



Screenshot: Lebih dari Sekedar Gambar, Bukti yang Berbicara

Aprilia Silvi Suciana¹, Yunan Prasetyo Kurniawan²

^{1,2} Magister Hukum Universitas Pancasila, Fakultas Hukum,

Universitas Pancasila, Menteng, Jakarta Pusat, Indonesia

Email : aprilias5223010@univpancasila.ac.id¹, yunanprasetyo@univpancasila.ac.id²

Abstract. *Electronic money laundering has become a critical issue as a form of cybercrime. Advances in technology demonstrate that digital forensic applications, particularly those utilizing smartphones, can be employed to uncover digital traces of money laundering transactions. This study aims to analyze the relevance of existing legal frameworks, the effectiveness of smartphone forensic techniques, and the challenges faced in their implementation in Indonesia. Based on a review of the literature and regulatory analysis, it was found that legal frameworks such as UU No. 8 of 2010 on the Prevention and Eradication of Money Laundering (TPPU) and UU No. 19 of 2016 on Information and Electronic Transactions (ITE) provide an adequate legal foundation. However, gaps in implementation, such as limited human and technological resources, remain significant obstacles. Forensic techniques, including metadata analysis and device extraction, have shown great potential in identifying the flow of illicit funds. Nonetheless, their application is hindered by data confidentiality and the lack of uniform technical standards. Given the increasing complexity of digital crimes, an integrated approach is required, combining regulatory strengthening with technological capacity building, to enhance the effectiveness of smartphone forensics in addressing electronic money laundering.*

Keywords: *Cyber Crime, Screenshot, Digital Evidence, Digital Forensics*

Abstrak. Pencucian uang elektronik telah menjadi isu krusial sebagai salah satu bentuk kejahatan siber. Kemajuan teknologi menunjukkan bahwa aplikasi forensik digital, khususnya yang menggunakan smartphone, dapat dimanfaatkan untuk mengungkap jejak digital dari transaksi pencucian uang. Penelitian ini bertujuan untuk menganalisis relevansi kerangka hukum yang ada, efektivitas teknik forensik berbasis smartphone, serta tantangan yang dihadapi dalam penerapannya di Indonesia. Berdasarkan tinjauan literatur dan analisis regulasi, ditemukan bahwa kerangka hukum seperti UU No. 8 Tahun 2010 tentang Pencegahan dan Pemberantasan Tindak Pidana Pencucian Uang (TPPU) dan UU No. 19 Tahun 2016 tentang Informasi dan Transaksi Elektronik (ITE) memberikan landasan hukum yang memadai. Namun, terdapat celah dalam implementasi, seperti keterbatasan sumber daya manusia dan teknologi, yang menjadi hambatan signifikan. Teknik forensik, termasuk analisis metadata dan ekstraksi perangkat, menunjukkan potensi besar dalam mengidentifikasi aliran dana ilegal. Meskipun demikian, penerapannya terhalang oleh isu kerahasiaan data dan kurangnya standar teknis yang seragam. Mengingat meningkatnya kompleksitas kejahatan digital, diperlukan pendekatan yang terintegrasi dengan mengombinasikan penguatan regulasi dan peningkatan kapasitas teknologi untuk meningkatkan efektivitas forensik berbasis smartphone dalam menangani pencucian uang elektronik.

Kata Kunci: Cyber Crime, Screenshot, Alat Bukti Digital, Digital Forensics

1. PENDAHULUAN

Seiring dengan kemajuan teknologi informasi dan komunikasi dalam beberapa dekade terakhir, berbagai perubahan fundamental telah terjadi di hampir seluruh aspek kehidupan manusia, termasuk di bidang sosial, ekonomi, dan hukum. Era digitalisasi tidak hanya menawarkan berbagai peluang inovatif, namun juga menciptakan tantangan baru, salah satunya adalah meningkatnya angka tindak kejahatan yang memanfaatkan teknologi informasi, yang dikenal sebagai cyber crime. Perubahan ini memaksa masyarakat dan sistem hukum untuk beradaptasi dengan realitas baru yang dituntut oleh kemajuan teknologi. Kejahatan ini meliputi berbagai bentuk, mulai dari penipuan daring, peretasan, penyebaran konten ilegal, hingga

pencemaran nama baik di media sosial. Mengingat sifatnya yang lintas batas dan sering kali sulit dilacak, cyber crime menjadi salah satu tantangan terbesar bagi sistem peradilan modern.

