JISPENDIORA: Jurnal Ilmu Sosial, Pendidikan dan Humaniora
Volume 3, Nomor 3, Desember 2024
E-ISSN: 2829-3886; P-ISSN: 2829-3479, Hal. 119-132
DOI: https://doi.org/10.56910/jispendiora.v3i3.2949
Available Online at: https://jurnal-stiepari.ac.id/index.php/jispendiora

Kekuatan Digital Forensik dalam Mengungkap Tindak Pidana *Cyber Crime* (Studi Kasus : *Hacker Ilegal* Akses Pembayaran Kereta *Commuter* Indonesia (KCI)

Ira Irmansyah
Magister Hukum Universitas Pancasila, Menteng, Jakarta Pusat, Indonesia

Korespondensi penulis: irairman5223002@univpancasila.ac.id

Abstract. *This research discusses the strategic role of digital forensics in uncovering cyber crime with a case study of the hacking of the Multi Trip Card (KMT) payment system owned by the Indonesian Commuter Train (KCI). This case involves perpetrators who use illegal software to manipulate digital balances on KMT cards, so that they only pay a small amount but get a large balance. This phenomenon causes financial losses as well as threats to public trust in electronic payment systems. The research method used is qualitative descriptive with a case study approach. The analysis was carried out on various digital traces, ranging from server logs, transaction records, to metadata that becomes electronic evidence. Digital forensics plays a role in the process of identifying, collecting, securing and analyzing data to ensure the validity of evidence. The findings suggest that electronic evidence can have legal force if obtained through lawful procedures, for example by using chains of custody and standardized forensic analysis methods. In addition, this study highlights the weakness of digital security systems that are a loophole for cybercriminals. Digital forensics is not only important in the investigation stage, but also as a means of security evaluation to anticipate similar crimes. Law enforcement against cases like this requires collaboration between law enforcement officials, forensic experts, digital service providers, and regulators. The application of the latest security technologies, such as data encryption, anomaly detection systems, and periodic audits, is considered to be able to minimize the potential for manipulation. The implication of this research is the need to increase awareness, strengthen regulations, and technological innovation in dealing with the development of cyber crime. Digital forensics is proving to be a vital instrument that not only supports investigations, but also maintains the integrity of digital systems.*

Keywords: *Evidence, Cyber, Digital, Forensics, Security.*

Abstrak. Penelitian ini membahas peran strategis digital forensik dalam mengungkap tindak pidana cyber crime dengan studi kasus peretasan sistem pembayaran Kartu Multi Trip (KMT) milik Kereta Commuter Indonesia (KCI). Kasus ini melibatkan pelaku yang menggunakan perangkat lunak ilegal untuk memanipulasi saldo digital pada kartu KMT, sehingga hanya membayar nominal kecil namun mendapatkan saldo besar. Fenomena ini menimbulkan kerugian finansial serta ancaman terhadap kepercayaan publik terhadap sistem pembayaran elektronik. Metode penelitian yang digunakan adalah deskriptif kualitatif dengan pendekatan studi kasus. Analisis dilakukan terhadap berbagai jejak digital, mulai dari log server, rekaman transaksi, hingga metadata yang menjadi bukti elektronik. Digital forensik berperan dalam proses identifikasi, pengumpulan, pengamanan, dan analisis data untuk memastikan keabsahan bukti. Temuan menunjukkan bahwa bukti elektronik dapat memiliki kekuatan hukum jika diperoleh melalui prosedur sah, misalnya dengan menggunakan chain of custody dan metode analisis forensik yang terstandarisasi. Selain itu, penelitian ini menyoroti lemahnya sistem keamanan digital yang menjadi celah bagi pelaku kejahatan siber. Digital forensik tidak hanya penting dalam tahap investigasi, tetapi juga sebagai sarana evaluasi keamanan untuk mengantisipasi kejahatan serupa. Penegakan hukum terhadap kasus seperti ini membutuhkan kolaborasi antara aparat penegak hukum, pakar forensik, penyedia layanan digital, serta regulator. Penerapan teknologi keamanan terbaru, seperti enkripsi data, sistem deteksi anomali, dan audit berkala, dinilai mampu meminimalisasi potensi manipulasi. Implikasi penelitian ini adalah perlunya peningkatan kesadaran, penguatan regulasi, dan inovasi teknologi dalam menghadapi perkembangan cyber crime. Digital forensik terbukti menjadi instrumen vital yang tidak hanya mendukung investigasi, tetapi juga menjaga integritas sistem digital.

Kata Kunci: Bukti, Cyber, Digital, Forensik, Keamanan.

Received: November 14, 2024; Revised: November 28, 2024; Accepted: Desember 16, 2024;
Published: Desember 30, 2024

1. PENDAHULUAN

Pesatnya perkembangan teknologi informasi dan komunikasi telah memberikan pengaruh yang besar terhadap berbagai bidang kehidupan, salah satunya sektor transportasi. Digitalisasi sistem pembayaran, seperti yang diterapkan pada Kereta Commuter Indonesia, menawarkan kemudahan dan efisiensi bagi masyarakat. Namun, di sisi lain, kemajuan ini juga membuka peluang bagi tindak pidana siber (*cyber crime*), seperti tindakan peretasan dan akses ilegal yang dapat merugikan institusi maupun pengguna layanan.

