Rewang Rencang : Jurnal Hukum Lex Generalis. Vol.7. No.7 (2026)
Tema/Edisi : Pidana (Bulan Tujuh)
https://jhlg.rewangrencang.com/

KEABSAHAN ALAT BUKTI DIGITAL DALAM PEMBUKTIAN KASUS *PHANTOM HACKER SCAM*

THE VALIDITY OF DIGITAL EVIDENCE IN PROVING PHANTOM HACKER SCAM CASES

Tegar San Putra, Sigit Sapto N. dan Meirza Aulia C.

Fakultas Hukum Universitas Merdeka Madiun

Korespondensi Penulis : Tegarsanputra@gmail.com

Citation Structure Recommendation :

Putra, Tegar San, Sigit Sapto N. dan Meirza Aulia C.. *Keabsahan Alat Bukti Digital dalam Pembuktian Kasus Phantom Hacker Scam*. Rewang Rencang : Jurnal Hukum Lex Generalis. Vol.7. No.7 (2026).

ABSTRAK

Penelitian ini mengkaji keabsahan alat bukti digital dalam pembuktian kasus *phantom hacker scam*, yaitu bentuk kejahatan siber yang dilakukan dengan manipulasi identitas digital dan jejak elektronik palsu untuk menipu korban. Objek riset dalam penelitian ini adalah alat bukti digital yang digunakan dalam proses penegakan hukum terhadap tindak pidana penipuan berbasis teknologi informasi. Tujuan penelitian ini adalah untuk menganalisis pengaturan hukum terkait alat bukti digital serta menilai kekuatan pembuktiannya dalam mengungkap dan membuktikan kasus *phantom hacker scam*. Metode penelitian yang digunakan adalah penelitian hukum normatif dengan pendekatan perundang-undangan dan pendekatan konseptual, melalui pengkajian ketentuan hukum pidana, hukum acara pidana, serta Undang-Undang Informasi dan Transaksi Elektronik. Hasil penelitian menunjukkan bahwa alat bukti digital memiliki keabsahan hukum sepanjang diperoleh dan dikelola sesuai dengan prinsip legalitas, integritas, dan autentikasi sebagaimana diatur dalam peraturan perundang-undangan. Namun demikian, pembuktian kasus *phantom hacker scam* menghadapi tantangan teknis dan yuridis, khususnya terkait validitas forensik digital dan keterkaitan alat bukti dengan pelaku. Oleh karena itu, penguatan kapasitas penegak hukum dan standar pembuktian digital menjadi faktor penting dalam menjamin efektivitas penegakan hukum kejahatan siber.

Kata Kunci: Alat Bukti Digital, Keabsahan Hukum, Kejahatan Siber, Pembuktian Pidana, *Phantom Hacker Scam*

ABSTRACT

This study examines the validity of digital evidence in proving cases of phantom hacker scams, a form of cybercrime committed by manipulating digital identities and false electronic footprints to deceive victims. The object of this study is digital evidence used in law enforcement against information technology-based fraud. The purpose of this study is to analyze the legal regulations related to digital evidence and assess its evidentiary strength in uncovering and proving cases of

phantom hacker fraud. The research method used is normative legal research with a regulatory and contextual approach, through an examination of provisions of criminal law, criminal procedure law and the Information and Electronic Transactions Law. The results show that digital evidence has legal validity as long as it is obtained and managed in accordance with the principles of legality, integrity, and authentication as stipulated in the legislation. However, proving cases of phantom hacker scams faces technical and legal challenges, particularly regarding the validity of digital forensics and the linkage of evidence to the perpetrator. Therefore, strengthening law enforcement capacity and digital evidence standards are important factors in ensuring the effectiveness of cybercrime law enforcement.
Keywords : Digital Evidence, Legal Validity, Cybercrime, Criminal Proof, Phantom Hacker Scam

A. PENDAHULUAN

Perkembangan teknologi informasi dan komunikasi telah membawa perubahan signifikan dalam pola kejahatan, khususnya kejahatan siber yang semakin kompleks dan sulit dideteksi. Salah satu bentuk kejahatan siber yang berkembang adalah *phantom hacker scam*, yaitu modus penipuan yang memanfaatkan rekayasa identitas digital, manipulasi sistem elektronik, dan jejak data palsu sehingga pelaku seolah tidak memiliki keberadaan nyata di ruang digital. Kejahatan ini tidak hanya menimbulkan kerugian ekonomi bagi korban, tetapi juga menghadirkan tantangan serius dalam proses pembuktian hukum karena alat bukti yang digunakan sepenuhnya berbasis elektronik.[1]