Dalam proses penegakan hukum terhadap kejahatan siber, bukti digital memiliki peranan yang sangat vital, karena mampu memberikan informasi yang mendalam mengenai pelaku dan teknik yang digunakan dalam melaksanakan tindak pidana. Salah satu jenis bukti digital yang sering ditemukan dalam kasus-kasus kejahatan siber adalah screenshot. Screenshot, yang juga dikenal sebagai tangkapan layar, adalah gambaran visual dari data digital yang diambil langsung dari perangkat elektronik seperti komputer, smartphone, atau tablet. Tangkapan layar ini sering kali berisi informasi penting, seperti percakapan melalui pesan elektronik, aktivitas transaksi online, atau tindakan digital lainnya yang relevan dengan tindak pidana yang sedang ditangani oleh aparat penegak hukum.

Meskipun tampak sederhana, penggunaan screenshot sebagai alat bukti menghadirkan kompleksitas tersendiri dalam hukum. Secara teknis, screenshot dapat diambil dan dimanipulasi dengan mudah, sehingga keasliannya kerap dipertanyakan. Di sisi lain, peraturan hukum yang mengatur mengenai alat bukti digital, khususnya di Indonesia, masih menghadapi berbagai keterbatasan dalam menghadapi keunikan sifat bukti digital. Hal ini menimbulkan pertanyaan kritis mengenai peran, kekuatan hukum, serta prosedur yang harus ditempuh untuk memastikan bahwa *screenshot* dapat diterima sebagai alat bukti yang sah di pengadilan.

Dalam perspektif hukum, sebuah alat bukti harus memenuhi prinsip legalitas, relevansi, dan akseptabilitas. Legalitas berkaitan dengan kesesuaian alat bukti dengan ketentuan hukum yang berlaku, relevansi mengacu pada keterkaitannya dengan perkara yang sedang diperiksa, sementara akseptabilitas mengacu pada penerimaan alat bukti tersebut oleh pengadilan. Untuk memenuhi ketiga prinsip ini, alat bukti digital seperti *screenshot* memerlukan dukungan dari keahlian *digital forensics*. *Digital forensics* adalah disiplin ilmu yang mempelajari teknik dan metode untuk mengidentifikasi, mengumpulkan, menganalisis, serta menyajikan bukti digital dengan cara yang dapat dipertanggungjawabkan di pengadilan. Dalam *Digital forensics* terdapat berbagai prosedur standar yang dirancang untuk memastikan validitas dan keaslian bukti digital, termasuk *screenshot*. Prosedur ini melibatkan serangkaian tahapan seperti data acquisition, data validation, serta penggunaan alat dan metode yang telah diakui secara internasional. Namun, dalam praktiknya, penerapan prosedur forensik terhadap *screenshot* sebagai alat bukti sering kali menghadapi kendala.

Melalui penelitian ini, diharapkan dapat ditemukan jawaban atas berbagai persoalan mendasar terkait posisi hukum *screenshot* dan bagaimana penerapan teknologi *digital forensics* dapat mendukung keabsahannya. Penelitian ini tidak hanya memberikan kontribusi dalam

pengembangan teori hukum digital, tetapi juga memberikan panduan praktis bagi aparat penegak hukum, pengacara, serta profesional di bidang forensik digital dalam menghadapi tantangan pembuktian di era digital.

2. METODE PENELITIAN

Metode yang digunakan dalam penelitian ini adalah Yuridis Normatif, yang mengedepankan analisis terhadap data sekunder, termasuk bahan hukum primer, sekunder, dan tersier, yang didukung oleh data primer. Penelitian ini bersifat deskriptif analitis, dengan tujuan untuk menguraikan dan menganalisis secara mendalam peraturan perundang-undangan, baik yang berlaku di tingkat nasional maupun internasional, terkait dengan teori-teori hukum yang membahas mengenai pembaruan dalam hukum pidana. Teknik pengumpulan data mencakup penelitian kepustakaan dan penelitian lapangan. Penelitian kepustakaan difokuskan pada pencarian bahan hukum dari berbagai referensi, seperti peraturan perundang-undangan serta teori-teori hukum yang relevan. Bahan hukum sekunder yang digunakan dalam penelitian ini mencakup doktrin, pendapat dari para ahli, buku-buku hukum, makalah ilmiah, hasil-hasil penelitian hukum, serta RUU yang dapat memberikan penjelasan terhadap bahan hukum primer. Setelah itu, data yang dikumpulkan akan dianalisis secara deskriptif untuk memberikan gambaran yang jelas tentang peraturan perundang-undangan yang berhubungan dengan pembentukan KUHAP, dan dianalisis lebih lanjut dengan menggunakan teori-teori hukum yang ada.