Kasus peretasan pada sistem pembayaran Kartu Multi Trip (KMT) milik KAI Commuter Indonesia merupakan salah satu contoh nyata ancaman keamanan siber di sektor transportasi publik. Kejadian ini terjadi pada akhir Februari 2024, di mana pelaku berhasil mengeksploitasi celah keamanan dalam aplikasi C-Access, sebuah platform yang memungkinkan pengguna untuk mengisi ulang saldo KMT. Dengan menggunakan perangkat lunak pihak ketiga seperti HttpCanary, pelaku mengubah proses pembayaran digital sehingga hanya perlu membayar nominal kecil, yakni Rp25, tetapi mendapatkan saldo hingga Rp12 juta melalui 25 transaksi ilegal dalam waktu tiga hari.

Modus yang digunakan cukup kompleks dan menunjukkan tingkat kecanggihan yang tinggi dalam memahami sistem digital. Pelaku mengatur ulang data pembayaran sehingga sistem membaca tagihan administrasi hanya Rp1. Transaksi ini dilakukan melalui aplikasi dompet digital seperti GoPay yang terintegrasi dengan C-Access. Dengan memanipulasi mekanisme top-up, pelaku tidak hanya berhasil merugikan KAI Commuter secara finansial tetapi juga menunjukkan adanya kelemahan serius dalam keamanan siber di aplikasi tersebut.

Tindakan ini terungkap setelah laporan resmi dilayangkan ke pihak kepolisian pada awal Maret 2024. Penyelidikan yang dilakukan oleh Polres Metro Depok mengungkap bukti kuat berupa perangkat yang digunakan pelaku, termasuk ponsel pintar, kartu KMT, kartu SIM, dan aplikasi yang terkait dengan aktivitas peretasan. Berdasarkan temuan ini, pelaku diancam dengan Pasal 33 juncto Pasal 49 serta Pasal 30 juncto Pasal 46 dalam Undang-Undang Nomor 1 Tahun 2024, yang menggantikan Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (ITE). Hukuman yang dapat dijatuhkan mencapai 10 tahun penjara.

Menanggapi insiden ini, KAI Commuter menyatakan komitmennya untuk memperkuat sistem keamanan informasi dengan mengadopsi standar internasional ISO 27001:2013. Standar ini mencakup audit berkala oleh auditor independen untuk memastikan sistem tetap terlindungi dari potensi serangan siber di masa depan. Perusahaan juga berkolaborasi dengan pihak kepolisian untuk menyelesaikan kasus ini secara tuntas sekaligus mengupayakan pencegahan agar kejadian serupa tidak terulang. Langkah-langkah penguatan meliputi peningkatan sistem

keamanan, evaluasi terhadap potensi celah dalam aplikasi, dan edukasi kepada pengguna untuk lebih waspada dalam menggunakan teknologi berbasis digital.

Kasus ini menjadi pengingat pentingnya perlindungan terhadap data dan sistem digital, terutama di era digitalisasi yang semakin masif. Dari kejadian ini, kita dapat belajar bahwa kolaborasi antara sektor swasta, pemerintah, dan masyarakat sangat diperlukan untuk menangani ancaman siber. Dengan langkah-langkah proaktif, insiden semacam ini diharapkan tidak hanya bisa dihindari tetapi juga mendorong pengembangan teknologi yang lebih aman dan tepercaya.

Cyber crime dalam bentuk hacking dan akses ilegal terhadap sistem pembayaran menjadi tantangan serius, mengingat kerentanan sistem digital terhadap serangan tersebut. Insiden ini tidak hanya mengancam keamanan data, tetapi juga integritas sistem pembayaran yang berbasis digital. Salah satu jenis ancaman yang sering muncul adalah penyalahgunaan celah keamanan oleh pihak-pihak yang tidak bertanggung jawab untuk mendapatkan keuntungan finansial dengan cara ilegal.

Digital forensik memainkan peran penting sebagai alat untuk mengungkap jejak digital pelaku kejahatan. Dengan teknik dan metode analisis yang canggih, digital forensik dapat mengidentifikasi, mengumpulkan, dan menganalisis bukti elektronik yang menjadi kunci dalam mengungkap kejahatan ini. Kemampuan digital forensik untuk melacak aktivitas siber, termasuk peretasan dan akses ilegal, memberikan kontribusi besar dalam memastikan penegakan hukum yang efektif serta mencegah kejadian serupa di masa depan.

Penelitian ini bertujuan untuk menganalisis peran digital forensik dalam mengungkap kasus kejahatan siber, terutama yang berkaitan dengan peretasan dan akses ilegal pada sistem pembayaran Kereta Commuter Indonesia. Melalui studi ini, diharapkan dapat memberikan pemahaman yang lebih mendalam mengenai fungsi digital forensik sebagai sarana penting dalam menangani tindak kejahatan siber serta berkontribusi pada penguatan sistem keamanan digital di Indonesia.