Kondisi tersebut menuntut adanya penyesuaian dalam sistem pembuktian hukum pidana, khususnya terkait pengakuan dan penilaian terhadap alat bukti digital. Dalam praktik peradilan, alat bukti digital seperti rekaman elektronik, data transaksi, log sistem, dan jejak aktivitas jaringan menjadi instrumen utama untuk mengungkap tindak pidana siber. Namun, penggunaan alat bukti digital masih menghadapi berbagai permasalahan yuridis, antara lain terkait keabsahan perolehan alat bukti, jaminan keutuhan dan keaslian data, serta keterkaitan antara alat bukti elektronik dengan subjek hukum pelaku kejahatan.[2]

---

[1] Elvina Tanoto, Jesslyn Tandy, dan Ricky Banke, *Kekuatan Alat Bukti Elektronik dalam Proses Pembuktian di Peradilan Pidana*, Jurnal Ilmu Hukum, Vol.2, No.1 (Oktober 2024), p.90–96.

[2] Arya Made Permana dan I Putu Rasmadi Arsha Putra, *Upaya Peningkatan Akses Keadilan terhadap Penerima Bantuan Hukum di Indonesia Melalui Paralegal*, Jurnal Ilmiah Kebijakan Hukum, Vol.17, No.22 (Januari-Juni 2023), p.221–34.

Permasalahan ini semakin kompleks dalam kasus *phantom hacker scam* karena pelaku secara sengaja menyamarkan identitas dan menggunakan teknologi untuk mengaburkan jejak digital, sehingga menuntut penerapan standar forensik digital dan pembuktian yang lebih ketat.[3] Oleh karena itu, kajian mengenai keabsahan alat bukti digital menjadi penting untuk memastikan bahwa proses pembuktian tetap menjunjung prinsip kepastian hukum, keadilan, dan perlindungan hak asasi manusia dalam penegakan hukum terhadap kejahatan siber.[4]

Dalam sistem peradilan pidana Indonesia, secara *de jure* alat bukti digital telah diakui sebagai alat bukti yang sah melalui Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik sebagaimana telah diubah dengan Undang-Undang Nomor 19 Tahun 2016, yang menyatakan bahwa informasi elektronik dan/atau dokumen elektronik merupakan alat bukti hukum yang sah. Selain itu, Pasal 184 KUHAP mengatur jenis alat bukti dalam hukum acara pidana, yaitu keterangan saksi, keterangan ahli, surat, petunjuk, dan keterangan terdakwa, yang dalam praktiknya dapat diperluas dengan alat bukti elektronik. Namun secara *de facto*, dalam praktik peradilan masih sering terjadi perbedaan penafsiran mengenai keabsahan alat bukti digital, terutama terkait proses perolehan, autentikasi, integritas data, serta hubungan antara alat bukti dengan pelaku. Ketidaksesuaian antara ketentuan normatif dan praktik di lapangan ini menimbulkan ketidakpastian hukum dalam pembuktian perkara kejahatan siber.

Permasalahan tersebut dapat dilihat dalam beberapa kasus penipuan berbasis teknologi, salah satunya kasus penipuan online yang melibatkan penggunaan akun palsu dan server luar negeri sehingga menyulitkan penegak hukum dalam membuktikan identitas pelaku. Dalam kasus tersebut, bukti berupa rekaman percakapan digital dan data transaksi sempat dipersoalkan keabsahannya karena tidak seluruh proses pengambilan data dilakukan sesuai prosedur forensik digital.

---

[3] Nurul Aini dan Fauziah Lubis, *Tantangan Pembuktian dalam Kasus Kejahatan Siber*, Jurnal Hukum, Vol.5, No.2 (Juli 2024), p.55–63.

[4] Pramukhtiko Suryo Kencono dan Ajeng Dwi Wahyuni, *Keabsahan Perolehan Alat Bukti Elektronik Sebagai Konsep Perluasan Objek Praperadilan*, Fairness and Justice : Jurnal Ilmiah Ilmu Hukum, Vol.23, No.1 (Mei 2025), p.24–32.

Hal ini menunjukkan bahwa meskipun secara normatif alat bukti digital telah diakui, namun dalam praktiknya masih terdapat kendala dalam pembuktian, terutama pada kasus yang melibatkan anonimitas dan manipulasi identitas digital seperti *phantom hacker scam*.