3. HASIL DAN PEMBAHASAN

Alat Bukti di Persidangan

Pasal 183 dalam Kitab Undang-Undang Hukum Acara Pidana (KUHAP) dengan jelas menyatakan bahwa seorang hakim hanya dapat memutuskan hukuman pidana terhadap seorang terdakwa jika terdapat setidaknya dua alat bukti yang sah secara hukum. Alat bukti ini merujuk pada segala hal yang terkait dengan tindakan tertentu, yang kemudian digunakan untuk membangun keyakinan hakim mengenai kebenaran tindakan pidana yang dilakukan oleh terdakwa. Dalam pandangan para ahli, konsep alat bukti ini mencakup unsur-unsur yang sangat penting yang mampu menggambarkan kejadian pidana dengan jelas, sehingga menjadi dasar bagi hakim untuk mengambil keputusan yang adil dan objektif.

Sistem pembuktian di Indonesia, yang berlandaskan pada prinsip negatif wettelijke bewijs theorie (teori pembuktian secara negatif menurut undang-undang), mengutamakan dua elemen yang saling berkaitan, yakni alat bukti yang sah dan keyakinan hakim. Hal ini

menegaskan bahwa seorang hakim tidak diperkenankan untuk memutuskan perkara atau memberikan hukuman hanya berlandaskan pada keyakinan pribadi, melainkan harus didukung oleh minimal dua alat bukti yang sah sesuai dengan ketentuan hukum yang berlaku di Indonesia.

Pesatnya perkembangan teknologi informasi memberikan dampak yang besar pada berbagai sektor kehidupan, termasuk dalam hal sistem pembuktian hukum. Kejahatan yang menggunakan teknologi informasi menuntut adanya inovasi dalam alat bukti. Salah satu bentuk inovasi tersebut adalah pengakuan terhadap alat bukti elektronik yang kini menjadi kategori baru dalam menyelesaikan kasus-kasus yang berhubungan dengan teknologi canggih.

Surya Praha menjelaskan bahwa alat bukti elektronik adalah data yang disimpan atau ditransmisikan melalui perangkat elektronik, jaringan, atau sistem komunikasi, yang dapat digunakan untuk mendukung pembuktian dalam proses hukum, khususnya dalam kejahatan yang melibatkan teknologi informasi. Konsep alat bukti elektronik ini juga diakui dalam *Budapest Convention* atau Konvensi Dewan Eropa tentang Kejahatan Siber, yang menyatakan bahwa bukti yang dikumpulkan secara elektronik dapat digunakan dalam penyelidikan tindak pidana. Surya Praha juga mengartikan alat bukti elektronik sebagai digital evidence, yaitu informasi atau data dalam bentuk biner yang dapat diandalkan dalam proses hukum. Indonesia telah mengadopsi panduan internasional tentang pengelolaan alat bukti elektronik melalui standar yang dikenal dengan *Information Technology Security Technology - Guidelines for Identification, Collection, Acquisition, and Preservation of Digital Evidence*, yang kini telah menjadi Standar Nasional Indonesia (SNI).

Alat bukti elektronik, yang merupakan perluasan dari alat bukti petunjuk, telah diakui dalam sistem hukum Indonesia, terutama melalui regulasi seperti Pasal 26A Undang-Undang No. 20 Tahun 2001 tentang Pemberantasan Tindak Pidana Korupsi, yang menyebutkan bahwa bukti yang sah dalam kasus korupsi termasuk informasi yang disimpan, dikirim, diterima, atau diproses secara elektronik menggunakan perangkat optik atau sejenisnya. Selain itu, alat bukti elektronik juga mencakup dokumen, yaitu segala jenis rekaman atau informasi yang bisa dilihat, dibaca, atau didengar, baik yang memerlukan alat bantu maupun tidak.

Lebih lanjut, dokumen ini bisa berupa tulisan, suara, gambar, peta, desain, foto, simbol, angka, atau perforasi dengan makna tertentu. Jenis dokumen ini tidak hanya terbatas pada media kertas, melainkan juga mencakup berbagai media fisik lainnya, termasuk media elektronik.

Alat bukti elektronik memiliki karakteristik yang membedakannya dari alat bukti tradisional. Tiga nomenklatur utama yang menjadi ciri khas alat bukti elektronik adalah.