2. METODE PENELITIAN

Dalam rangka menjawab rumusan masalah tersebut, penelitian ini mengadopsi pendekatan deskriptif kualitatif dengan metode studi kasus. Pendekatan ini memungkinkan penelitian untuk mengeksplorasi secara mendalam fenomena kejahatan siber pada sistem pembayaran digital KAI Commuter Indonesia, dengan penekanan pada analisis forensik digital dan aspek keamanan siber. Data yang diperoleh akan dianalisis secara tematik untuk mengidentifikasi pola, hubungan, dan implikasi terkait kejahatan siber dan keamanan digital.

Analisis akan dilakukan menggunakan dokumen laporan kasus, berita terkait, publikasi akademik tentang keamanan digital, dan literatur mengenai digital forensik. Dengan demikian, hasil penelitian ini diharapkan tidak hanya bersifat akademis tetapi juga aplikatif bagi pengembangan kebijakan dan praktik keamanan digital di Indonesia.

3. PEMBAHASAN

Pembuktian Tindak Pidana *Cyber crime* di Indonesia

Perkembangan pesat teknologi komunikasi berbasis internet telah mengubah banyak aspek kehidupan, mulai dari mempermudah komunikasi hingga meningkatkan efisiensi di berbagai bidang. Namun, kemajuan ini juga memunculkan tantangan besar berupa munculnya berbagai jenis kejahatan siber (*cyber crime*) yang menggunakan internet sebagai media utama. Fenomena ini terjadi karena internet memungkinkan interaksi virtual tanpa batas geografis dan fisik, sehingga pelaku kejahatan dapat melakukan tindakan ilegal tanpa mudah terdeteksi. Karakteristik dunia maya yang anonim dan terdesentralisasi mempermudah pelaku untuk menghapus jejak digital mereka, sehingga identitas mereka sering kali sulit dilacak oleh penegak hukum.

Salah satu jenis kejahatan yang semakin sering terjadi adalah kejahatan komputer (*computer crime*), yang dikenal luas dengan istilah *cyber crime*. Kejahatan ini mencakup berbagai aktivitas ilegal, seperti peretasan, pencurian data, manipulasi sistem, hingga penyebaran malware, yang semuanya memanfaatkan celah keamanan pada jaringan komputer. Fenomena ini menjadi lebih kompleks karena dunia saat ini seolah menjadi tanpa batas ("*borderless*"), di mana informasi, peristiwa, termasuk tindak kejahatan, dapat menyebar secara real-time ke seluruh penjuru dunia. Teknologi informasi yang berkembang pesat ini ibarat membuat dunia "mengecil", menghadirkan peluang dan risiko yang sama besar.

Menghadapi kejahatan siber, salah satu tantangan utama adalah proses pembuktian tindak pidana. Dalam konteks hukum pidana, pembuktian adalah aspek krusial dalam proses peradilan karena berpengaruh pada keputusan terhadap terdakwa. Pembuktian mencakup prosedur yang sah secara hukum untuk membuktikan kebenaran tuduhan, serta bukti-bukti yang diakui dan diterima oleh undang-undang. Proses ini berperan penting karena jika pembuktian gagal, terdakwa dapat dibebaskan. Sebaliknya, jika bukti cukup, terdakwa dapat dinyatakan bersalah dan dijatuhi hukuman.

Proses pembuktian biasanya dimulai sejak adanya indikasi peristiwa pidana. Penyelidikan dilakukan untuk mencari tahu apakah suatu peristiwa dapat dikategorikan sebagai tindak pidana. Penyidikan selanjutnya dilakukan untuk mengumpulkan bukti yang relevan, sesuai dengan ketentuan dalam Pasal 1 angka 13 Undang-Undang Nomor 2 Tahun 2002 tentang

Kepolisian. Dalam kasus kejahatan siber, bukti digital seperti log data, metadata, dan dokumen elektronik sangat vital. Pasal 5 Undang-Undang Informasi dan Transaksi Elektronik (UU ITE) secara tegas menyatakan bahwa informasi elektronik beserta hasil cetaknya dapat dijadikan bukti yang sah di pengadilan.

Cyber crime memiliki ciri khas yang membedakannya dari kejahatan konvensional, termasuk dalam hal pelaku, korban, modus operandi, dan tempat kejadian. Oleh karena itu, dibutuhkan pendekatan serta peraturan khusus yang di luar cakupan Kitab Undang-Undang Hukum Pidana (KUHP) untuk menangani masalah ini. Perkembangan teknologi yang cepat mengharuskan sistem hukum untuk lebih fleksibel dan responsif terhadap perubahan yang terjadi di dunia maya. Dalam hal ini, kepolisian sebagai aparat penegak hukum memiliki peran penting, mulai dari penyelidikan awal hingga pengumpulan bukti yang sah untuk diajukan di pengadilan.

Keberhasilan penanganan *cyber crime* juga sangat bergantung pada kemampuan aparat untuk menggunakan alat dan metode forensik digital. Digital forensik menjadi elemen penting dalam mengungkap bukti elektronik yang dapat memberikan petunjuk atas identitas pelaku, kronologi kejadian, serta modus operandi yang digunakan. Proses ini melibatkan pengumpulan, analisis, dan pelaporan bukti digital dengan standar tertentu, seperti yang diatur oleh panduan internasional.

