbatas, di mana informasi yang dibagikan kepada media dikontrol untuk mencegah gangguan investigasi. Penyidik bekerja secara sistematis dan tidak terburu-buru, memastikan semua bukti terkumpul sebelum mengambil tindakan lebih lanjut. Selain penanganan reaktif, pendekatan preventif juga diterapkan melalui sosialisasi dan pencegahan kejahatan kepada masyarakat dan nasabah bank tentang modus skimming dan cara melindungi data pribadi.

Patroli intensif di lokasi ATM rentan juga ditingkatkan untuk mencegah aksi pelaku, program edukasi keamanan digital dilakukan secara berkala melalui media sosial, spanduk di bank, atau seminar keamanan digital untuk meningkatkan kewaspadaan masyarakat. Implementasi upaya-upaya tersebut mencerminkan penerapan teori penegakan hukum yang holistik, di mana tidak hanya fokus pada aspek represif tetapi juga preventif. Pendekatan multidisiplin yang melibatkan berbagai stakeholder, dari penegak hukum hingga masyarakat, menunjukkan pemahaman bahwa kejahatan siber memerlukan penanganan yang komprehensif. Kerja sama antara pemerintah, lembaga penegak hukum, sektor perbankan, dan masyarakat menjadi kunci utama dalam pencegahan dan penanggulangan kejahatan serupa.

Implementasi upaya-upaya tersebut mencerminkan penerapan teori penegakan hukum yang holistik, di mana tidak hanya fokus pada aspek represif tetapi juga preventif. Pendekatan multidisiplin yang melibatkan berbagai stakeholder, dari penegak hukum hingga masyarakat, menunjukkan pemahaman bahwa kejahatan siber memerlukan penanganan yang komprehensif. Kerja sama antara pemerintah, lembaga penegak hukum, sektor perbankan, dan masyarakat menjadi kunci utama dalam pencegahan dan penanggulangan kejahatan serupa.

Efektivitas upaya-upaya yang dilakukan dapat dievaluasi dari perspektif teori sistem peradilan pidana yang menekankan pada koordinasi dan sinkronisasi komponen peradilan pidana. Keberhasilan penanganan kasus skimming ATM Bank BNI Cabang Padang menunjukkan bahwa meskipun menghadapi berbagai kendala, sistem peradilan pidana mampu beradaptasi dengan perkembangan teknologi melalui peningkatan kapasitas dan koordinasi antarlembaga.

Namun demikian, upaya-upaya yang telah dilakukan masih perlu terus dikembangkan dan disempurnakan. Tantangan kejahatan siber yang terus berkembang memerlukan respon yang dinamis dan adaptif dari seluruh komponen sistem peradilan pidana.[27] Investasi dalam teknologi, pelatihan sumber daya manusia, dan penguatan kerja sama internasional menjadi prioritas utama dalam menghadapi ancaman kejahatan siber di masa depan.

Dari perspektif teori penegakan hukum Wayne La-Fave, upaya yang dilakukan penyidik menunjukkan penerapan diskresi yang tepat dalam menghadapi keterbatasan sumber daya dan kompleksitas kasus.[28] Penyidik tidak hanya mengandalkan aspek normatif hukum, tetapi juga mempertimbangkan aspek praktis dan keterbatasan yang ada dalam mengoptimalkan penegakan hukum.

Keseluruhan upaya yang dilakukan oleh penyidik Satreskrim Polresta Padang mencerminkan evolusi penegakan hukum di era digital, di mana metode konvensional harus dipadukan dengan pendekatan teknologi modern. Hal ini sejalan dengan prinsip bahwa penegakan hukum harus dapat beradaptasi dengan perkembangan zaman tanpa mengorbankan prinsip-prinsip dasar keadilan dan due process of law.[29]

KESIMPULAN

Berdasarkan pembahasan yang telah diuraikan, dapat disimpulkan beberapa hal penting terkait penyidikan tindak pidana pencurian informasi data melalui *skimming* ATM Bank BNI Cabang Padang. *Pertama*, proses pengumpulan alat bukti dilakukan melalui lima tahap sistematis yang mencerminkan penerapan teori sistem peradilan pidana: penangkapan dan penahanan berdasarkan surat perintah yang sah, penyitaan barang bukti yang komprehensif mencakup perangkat fisik dan digital, pemeriksaan saksi dari berbagai pihak terkait, pemeriksaan tersangka yang mengungkap struktur organisasi kejahatan, dan analisis alat bukti yang mengintegrasikan forensik digital dan konvensional.

Kedua, kendala yang dihadapi penyidik sangat kompleks dan multidimensional, meliputi kompleksitas teknologi pelaku yang semakin canggih, keterbatasan alat dan keahlian forensik digital, kesulitan koordinasi dengan lembaga lain terutama lintas yurisdiksi, keterbatasan sumber daya manusia dan logistik, dinamika pelaku dan isu perlindungan data, kendala hukum dan pembuktian dalam konteks cyber crime, inkonsistensi keterangan saksi, masalah pengelolaan barang bukti fisik, serta tekanan eksternal dari media dan waktu[108]. Kendala-kendala ini mencerminkan lima faktor yang mempengaruhi efektivitas penegakan hukum menurut teori Soerjono Soekanto.