- Informasi Elektronik

Informasi yang dihasilkan, dikirim, diterima, atau disimpan dalam bentuk elektronik dan memiliki relevansi terhadap perkara yang sedang ditangani. Informasi ini mencakup data komunikasi digital seperti email, pesan instan, atau data transaksi elektronik.

- Dokumen Elektronik

Dokumen yang dibuat atau disimpan secara digital, baik dalam format teks, audio, video, maupun kombinasi dari semuanya. Dokumen elektronik dapat mencakup kontrak digital, laporan keuangan berbasis perangkat lunak, atau bukti digital lainnya yang relevan dalam proses hukum.

- Hasil Cetakan

Alat bukti elektronik juga dapat diwujudkan dalam bentuk cetakan dari informasi atau dokumen digital. Hasil cetakan ini harus memuat informasi yang valid dan relevan dengan perkara serta memiliki keterkaitan dengan alat bukti elektronik lainnya.

Keberadaan alat bukti elektronik membawa dampak besar dalam sistem pembuktian hukum di Indonesia. Di satu sisi, alat bukti elektronik memberikan fleksibilitas dan kemudahan dalam pengumpulan serta penyajian bukti untuk mengungkap kejahatan modern. Namun, di sisi lain, alat bukti elektronik juga menimbulkan tantangan, terutama dalam aspek validitas, keaslian, dan penerimaan di pengadilan.

Screenshot sebagai Alat Bukti dalam Tindak Pidana Cyber Crime

Proses pembuktian dalam tindak pidana khusus sering kali menghadapi tantangan yang kompleks, terutama dalam kaitannya dengan pengumpulan dan penggunaan alat bukti di persidangan. Salah satu hambatan utama adalah menentukan alat bukti yang memenuhi kriteria keabsahan hukum sehingga dapat digunakan sebagai dasar dakwaan terhadap individu yang diduga melakukan tindak pidana. Dalam kejahatan berbasis teknologi informasi, seperti *cyber crime*, tantangan ini semakin kompleks. Penggunaan teknologi dalam tindak pidana ini kerap menghasilkan bukti yang berbentuk elektronik, seperti rekaman percakapan, data digital, dan dokumen elektronik. Oleh karena itu, diperlukan pendekatan yang hati-hati untuk memastikan bahwa bukti tersebut sesuai dengan peraturan hukum formil yang berlaku.

Hasil cetakan dari informasi atau dokumen elektronik diakui sebagai alat bukti yang sah menurut hukum, berdasarkan Pasal 5 ayat (1) Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (UU ITE), yang telah diperbarui melalui Undang-Undang Nomor 19 Tahun 2016. Pasal tersebut menetapkan bahwa informasi dan dokumen dalam bentuk elektronik, beserta hasil cetaknya, memiliki kekuatan pembuktian yang sah, dengan syarat informasi tersebut sesuai dengan versi elektronik aslinya. Adanya regulasi ini

memberikan dasar hukum yang jelas untuk alat bukti elektronik dalam proses peradilan, meskipun dalam praktiknya sering kali ditemui kendala teknis yang menghambat penerapannya secara optimal.

Salah satu tantangan utama dalam menggunakan alat bukti elektronik adalah memastikan keutuhan dan keasliannya sebagaimana dipersyaratkan oleh Pasal 6 UU ITE. Keutuhan alat bukti elektronik harus dapat dijamin agar bukti tersebut tetap relevan dan dapat diterima di pengadilan. Namun, proses ini sering kali terkendala oleh keterbatasan teknis, seperti risiko manipulasi data dan kesulitan dalam mengautentikasi sumber bukti. Hal ini menjadi hambatan yang signifikan dalam pelaksanaan hukum acara pidana di Indonesia, terutama ketika hakim harus memutuskan berdasarkan alat bukti elektronik yang keabsahannya masih diragukan.

Surya Praha menyatakan bahwa bukti elektronik, termasuk hasil cetakan dari informasi elektronik, cenderung hanya berperan sebagai pelengkap dalam proses persidangan, bukan sebagai bukti yang dapat menentukan secara langsung hasilnya. Kondisi ini bisa menimbulkan masalah yang sangat serius apabila hakim salah menarik kesimpulan berdasarkan alat bukti yang tidak valid. Sebagai informasi, tujuan utama dari penggunaan alat bukti adalah untuk mempresentasikan peristiwa yang telah terjadi, memberikan pemahaman mengenai sebab-akibat dari tindakan yang dilakukan oleh terdakwa, dan menjadi landasan bagi hakim dalam memberikan keputusan yang tepat dan adil.