Keberadaan tindak pidana siber (cyber crime) yang memanfaatkan internet sebagai sarana utama menimbulkan tantangan besar bagi aparat penegak hukum, terutama dalam hal mengidentifikasi, melacak, dan mengumpulkan bukti yang cukup untuk membuktikan kesalahan pelaku. Kesulitan ini disebabkan oleh sifat dunia maya yang anonim, dengan data jaringan internet atau komputer sering kali sulit diakses atau dilindungi oleh enkripsi canggih. Pelaku kejahatan, baik yang menyediakan layanan internet maupun yang memanfaatkan jaringan untuk aktivitas ilegal seperti perjudian online, sering kali dapat dengan mudah menghapus atau menyembunyikan jejak digital mereka, membuat proses investigasi semakin kompleks.

Ketika terdapat indikasi awal terjadinya tindak pidana, penyelidikan dimulai untuk menentukan apakah kasus tersebut dapat dilanjutkan ke tahap penyidikan. Berdasarkan Pasal 1 angka 13 Undang-Undang Nomor 2 Tahun 2002 tentang Kepolisian, penyidikan mencakup serangkaian langkah untuk mengumpulkan bukti yang memadai guna mengungkap kejadian tindak pidana dan mengidentifikasi pelakunya.

Dalam penyelidikan kejahatan siber, penyidik menggunakan berbagai alat investigasi yang telah menjadi standar, di antaranya :

1. Pengumpulan Informasi

   Informasi dasar dikumpulkan melalui observasi tempat kejadian perkara (*crime scene search*) dan analisis perangkat elektronik, seperti komputer dan ponsel. Proses ini dapat mencakup analisis bukti elektronik yang ada di hard disk atau memori komputer untuk menemukan data relevan yang berkaitan dengan kasus yang sedang diselidiki.
2. Wawancara dan Interogasi

   Proses wawancara melibatkan pengumpulan informasi dari saksi, korban, atau pihak lain yang memiliki kaitan dengan kasus. Sedangkan interogasi dilakukan kepada tersangka menggunakan pendekatan-pendekatan seperti logis (meyakinkan tersangka melalui alasan rasional), indifference (berpura-pura memiliki cukup bukti untuk memancing pengakuan), dan *facing-saving approach* (memahami alasan tersangka melakukan tindakannya).
3. Penggunaan Teknologi

   Teknologi forensik digital menjadi alat penting dalam investigasi *cyber crime*. Teknik data recovery digunakan untuk memulihkan informasi yang telah dihapus atau rusak. Selain itu, teknologi canggih lainnya, seperti analisis jaringan dan log digital, diterapkan untuk mengumpulkan dan memverifikasi bukti elektronik.
4. Penyusunan Laporan Kasus

   Setelah bukti dikumpulkan, penyidik menyusun laporan yang mencakup laporan penyelidikan, penyidikan, dokumentasi bukti elektronik, hasil laboratorium forensik, pernyataan tertulis saksi dan tersangka, serta rekaman dan foto tempat kejadian perkara.
5. Pemeriksaan Berkas oleh Jaksa Penuntut Umum

   Berkas perkara diperiksa untuk memastikan kelengkapan bukti dan validitas fakta. Apabila ditemukan kekurangan, jaksa akan memberikan petunjuk kepada penyidik untuk melengkapi data sebelum kasus diserahkan ke pengadilan.
6. Proses Penuntutan

   Jaksa menyusun surat dakwaan dengan merujuk pada bukti yang sah, sesuai dengan ketentuan Pasal 183 KUHAP yang mengharuskan adanya minimal dua alat bukti. Jika persyaratan tersebut terpenuhi, kasus akan dilanjutkan ke pengadilan untuk tahap pemeriksaan lebih lanjut.

Namun, jika bukti yang ada tidak cukup kuat atau terdapat kelemahan dalam peraturan perundang-undangan yang mengatur tindak pidana tersebut, proses penyidikan dan penuntutan bisa dihentikan. Oleh karena itu, koordinasi yang kuat antara penyidik dan jaksa, disertai dukungan regulasi yang adaptif terhadap perkembangan teknologi, menjadi elemen kunci

dalam pemberantasan *cyber crime*. Proses ini juga membutuhkan pendekatan lintas lembaga dan kolaborasi internasional untuk mengatasi tantangan global yang ditimbulkan oleh kejahatan berbasis internet.

Peran Digital Forensik dalam Mengungkap dan Membuktikan Tindak Pidana Akses Ilegal Pada Sistem Informasi PT Kereta Commuter Indonesia (KCI)

Akses ilegal terhadap sistem informasi telah menjadi salah satu ancaman serius di era digital. Tindak pidana ini tidak hanya melibatkan peretasan terhadap data sensitif, tetapi juga dapat mengganggu operasional perusahaan, merusak kepercayaan publik, hingga menciptakan risiko finansial yang signifikan. PT Kereta Commuter Indonesia (KCI), sebagai penyedia layanan transportasi berbasis teknologi, memiliki sistem informasi yang menjadi tulang punggung operasionalnya. Sistem ini mencakup manajemen tiket, jadwal kereta, dan data pelanggan yang sensitif. Oleh karena itu, setiap upaya akses ilegal terhadap sistem ini memerlukan respons yang cepat dan komprehensif untuk mengungkap pelaku serta memitigasi dampaknya.