Ketiga, upaya mengatasi kendala dilakukan secara holistik melalui peningkatan kapasitas forensik digital dengan pelatihan intensif dan pengadaan alat canggih, optimalisasi koordinasi dengan lembaga dalam dan luar negeri, pemanfaatan teknologi modern untuk pengumpulan dan analisis bukti, peningkatan sistem pengelolaan barang bukti, pelatihan khusus penanganan saksi, manajemen faktor eksternal, dan program sosialisasi serta pencegahan. Upaya-upaya ini mencerminkan penerapan *Crime Control Model* yang diimbangi dengan *Due Process Model* dalam teori sistem peradilan pidana.

Kasus skimming ATM Bank BNI Cabang Padang menunjukkan bahwa penegakan hukum di era digital memerlukan pendekatan multidisiplin yang mengintegrasikan aspek hukum, teknologi, dan koordinasi antarlembaga. Keberhasilan penyidikan tidak hanya ditentukan oleh penguasaan teknologi, tetapi juga kemampuan adaptasi sistem peradilan pidana dalam menghadapi perkembangan modus operandi kejahatan siber.

---

[27] Gabriel, A., Pinasang, D. R., & Bawole, H. Y. A. *Op.Cit.,* p. 15

[28] Rahardjo, S. (2010). *Sosiologi Hukum Perkembangan Metode Dan Pilihan Masalah*. Yogyakarta: Genta Publishing, pp. 191-192.

[29] Harahap, M. Y., *Op.Cit.,* p. 106.

Penelitian ini memberikan kontribusi terhadap pengembangan ilmu hukum pidana, khususnya dalam konteks penegakan hukum *cyber crime*, serta memberikan masukan praktis bagi aparat penegak hukum dalam menangani kasus serupa di masa depan. Diperlukan komitmen berkelanjutan dari semua pihak untuk terus meningkatkan kapasitas penegakan hukum dalam menghadapi tantangan kejahatan siber yang terus berkembang.

DAFTAR PUSTAKA

Abdul Wahid dan Mohamad Latib. (2005). *Kejahatan Mayantara*. Bandung: Rafika Aditama.

Adami Chazawi. (2003). *Kejahatan Terhadap Harta Benda*. Malang: Bayumedia.

Andi Hamzah. (2004). *Asas-Asas Hukum Pidana*. Jakarta: Rineka Cipta.

Angelica Gabriel, Dani Robert Pinasang dan Herlyanty Y.A. Bawole. "Penegakan Hukum Terhadap Kejahatan Skimming Atm Berdasarkan Undang-Undang Nomor 19 Tahun 2016 Tentang Perubahan Atas Undang-Undang Nomor 11 Tahun 2008 Tentang Informasi Dan Transaksi Elektronik." *Lex Privatum* 13, no. 5 (2024): 1-15.

Barda Nawawi Arief. (2006). *Tindak Pidana Mayantara Perkembangan Kajian Cybercrime di Indonesia*. Jakarta: RajaGrafindo Persada.

Bryan A. Garner. (2009). *Black's Law Dictionary. Ninth Edition*. St. Paul: Thomson Reuters.

Budi Suhariyanto. (20313). *Tindak Pidana Teknologi Informasi (Cybercrime): Urgensi Pengaturan dan Celah Hukumnya*, Jakarta: Rajawali Pers

Didik M, Arief Mansur dan Elisatris Gultom. (2005). *Cyber Law Aspek Hukum Teknologi Informasi*. Bandung: Refika Aditama.

Hamzah Mardiansyah, Kastubi, Agus Wibowo, Aribandi, dan Markus Suryoutomo. "Penyidikan Tindak Pidana Pencurian dengan Kekerasan: Perspektif Kebijakan Kepolisian." *Jurnal Kolaboratif Sains* 8, no. 2 (2024): 1130-1140.

Jovin Ganda Ramdhan dan Sumiyati. "Perlindungan Hukum Terhadap Nasabah Korban Skimming Ditinjau Dari Undang Undang Nomor 8 Tahun 1999." *Jurnal Ilmu Hukum* 12, no. 1 (2019): 75-85.

Kristan dan Yopi Gunawan. (2013). *Sekelumit Tentang Penyadapan Dalam Hukum Positif di Indonesia*. Bandung: Nuansa Aulia

Leden Marpaung. (2011). *Proses Penanganan Perkara Pidana: Penyidikan Dan Penyelidikan*. Jakarta: Sinar Grafika.

M. Yahya Harahap. (2007). *Pembahasan Dan Penerapan KUHAP Penyidikan Dan Penuntutan*. Jakarta: Sinar Grafika.

Peter Mahmud Marzuki. (2011). *Penelitian Hukum*. Jakarta: Prenadamedia.

Republik Indonesia. *Undang-Undang Nomor 19 Tahun 2016 tentang Perubahan Atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik*. Lembaran Negara Republik Indonesia Tahun 2016 Nomor 251.

Republik Indonesia. *Undang-Undang Nomor 8 Tahun 1981 tentang Hukum Acara Pidana*. Lembaran Negara Republik Indonesia Tahun 1981 Nomor 76.

Romli Atmasasmita. (1996). *Sistem Peradilan Pidana (Criminal Justice System) Perspektif Ekstensialisme dan Abolisionisme*. Bandung: Bina Cipta.

Satjipto Rahardjo. (2010). *Sosiologi Hukum Perkembangan Metode Dan Pilihan Masalah*. Yogyakarta: Genta Publishing.

Soerjono Soekanto. (2021). *Faktor-Faktor Yang Mempengaruhi Penegakan Hukum*. Jakarta: Rajawali Press.