Penyusunan Kitab Undang-Undang Hukum Acara Pidana (KUHAP) dilakukan oleh lembaga legislatif dengan tujuan untuk mengatur seluruh tahapan proses pemeriksaan serta pengambilan keputusan yang berkaitan dengan perkara pidana. Dalam hal penggunaan alat bukti elektronik, hakim memiliki kewajiban untuk memeriksa keabsahan bukti-bukti yang diajukan oleh pihak-pihak yang terlibat dalam persidangan. Proses pemeriksaan ini sangat krusial, karena bertujuan agar setiap keputusan yang dikeluarkan oleh hakim berdasarkan alat bukti tersebut dapat mencerminkan kebenaran materiil, yaitu kebenaran yang sesuai dengan fakta-fakta yang ada serta realitas yang terjadi, bukan sekadar kesimpulan atau interpretasi semata. Dengan demikian, tujuan utama dari hukum acara pidana, yaitu tercapainya peradilan yang adil dan ideal, dapat terwujud.

Walaupun Pasal 5 ayat (1) UU ITE mengakui informasi elektronik sebagai alat bukti yang sah, Mahkamah Konstitusi dalam Putusan Nomor 20/PUU-XIV/2016 memberikan klarifikasi tambahan terkait hal tersebut. Dalam pasal ini, frasa "informasi elektronik dan/atau dokumen elektronik" hanya dapat dijadikan alat bukti jika pengumpulannya dilakukan dalam konteks penegakan hukum yang diatur oleh permintaan dari lembaga penegak hukum seperti

kepolisian, kejaksaan, atau lembaga lain yang ditetapkan oleh undang-undang. Penafsiran ini menekankan bahwa penggunaan informasi elektronik sebagai alat bukti harus dilakukan dengan mengikuti prosedur yang sangat ketat dan selaras dengan ketentuan hukum yang berlaku di negara ini.

Keberadaan alat bukti elektronik memainkan peran penting dalam memberikan kepastian hukum terhadap transaksi dan interaksi yang dilakukan melalui sistem elektronik. Dalam pembuktian hukum, alat bukti ini harus mampu memberikan gambaran yang jelas dan dapat dipercaya mengenai fakta yang terjadi. Dengan adanya peraturan yang mengatur penggunaan alat bukti elektronik, termasuk hasil cetaknya, diharapkan dapat menciptakan landasan hukum yang kokoh untuk menyelesaikan kasus-kasus pidana khusus berbasis teknologi informasi, sehingga proses peradilan dapat berjalan secara transparan, akuntabel, dan adil.

Prosedur Forensik dalam Memastikan Keabsahan Screenshot sebagai Alat Bukti

Perkembangan teknologi informasi dan komunikasi telah membawa perubahan besar dalam berbagai sektor, termasuk di bidang hukum di Indonesia. Dampaknya sangat dirasakan dalam penegakan hukum, khususnya terkait tindak pidana yang semakin banyak memanfaatkan media digital sebagai sarana utama. Fenomena ini menuntut sistem hukum untuk beradaptasi dengan menghadirkan metode yang relevan, salah satunya adalah konsep digital forensik.

Digital forensik merupakan bagian dari ilmu forensik yang khusus mempelajari bagaimana cara mengidentifikasi, mengumpulkan, menganalisis, memproses, dan menyusun laporan terkait data elektronik. Data yang dihasilkan dari proses digital forensik ini sangat berguna dalam membantu penyelesaian investigasi pada kasus hukum yang membutuhkan bukti berbentuk digital. Peran digital forensik dalam proses penyelidikan dan penyidikan sangat vital, di mana ia berfungsi sebagai alat bantu bagi penyidik untuk memperkuat proses hukum. Selain itu, peran ini telah diatur secara jelas dalam Undang-Undang Nomor 19 Tahun 2016 mengenai Informasi dan Transaksi Elektronik (UU ITE) serta dalam Kitab Undang-Undang Hukum Acara Pidana (KUHAP), yang memberikan landasan hukum yang kuat untuk penggunaannya dalam dunia hukum.

UU ITE memberikan dasar hukum yang jelas terkait validitas dan keabsahan alat bukti elektronik. Dalam proses hukum, alat bukti elektronik dapat diterima sebagai bukti yang sah jika memenuhi persyaratan tertentu, baik secara formil maupun materiil.