Digital forensik merupakan disiplin ilmu yang menggabungkan teknologi, hukum, dan investigasi untuk mengidentifikasi, mengumpulkan, menganalisis, dan memelihara bukti elektronik. Dalam kejahatan akses ilegal pada KCI, peran digital forensik sangat strategis karena aktivitas mencurigakan pada jaringan perusahaan, seperti upaya akses tanpa izin atau transfer data yang tidak biasa, dapat dideteksi melalui analisis log server dan perangkat lunak keamanan jaringan. Digital forensik membantu dalam mengidentifikasi jejak digital pelaku, termasuk alamat IP, waktu akses, dan perangkat yang digunakan.

Dalam banyak kasus, pelaku mencoba menghapus jejak mereka dengan menghapus data atau menggunakan enkripsi. Digital forensik menggunakan teknologi pemulihan data, seperti teknik recovery disk dan alat forensik perangkat keras, untuk mengakses informasi yang telah dihapus atau disembunyikan. Jejak digital berupa log akses, metadata file, atau pola anomali dalam lalu lintas data dianalisis untuk mengungkapkan metode dan tujuan dari serangan tersebut. Proses ini melibatkan alat forensik seperti EnCase dan Forensic Toolkit (FTK) untuk memberikan analisis yang mendalam. Untuk mengungkap kejahatan akses ilegal, langkah-langkah yang dilakukan:

1. Identifikasi Insiden

   Langkah awal dalam mengungkap kejahatan akses ilegal adalah proses identifikasi insiden. Identifikasi ini sering dimulai dengan laporan dari sistem pemantauan keamanan, seperti intrusion detection systems (IDS) atau security information and event management (SIEM). Insiden dapat berupa anomali aktivitas pengguna, akses yang tidak

sah, atau perubahan mencurigakan pada sistem informasi. Dalam KCI, insiden mungkin dilaporkan melalui laporan penggunaan abnormal pada aplikasi pengisian saldo kartu Multi Trip (KMT) atau anomali dalam integrasi pembayaran digital.

Tim keamanan siber bertanggung jawab untuk mengevaluasi dampak awal insiden ini. Penilaian melibatkan analisis cepat atas data operasional yang terpengaruh, termasuk transaksi finansial, data pelanggan, dan integritas sistem secara keseluruhan. Tujuannya adalah untuk memahami skala ancaman sehingga langkah-langkah mitigasi dapat segera diterapkan untuk mencegah kerugian lebih lanjut.

2. Pengumpulan Bukti Digital

   Proses ini merupakan salah satu tahap paling kritis dalam digital forensik. Bukti yang relevan harus dikumpulkan secara sistematis dan sesuai dengan protokol hukum yang ketat agar dapat diterima di pengadilan. Jenis Bukti yang Dikumpulkan:

   a. Log Sistem

      Log server atau aplikasi yang menunjukkan aktivitas mencurigakan, termasuk upaya akses tidak sah, perubahan konfigurasi, atau pemrosesan data yang tidak biasa.

   b. Data Perangkat Keras

      Informasi dari perangkat yang digunakan pelaku, seperti ponsel, laptop, atau alat lain yang terhubung ke sistem KCI.

   c. Bukti Transaksi Digital

      Bukti rekaman dari dompet digital yang digunakan dalam transaksi manipulatif.

   d. Metadata

      Informasi tambahan seperti IP address, lokasi geografis, dan waktu aktivitas yang membantu melacak jejak pelaku.

   e. Jejak Elektronik

      Data yang sudah dihapus dapat dipulihkan menggunakan teknik recovery disk untuk menemukan informasi penting yang mungkin disembunyikan oleh pelaku.

   Pengumpulan bukti ini memerlukan pendekatan khusus untuk menjaga integritas data. Setiap bukti yang dikumpulkan harus direkam dalam rantai pengawasan (*chain of custody*) guna memastikan bahwa data tidak diubah atau dimanipulasi.

3. Pemulihan dan Analisis Data

   Setelah bukti dikumpulkan, tahap selanjutnya adalah pemulihan dan analisis data. Bukti elektronik yang diperoleh mungkin tidak dalam kondisi utuh, mengingat pelaku sering berusaha menghapus atau mengubah data untuk menutupi jejak mereka. Oleh karena itu, teknik pemulihan data, seperti *disk recovery* dan data carving, digunakan untuk

mengakses data yang telah dihapus atau rusak. Data yang berhasil dipulihkan akan dianalisis untuk mencari pola-pola yang mengarah pada pelaku dan metode yang mereka gunakan. Teknik analisis ini mencakup pemeriksaan lebih lanjut terhadap log akses dan metadata untuk melacak kegiatan yang mencurigakan.