Secara normatif, aturan yang sering menjadi permasalahan adalah ketentuan dalam Pasal 5 dan Pasal 44 Undang-Undang Informasi dan Transaksi Elektronik yang mengatur tentang pengakuan alat bukti elektronik, serta Pasal 184 KUHAP yang belum secara eksplisit mengatur alat bukti digital. Selain itu, belum adanya standar teknis yang rinci mengenai prosedur forensik digital dan *chain of custody* menyebabkan perbedaan penerapan dalam praktik peradilan. Akibatnya, hakim sering menghadapi kesulitan dalam menilai kekuatan pembuktian alat bukti elektronik, terutama ketika data diperoleh dari sistem luar negeri atau melalui teknologi anonimitas.

Beberapa penelitian terdahulu telah membahas mengenai alat bukti digital dalam tindak pidana siber. Penelitian pertama menyatakan bahwa alat bukti elektronik telah diakui dalam hukum Indonesia, namun masih memerlukan penguatan dalam aspek teknis pembuktian. Penelitian kedua menegaskan bahwa penggunaan forensik digital sangat penting dalam mengungkap kejahatan siber, tetapi belum semua aparat penegak hukum memiliki kemampuan yang memadai. Penelitian ketiga menjelaskan bahwa kejahatan berbasis teknologi sering melibatkan lintas negara sehingga menyulitkan proses pembuktian di pengadilan. Penelitian keempat menyimpulkan bahwa meskipun regulasi sudah ada, namun implementasi di lapangan masih belum optimal karena belum adanya standar yang seragam dalam penilaian alat bukti elektronik.

Berbeda dengan penelitian sebelumnya, penelitian ini secara khusus mengkaji keabsahan alat bukti digital dalam pembuktian kasus *phantom hacker scam*, yang memiliki tingkat kompleksitas lebih tinggi karena melibatkan penyamaran identitas, manipulasi data, serta penggunaan teknologi anonimitas. Penelitian ini juga menyoroti kesenjangan antara ketentuan hukum secara normatif dengan praktik di lapangan, sehingga diharapkan dapat memberikan kontribusi dalam pengembangan hukum pembuktian pidana di era digital.

Berdasarkan uraian tersebut, tujuan penelitian ini adalah untuk menganalisis keabsahan alat bukti digital dalam pembuktian tindak pidana *phantom hacker scam*, mengkaji permasalahan yang timbul antara ketentuan hukum secara *de jure* dengan praktik *de facto*, serta memberikan rekomendasi mengenai standar pembuktian yang dapat menjamin kepastian hukum, keadilan, dan efektivitas penegakan hukum dalam menghadapi kejahatan siber yang semakin kompleks.

Kondisi tersebut menimbulkan tantangan serius bagi aparat penegak hukum dalam membuktikan unsur kesalahan pelaku secara meyakinkan di persidangan. Alat bukti digital yang diajukan harus mampu menunjukkan bahwa data elektronik diperoleh melalui cara yang sah, tidak mengalami perubahan sejak pertama kali dikumpulkan, serta memiliki relevansi langsung dengan perbuatan pidana yang didakwakan[5]. Dalam konteks *phantom hacker scam*, kesulitan pembuktian semakin meningkat karena penggunaan teknologi anonimitas, pemalsuan identitas digital, dan pemanfaatan jaringan lintas negara yang kerap mengaburkan hubungan kausal antara perbuatan, alat bukti, dan pelaku. Akibatnya, meskipun secara normatif alat bukti digital telah diakui dalam sistem hukum pidana Indonesia, efektivitas penggunaannya sangat bergantung pada ketepatan prosedur perolehan bukti, kemampuan teknis aparat dalam melakukan analisis forensik digital, serta kecermatan hakim dalam menilai keabsahan dan kekuatan pembuktian alat bukti tersebut. Oleh karena itu, kajian mengenai keabsahan alat bukti digital dalam pembuktian kasus *phantom hacker scam* menjadi penting untuk memastikan bahwa perkembangan hukum pembuktian mampu mengimbangi dinamika kejahatan siber yang terus berkembang.

Penelitian-penelitian terdahulu menunjukkan bahwa tantangan utama dalam pembuktian kejahatan siber terletak pada aspek forensik digital dan kemampuan penegak hukum dalam menjaga rantai penguasaan (*chain of custody*) alat bukti elektronik. Beberapa kajian juga menegaskan bahwa meskipun alat bukti digital telah diakui secara normatif, masih terdapat kesenjangan antara pengaturan hukum dan penerapannya di tingkat praktik peradilan.

[5] Ni Made Trisma Dewi dan Reido Lardiza Fahrial, *Suatu Kajian Yuridis terhadap Penggunaan Alat Bukti Elektronik dalam Kejahatan Cyber dalam Sistem Penegakan Hukum*, Jurnal Hukum Saraswati (JHS), Vol.3, No.2 (September 2021), p.11–25.