- Syarat Formil Alat Bukti Elektronik

Menurut Pasal 5 ayat (4) UU ITE, terdapat ketentuan khusus yang mengatur syarat formil penggunaan alat bukti elektronik. Pasal ini menyatakan bahwa alat bukti elektronik tidak sah digunakan untuk jenis surat tertentu yang oleh peraturan perundang-undangan wajib dibuat dalam bentuk tulisan fisik. Demikian juga, dokumen yang wajib disusun dalam bentuk akta notaris atau akta yang diterbitkan oleh pejabat pembuat akta, sebagaimana diatur oleh hukum, tidak dapat dijadikan alat bukti elektronik.

Hal ini berarti dokumen-dokumen yang diwajibkan untuk diterbitkan secara tertulis atau disahkan melalui akta notaris tidak dapat diajukan sebagai alat bukti jika hanya berbentuk elektronik.

- **Syarat Materiil Alat Bukti Elektronik**

Pasal 6 dalam UU ITE mengatur mengenai syarat materiil yang harus dipenuhi agar alat bukti elektronik dapat diterima. Pasal ini menetapkan bahwa informasi atau dokumen dalam bentuk elektronik dapat diterima sebagai bukti yang sah apabila memenuhi kriteria tertentu, seperti: informasi tersebut harus dapat diakses dan ditampilkan ulang, informasi harus tetap utuh tanpa adanya perubahan, serta informasi tersebut harus dapat dipertanggungjawabkan dan memberikan penjelasan yang jelas terkait suatu kejadian. Di sisi lain, Pasal 15 ayat (2) UU ITE mengatur kewajiban penyelenggara sistem elektronik. Pasal ini menjelaskan bahwa penyelenggara sistem elektronik bertanggung jawab sepenuhnya terhadap pengelolaan dan pengoperasian sistem tersebut, termasuk memastikan bahwa sistem elektronik yang digunakan memiliki tingkat keamanan yang memadai dan berfungsi dengan baik tanpa gangguan.

Pasal 16 UU ITE memberikan rincian lebih lanjut terkait persyaratan minimum untuk penyelenggara sistem elektronik, yaitu:

- Mampu menampilkan kembali informasi elektronik secara utuh sesuai masa retensi yang ditetapkan.
- Melindungi ketersediaan, keutuhan, keaslian, kerahasiaan, dan keteraksesan informasi elektronik.
- Memiliki prosedur operasional yang jelas dan dapat dipahami.
- Dilengkapi dengan mekanisme berkelanjutan untuk menjaga kebaruan dan kebertanggungjawaban prosedur atau petunjuk

Ketentuan ini menunjukkan bahwa validitas alat bukti elektronik tidak hanya bergantung pada keberadaan informasi itu sendiri, tetapi juga pada bagaimana sistem yang mengelolanya dioperasikan dan dikelola.

Dalam penegakan hukum, digital forensik tidak hanya membantu mengidentifikasi bukti digital, tetapi juga memastikan keabsahannya di pengadilan. Proses digital forensik melibatkan metode yang terstandar untuk mengumpulkan, menganalisis, dan menyajikan bukti elektronik secara ilmiah. Dengan demikian, keakuratan data yang diperoleh tidak diragukan dan dapat diterima sebagai bukti sah di persidangan.

Melalui penerapan digital forensik, aparat penegak hukum dapat lebih efektif dalam menangani berbagai bentuk kejahatan digital yang semakin kompleks. Digital forensik memungkinkan pengungkapan kasus seperti pencurian data, kejahatan siber, dan penipuan berbasis elektronik dengan lebih akurat, sehingga membantu mengidentifikasi pelaku dan modus operandi yang digunakan. Selain itu, penerapan digital forensik juga berperan dalam mencegah penyalahgunaan teknologi dengan memberikan efek jera melalui pengungkapan kasus yang transparan dan berbasis bukti ilmiah. Tidak hanya itu, digital forensik meningkatkan efektivitas proses penyidikan dengan menyediakan bukti digital yang dapat mendukung proses investigasi secara menyeluruh, sehingga membantu aparat penegak hukum dalam membangun kasus yang kuat di pengadilan.

Pemanfaatan digital forensik dalam sistem penegakan hukum modern menghadirkan peluang besar sekaligus tantangan yang signifikan. Di satu sisi, digital forensik memungkinkan pengumpulan, analisis, dan pelaporan data elektronik secara menyeluruh untuk mengungkap berbagai bentuk kejahatan siber seperti pencurian data, penipuan online, hingga tindak pidana korupsi yang menggunakan sarana digital. Namun, penerapan ini tidak terlepas dari berbagai kendala yang kompleks. Salah satu tantangan utama adalah memastikan validasi dan keaslian bukti digital. Bukti yang diajukan harus terjamin tidak mengalami manipulasi, baik secara sengaja maupun tidak, selama proses pengumpulan dan analisis. Hal ini membutuhkan metode dan perangkat teknologi yang canggih serta protokol yang ketat.