4. Wawancara dan Interogasi

   Selain bukti digital, penyelidik juga dapat melakukan wawancara atau interogasi terhadap individu-individu yang terlibat dalam peristiwa tersebut. Wawancara ini dapat melibatkan saksi, korban, atau bahkan pelaku yang telah ditangkap. Melalui wawancara, penyelidik dapat mengumpulkan informasi yang mungkin tidak dapat ditemukan hanya dengan menganalisis bukti digital. Teknik interogasi seperti pendekatan logis, facing-saving approach, dan indifference sering kali digunakan untuk memperoleh pengakuan atau konfrontasi antara tersangka dengan saksi.

5. Penyusunan Laporan Kasus

   Setelah seluruh bukti terkumpul dan dianalisis, langkah berikutnya adalah menyusun laporan kasus yang mendetail. Laporan ini perlu memuat semua temuan penting, termasuk kronologi kejadian, metode yang diterapkan oleh pelaku, serta bukti digital yang mendukung dugaan mengenai pihak yang bertanggung jawab atas kejahatan tersebut. Laporan ini akan menjadi acuan bagi aparat penegak hukum, baik untuk melanjutkan penyidikan maupun untuk dipergunakan dalam proses persidangan.

Digital forensik mengandalkan sejumlah alat teknologi yang sangat penting dalam investigasi kasus kejahatan dunia maya. Beberapa alat yang digunakan untuk mengungkap akses ilegal pada sistem informasi antara lain:

1. Wireshark dan Splunk untuk analisis lalu lintas jaringan guna mendeteksi aktivitas mencurigakan.
2. Forensic Toolkit (FTK) dan EnCase untuk mengakses dan menganalisis data yang terhapus dari perangkat.
3. Sleuth Kit dan Autopsy untuk mengekstrak dan menganalisis bukti dari disk yang terinfeksi malware.
4. IDA Pro dan Cuckoo Sandbox digunakan dalam analisis malware untuk mengetahui asal dan tujuan serangan.

Selain itu, penggunaan teknik analisis forensik pada malware dapat membantu dalam menemukan program jahat yang digunakan pelaku untuk mengeksploitasi kelemahan dalam sistem informasi PT KCI.

Kekuatan Alat Bukti Digital yang Diperoleh Melalui Digital Forensik dalam Mendukung Proses Penegakan Hukum Terhadap Pelaku Kejahatan Siber

Keamanan digital dan penyelidikan terhadap kejahatan siber telah berkembang pesat, seiring dengan meningkatnya jumlah kasus *cyber crime*. Salah satu instrumen kunci dalam mengungkap dan membuktikan tindak pidana siber adalah *digital forensics* (forensik digital), yang berperan penting dalam mengumpulkan, menganalisis, dan menyajikan bukti digital yang dapat dipertanggungjawabkan di pengadilan. Keberhasilan penegakan hukum terhadap pelaku kejahatan siber sangat bergantung pada kekuatan bukti digital yang diperoleh melalui digital forensik. Oleh karena itu, sangat penting untuk menghubungkan penggunaan bukti digital dengan peraturan perundang-undangan yang relevan, seperti Undang-Undang Informasi dan Transaksi Elektronik (ITE) serta Kitab Undang-Undang Hukum Acara Pidana (KUHAP). Forensik digital mencakup berbagai prosedur teknis yang memungkinkan penyidik untuk menemukan, mengidentifikasi, dan memulihkan data yang mungkin terhapus atau disembunyikan. Alat bukti digital yang diperoleh melalui forensik digital dapat berupa data yang ditemukan dalam perangkat komputer, server, atau jaringan yang digunakan oleh pelaku kejahatan siber. Proses ini tidak hanya melibatkan pencarian data, tetapi juga mencakup identifikasi jejak digital yang ditinggalkan oleh pelaku di dunia maya.

Proses pengumpulan bukti digital harus mengikuti prosedur yang sangat ketat agar bukti tersebut sah dan dapat diterima di pengadilan. Salah satu prinsip utama dalam digital forensics adalah integritas bukti. Setiap bukti yang ditemukan harus dipertahankan dengan cara yang memastikan bahwa bukti tersebut tidak berubah selama proses pengumpulan hingga analisis, serta disimpan dengan aman dalam format yang tidak bisa dimanipulasi.

Alat bukti digital yang diperoleh melalui forensik digital memiliki kekuatan yang sangat besar dalam mendukung proses penegakan hukum, asalkan bukti tersebut diperoleh secara sah dan sahih. Alat bukti digital mencakup berbagai jenis data seperti log server, rekaman komunikasi digital, riwayat transaksi, metadata, serta file atau dokumen yang dapat mengungkap tindakan ilegal yang dilakukan pelaku.

Bukti-bukti ini dapat digunakan untuk mengidentifikasi pelaku, membuktikan adanya tindak pidana, dan memperlihatkan keterlibatan pelaku dalam suatu kegiatan ilegal. Misalnya, dalam kasus akses ilegal ke sistem informasi, bukti yang diperoleh bisa berupa rekaman aktivitas login yang tidak sah, perubahan data yang mencurigakan, atau bukti transfer data yang menunjukkan adanya akses tanpa izin ke dalam sistem.

Berdasarkan Pasal 5 Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (ITE) yang kemudian diubah melalui Undang-Undang Nomor 19 Tahun

2016, informasi elektronik serta salinan cetaknya dapat dijadikan bukti yang sah di pengadilan. Dalam hal ini, bukti yang diperoleh melalui digital forensik dapat diterima di pengadilan selama memenuhi ketentuan yang diatur dalam undang-undang tersebut, yang menyatakan bahwa informasi elektronik memiliki kekuatan hukum yang sah.