Selain itu, kompetensi aparat penegak hukum menjadi faktor krusial. Aparat yang menangani bukti digital memerlukan pelatihan khusus agar mampu mengelola, memverifikasi, dan menyajikan bukti secara efektif di pengadilan. Kurangnya keahlian di bidang ini dapat menimbulkan celah dalam pembuktian yang berpotensi merugikan proses hukum. Tantangan lain yang tidak kalah penting adalah menjaga keseimbangan antara kebutuhan pengungkapan tindak pidana dan perlindungan privasi individu. Dalam pengumpulan dan analisis bukti digital, sering kali terdapat risiko pelanggaran privasi, seperti akses terhadap data pribadi yang tidak relevan dengan kasus. Hal ini memerlukan penerapan regulasi ketat yang mengatur batasan dalam pengumpulan data, sehingga tidak hanya menjamin keabsahan bukti, tetapi juga menghormati hak-hak individu.

Untuk dapat diterapkan dengan efektif, digital forensik memerlukan dukungan dari kerangka hukum yang kuat, yang juga mengikuti perkembangan teknologi terkini. Dalam hal ini, Undang-Undang Nomor 19 Tahun 2016 tentang Informasi dan Transaksi Elektronik telah menetapkan dasar hukum yang jelas terkait dengan keabsahan bukti elektronik, yang mencakup kedua aspek, yaitu formil dan materiil. Dari segi formil, bukti elektronik tidak berlaku untuk jenis dokumen yang diwajibkan berbentuk tertulis atau dalam bentuk akta notariil, sementara dari segi materiil, bukti elektronik harus memenuhi beberapa persyaratan, seperti dapat diakses, ditampilkan, dijaga keutuhannya, serta dapat dipertanggungjawabkan. Selain itu, ketentuan lain yang diatur dalam undang-undang ini mencakup kewajiban penyelenggara sistem elektronik untuk menjaga dan mengelola data dengan standar yang tinggi, guna menjamin keandalan, keamanan, dan akuntabilitasnya..

4. KESIMPULAN

Berdasarkan analisis, peran dan kekuatan hukum *screenshot* sebagai alat bukti dalam tindak pidana *cyber crime*, khususnya dalam proses penegakan hukum di pengadilan, sangat signifikan, tetapi bergantung pada validitas dan keasliannya. *Screenshot*, sebagai salah satu bentuk alat bukti elektronik, memiliki kekuatan hukum yang diakui berdasarkan Pasal 5 ayat (1) UU ITE. Namun, kekuatan ini hanya dapat diakui jika *screenshot* memenuhi persyaratan formil dan materiil, seperti keutuhan informasi, kemampuan untuk diverifikasi, dan keterkaitannya dengan alat bukti elektronik lainnya. Dalam hal ini, pengadilan menerapkan standar yang ketat untuk memastikan bahwa *screenshot* mencerminkan fakta yang sesuai dengan realitas dan tidak mengalami manipulasi.

Terkait prosedur forensik untuk memastikan validitas *screenshot* sebagai alat bukti digital, digital forensik menjadi komponen kunci. Prosedur forensik melibatkan langkah-langkah seperti identifikasi, pengumpulan, analisis, dan pelaporan data secara ilmiah. Hal ini memastikan bahwa *screenshot* dapat diakses, ditampilkan, dan diverifikasi keasliannya. Regulasi dalam UU ITE dan Standar Nasional Indonesia (SNI) telah memberikan panduan terkait tata kelola sistem elektronik dan alat bukti digital untuk menjaga keandalan serta akuntabilitas data.

DAFTAR PUSTAKA

Abdullah, R. A. F. (2022). *Urgensi digital forensik dalam menganalisis barang bukti elektronik untuk pembuktian tindak pidana informasi dan transaksi elektronik* [Skripsi, Universitas Hasanuddin].