Dalam proses pembuktian tindak pidana, termasuk dalam kasus kejahatan siber, KUHAP menetapkan bahwa bukti yang sah adalah bukti yang diperoleh sesuai dengan prosedur hukum yang berlaku dan dapat digunakan untuk membuktikan kesalahan terdakwa. Pasal 183 KUHAP mengatur bahwa setidaknya dua alat bukti yang sah dan saling mendukung diperlukan untuk membuktikan kesalahan terdakwa.

Bukti digital yang diperoleh melalui digital forensik dapat dijadikan sebagai dua alat bukti yang sah, misalnya dengan menggabungkan bukti berupa rekaman digital dan keterangan dari saksi ahli forensik digital. Dalam prakteknya, bukti digital ini harus diperiksa oleh penyidik dan diuji di pengadilan melalui proses yang memastikan bahwa bukti tersebut benar-benar berasal dari perangkat yang digunakan oleh pelaku dan tidak dimanipulasi.

Agar bukti digital yang diperoleh memiliki kekuatan yang sah di pengadilan, penggunaan prosedur dan standar forensik yang benar sangat penting. Ini termasuk penggunaan perangkat forensik yang sah dan disertifikasi, serta keterampilan profesional dalam memeriksa dan menganalisis bukti digital. Penggunaan metode yang tidak sah atau prosedur yang salah dapat menyebabkan bukti dianggap tidak sah atau bahkan bisa merusak proses penyidikan.

Selain itu, dalam kasus kejahatan siber, koordinasi antara lembaga penegak hukum, penyidik digital, serta pihak-pihak terkait lainnya sangat diperlukan untuk memastikan bahwa bukti yang diperoleh dapat dipertanggungjawabkan dan diterima di pengadilan.

4. KESIMPULAN

Digital forensik memainkan peran penting dalam mengidentifikasi, mengumpulkan, menganalisis, dan mengamankan bukti-bukti digital yang terkait dengan akses ilegal pada sistem informasi PT Kereta Commuter Indonesia (KCI). Proses forensik digital ini melibatkan pengumpulan bukti dari perangkat keras dan perangkat lunak yang terlibat, termasuk analisis jejak digital seperti log aktivitas dan metadata yang dapat menunjukkan adanya akses yang tidak sah. Dengan menggunakan teknik-teknik seperti pemulihan data yang terhapus dan pelacakan jejak digital, digital forensik dapat membantu pihak berwenang menemukan bukti yang dapat digunakan untuk mengidentifikasi pelaku dan mendukung proses penyidikan lebih lanjut. Alat bukti digital yang diperoleh melalui proses digital forensik memiliki kekuatan yang signifikan dalam mendukung proses penegakan hukum, terutama dalam mengatasi kejahatan

siber. Bukti digital, seperti data dari server, perangkat pengguna, dan jejak transaksi, sering kali menjadi elemen penting dalam membuktikan tindak pidana siber. Sesuai dengan peraturan perundang-undangan yang berlaku, bukti digital ini harus memenuhi standar tertentu agar dapat diterima di pengadilan, seperti memastikan keaslian dan integritas bukti yang terjaga selama proses forensik. Undang-undang yang mengatur perlindungan data pribadi dan kejahatan siber di Indonesia, seperti UU ITE (Informasi dan Transaksi Elektronik), memberikan landasan hukum untuk penggunaan bukti digital dalam proses peradilan.

DAFTAR PUSTAKA

Arief, B. N. (2005). Pembaharuan hukum pidana dalam perspektif kajian perbandingan (Cet. 1). Bandung: Citra Aditya Bakti.

Arifah, D. A. (2011). Kasus cybercrime di Indonesia. Jurnal Bisnis dan Ekonomi, 18(2), 185-195. file:///C:/Users/User/Downloads/fvm939e.pdf

Djanggih, H. (2013, November 15). Kebijakan hukum pidana dalam penanggulangan cybercrime di bidang kesusilaan. Jurnal Media Hukum, 1(2). https://osf.io/c9m25

Ekundayo, F. (2024, November 30). Big data and machine learning in digital forensics: Predictive technology for proactive crime prevention. World Journal of Advanced Research and Reviews, 24(2), 2692-2709. https://wjarr.com/node/16513

Hermawan, R. (2013). Kesiapan aparatur pemerintah dalam menghadapi. Jurnal Teknik Informatika, 6(1), 43-50.

https://doi.org/10.14569/IJACSA.2022.0130939

https://doi.org/10.30574/wjarr.2024.24.2.3659

https://doi.org/10.33172/jpbh.v7i2.193

https://doi.org/10.36106/ijsr/9633529

https://doi.org/10.4018/979-8-3693-6517-5.ch011

https://doi.org/10.5120/ijca2017914729

https://doi.org/10.54938/ijemdcsai.2022.01.1.37

https://doi.org/10.62311/nesx/97422614

K, Y., & Venumadhava, G. S. (2022, February 1). Cyber forensic tools and its application in the investigation of digital crimes: Preventive measures with case studies. International Journal of Scientific Research, 71-73. https://www.worldwidejournals.com/international-journal-of-scientific-research-(IJSR)/fileview/cyber-forensic-tools-and-its-application-in-the-investigation-of-

digital-crimes-preventive-measures-with-case-studies_February_2022_6126714570_9633529.pdf

Krishna Pasupuleti, M. (2024). Digital forensics uncovering cyber evidence. In Digital forensic science (pp. 41-49). National Education Services. https://www.nationaleducationservices.org/digital-forensics-uncovering-cyber-evidence/pid-2226747091

Legacy, S. (2024, September). Cyber forensics and cyber crime investigation: Utilizing AI for faster and more accurate results.