- Anggraeni, D. R., & Salsabila, M. (2024). Analisis yuridis peran digital forensik dalam pembuktian tindak pidana di Indonesia. *Media Hukum Indonesia (MHI)*, 2(2).
- Ariana, I. N. (2022). Tinjauan yuridis terhadap kedudukan alat bukti elektronik berdasarkan Putusan MK Nomor 20/PUU-XIV/2016. *UNES Law Review*, 5(1), 1–19.
- Chazawi, A., & Ferdian, A. (2015). *Tindak pidana informasi & transaksi elektronik: Penyerangan terhadap kepentingan hukum pemanfaatan teknologi informasi dan transaksi elektronik: UU No. 11 Tahun 2008 tentang Informasi & Transaksi Elektronik*. Media Nusa Creative.
- Harahap, M. Y. (2002). *Pembahasan permasalahan dan penerapan KUHP: Pemeriksaan sidang pengadilan, banding, kasasi, dan peninjauan kembali*. Jakarta: Sinar Grafika.
- Heryogi, A., Ruba'i, M., & Sugiri, B. (2017). Fungsi bukti elektronik dalam hukum acara pidana pasca putusan Mahkamah Konstitusi Nomor 20/PUU-XIV/2016. *Jurnal Ilmiah Pendidikan Pancasila dan Kewarganegaraan*, 2(1), 7–17.
- Hiariej, E. O. S. (2013). *Teori dan hukum pembuktian*. Jakarta: Erlangga.
- Hidayat, A. R. (2021). *Analisis urgensi pemeriksaan digital forensic pada persidangan tindak pidana informasi dan transaksi elektronik (ITE) perkara melanggar kesusilaan dan relevansinya dengan pertimbangan hukum hakim dalam menjatuhkan putusan (Studi Putusan Nomor: 120/Pid. Sus/2020/PN SKH)* [Skripsi tidak diterbitkan].
- Holt, T. J., Bossler, A. M., & Seigfried-Spellar, K. C. (2022). *Cybercrime and digital forensics: An introduction* (3rd ed.). Routledge.
- Huda, M. N. (2017). Pentingnya alat bukti dalam pembuktian minim saksi. *Voice Justisia: Jurnal Hukum dan Keadilan*, 1(2), 95–107.
- Imron, A., & Iqbal, M. (2019). *Hukum pembuktian*. Surabaya: LaksBang Pressindo.
- Isma, N. L., & Koyimatun, A. (2014). Kekuatan pembuktian alat bukti informasi elektronik pada dokumen elektronik serta hasil cetaknya dalam pembuktian tindak pidana. *Jurnal Penelitian Hukum Gadjah Mada*, 1(2), 109–116.
- Makarim, E. (2005). *Kompilasi hukum telematika*. Jakarta: FH UI Press.
- Manggala, B. S., Putri, A., Suzeeta, N. S., Zalfa, N., Marpaung, V. C., Natalia, I. H., & Nugroho, A. A. (2024). Analisis yuridis peran digital forensik dalam pembuktian kasus penipuan berkedok investasi online (Studi Kasus Doni Salmanan). *Media Hukum Indonesia (MHI)*, 2(2), 295–301.
- Medeline, F., Rusmiati, E., & Ramadhani, R. H. (2022). Forensik digital dalam pembuktian tindak pidana ujaran kebencian di media sosial. *PAMPAS: Journal of Criminal Law*, 3(3), 310–325.
- Michael, P. I. A., & Cahyarini, L. L. (n.d.). Kekuatan verifikasi akibat cetakan (screenshot/printscreen) dan pertimbangan hakim pada aspek perkara perdata. *Notarius*, 17(1), 280–291.

- Mutiara, D., Mulyadi, D., & Galih, Y. S. (2024). Analisis yuridis terhadap pemeriksaan alat bukti elektronik berupa hasil screenshot handphone dihubungkan dengan Pasal 6 Undang-Undang Nomor 19 Tahun 2016 tentang Perubahan atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik. *Pustaka Galuh Justisi*, 2(2), 116–144.
- Ponno, J. D. (2023). Penerapan digital forensik dalam pembuktian pencemaran nama baik di dunia maya. *Lex Administratum*, 12(1).
- Prahara, S. (2022). *Pembuktian elektronik dan digital forensik di Indonesia*. Bengkulu: LPPM Universitas Bung Hatta.
- Sasangka, H., & Rosita, L. (2003). *Hukum pembuktian dalam perkara pidana: Untuk mahasiswa dan praktisi*. Mandar Maju.
- Suhariyanto, B. (2013). *Tindak pidana teknologi informasi (Cybercrime): Urgensi pengaturan dan celah hukumnya*. Jakarta: Prestasi Pustaka Publisher.
- Sutarman, H., Widiani, I. G., & Amin, I. (2007). *Cyber crime: Modus operandi dan penanggulangannya*. LaksBang Pressindo.