Magdalena, M., & Setiyadi, M. R. (2007). Cyberlaw, tidak perlu takut (Ed. 1). Yogyakarta: Andi.

Makarim, E. (2003). Kompilasi hukum telematika (Ed. 1). Jakarta: University Press.

Mansur, D. M. A., & Gultom, E. (2005). Cyber law: Aspek hukum teknologi informasi (Ed. 1). Bandung: Refika Aditama.

Mariyanna, S. K. (2017). Post graduate diploma cyber law & cyber forensics machine learning for cyber forensics and judicial admissibility project assignment submitted by Shiva Kumar Mariyanna ID No. CLCF/667/17 year of study.

Muis, M. (2019). Penanggulangan cyber crime. Universitas Muhamadiyah Sumatera Utara.

Mumpuni, A. (2024). Pemuda Depok berhasil bobol saldo KAI Rp12 juta, begini modusnya. Tirto.id2. https://tirto.id/pemuda-depok-berhasil-bobol-saldo-kai-rp12-juta-begini-modusnya-gWFx#google_vignette

Nurcahyo, A. T. (2024). Polisi ungkap cara pelaku bobol sistem top up saldo KMT KAI Commuter, raup Rp12 juta selama 3 hari. Prfmnews.id. https://prfmnews.pikiran-rakyat.com/nasional/pr-137805231/polisi-ungkap-cara-pelaku-bobol-sistem-top-up-saldo-kmt-kai-commuter-raup-rp12-juta-selama-3-hari?page=all

Rahmawati, I. (2017). The analysis of cyber crime threat risk management to increase cyber defense. Jurnal Pertahanan & Bela Negara, 7(2), 51-66.

Ramli, A. M. (2006). Cyber law and HAKI dalam sistem hukum Indonesia (Ed. 1). Bandung: Abacus.

Riadi, I., Fadlil, A., & Sari, T. (2017, July 17). Image forensic for detecting splicing image with distance function. International Journal of Computer Applications, 169(5), 6-10. http://www.ijcaonline.org/archives/volume169/number5/riadi-2017-ijca-914729.pdf

Rukmini, M. (2006). Aspek hukum pidana dan kriminologi: Sebuah bunga rampai (Cet. 1). Bandung: Refika Aditama.

Sahetapy. (2005). Pisau analisis kriminologi (E. L. Sahetapy, Ed., Ed. 1). Bandung: Citra Aditya Bakti.

Saputro, B. N. J. A. (2014). Kepastian hukum bukti digital cybercrime dalam komputer forensik. Universitas Jember.

Singh, A., Singh, S. K., Vege, H. K., & Singh, N. (2022). A framework for crime detection and diminution in digital forensics (CD3F). International Journal of Advanced Computer Science and Applications, 13(9). http://thesai.org/Publications/ViewPaper?Volume=13&Issue=9&Code=IJACSA&SerialNo=39

Sitompul, A. (2004). Hukum internet (Cet. 2). Bandung: Citra Aditya Bakti.

Subair, S., Yosif, D., Ahmed, A., & Thron, C. (2022, May 30). Cyber crime forensics. International Journal of Emerging Multidisciplinaries: Computer Science & Artificial Intelligence, 1(1), 41-49. http://ojs.ijemd.com/index.php/ComputerScienceAI/article/view/37

Suhariyanto, B. (2013). Tindak pidana teknologi informasi (cybercrime): Urgensi pengaturan dan celah hukumnya (Ed. 1). Jakarta: Rajawali Pers.

Suparni, N. (2009). Cyberspace: Problematika dan antisipasi pengaturannya (Ed. 1). Jakarta: Sinar Grafika.

Wahid, A., & Labib, M. (2005). Kejahatan mayantara: Cyber crime (Ed. 1). Jakarta: Refika Aditama.

Widodo. (2009). Sistem pemidanaan dalam cyber crime: Alternatif ancaman pidana kerja sosial dan pidana pengawasan bagi pelaku cyber crime (Ed. 1). Yogyakarta: Laksbang Mediatama.

Yogi, M. K., & Mundru, Y. (2024). Illuminating evidence. In Redefining security with cyber AI (pp. 195-229). https://services.igi-global.com/resolvedoi/resolve.aspx?doi=10.4018/979-8-3693-6517-5.ch011

Yustia, M. A. (2010). Pembuktian dalam hukum pidana Indonesia terhadap cyber crime. Jurnal Pranata Hukum, 5(2), 77-90.