Perkembangan kajian keilmuan saat ini menekankan pentingnya standar pembuktian digital yang menjamin keandalan alat bukti sekaligus melindungi hak asasi tersangka dan korban dalam proses peradilan pidana. Standar itu mencakup pengaturan yang jelas mengenai tata cara perolehan, pengamanan, pemeriksaan, dan penyajian alat bukti digital agar tidak menimbulkan pelanggaran hak privasi, penyalahgunaan kewenangan dan kesalahan penafsiran terhadap data elektronik. Selain itu, prinsip *due process of law* harus menjadi landasan utama, sehingga setiap tindakan penyitaan, penggeledahan sistem elektronik, serta analisis data digital dilakukan berdasarkan izin dan mekanisme hukum yang sah. Bagi tersangka, standar pembuktian digital berfungsi sebagai jaminan perlindungan dari tuduhan yang didasarkan pada alat bukti yang tidak autentik atau telah dimanipulasi, sedangkan bagi korban, standar tersebut memberikan kepastian hukum bahwa laporan dan bukti digital yang diajukan akan dinilai secara objektif dan profesional. Dengan demikian, keseimbangan antara efektivitas penegakan hukum dan perlindungan hak asasi manusia dapat terwujud, khususnya dalam penanganan tindak pidana siber yang kompleks dan terus berkembang.

Beberapa penelitian terdahulu telah mengkaji mengenai penggunaan alat bukti digital dalam tindak pidana siber. Penelitian pertama menjelaskan bahwa pengakuan alat bukti elektronik dalam Undang-Undang Informasi dan Transaksi Elektronik telah memberikan dasar hukum yang kuat, namun belum diikuti dengan pengaturan teknis yang rinci mengenai prosedur forensik digital dalam pembuktian di pengadilan. Penelitian kedua menyatakan bahwa kendala utama dalam pembuktian kejahatan siber terletak pada kemampuan aparat penegak hukum dalam menjaga integritas data elektronik serta memastikan keaslian alat bukti sejak tahap penyidikan hingga persidangan. Penelitian ketiga menunjukkan bahwa perkara kejahatan siber yang melibatkan jaringan lintas negara sering mengalami kesulitan pembuktian karena perbedaan yurisdiksi dan keterbatasan akses terhadap data digital yang berada di luar wilayah hukum Indonesia. Penelitian keempat menegaskan bahwa meskipun prinsip *chain of custody* telah dikenal dalam praktik forensik digital, penerapannya di Indonesia belum dilakukan secara konsisten sehingga sering menimbulkan perdebatan mengenai keabsahan alat bukti elektronik di persidangan.

Meskipun penelitian-penelitian tersebut telah memberikan kontribusi penting dalam kajian hukum pembuktian tindak pidana siber, sebagian besar masih membahas alat bukti digital secara umum dan belum secara khusus mengkaji keabsahan alat bukti digital dalam kasus *phantom hacker scam* yang memiliki karakteristik lebih kompleks karena melibatkan penyamaran identitas, manipulasi sistem elektronik, serta penggunaan teknologi anonimitas untuk menghilangkan jejak pelaku. Selain itu, penelitian sebelumnya lebih banyak menitikberatkan pada aspek normatif, sedangkan penelitian ini tidak hanya mengkaji ketentuan hukum secara de jure, tetapi juga menganalisis penerapannya secara de facto dalam praktik peradilan pidana. Oleh karena itu, penelitian ini memiliki kebaruan karena secara khusus menelaah keabsahan alat bukti digital dalam pembuktian kasus *phantom hacker scam* dengan menekankan pada kesesuaian antara ketentuan hukum, standar forensik digital, dan praktik pembuktian di pengadilan, sehingga diharapkan dapat memberikan kontribusi dalam pengembangan hukum pembuktian pidana di era kejahatan siber yang semakin kompleks.

Berdasarkan kondisi tersebut, penelitian ini dilakukan untuk mengkaji keabsahan alat bukti digital dalam pembuktian kasus *phantom hacker scam* serta menilai sejauh mana alat bukti tersebut memiliki kekuatan pembuktian dalam proses peradilan pidana. Penelitian ini bertujuan untuk memberikan pemahaman yang komprehensif mengenai dasar hukum penggunaan alat bukti digital dan mengidentifikasi tantangan yuridis yang muncul dalam pembuktian kejahatan siber, sehingga dapat memberikan kontribusi teoritis dan praktis bagi pengembangan hukum pembuktian di Indonesia. Melalui kajian normatif yang menitikberatkan pada analisis peraturan perundang-undangan, doktrin hukum, dan

perkembangan putusan pengadilan terkait pembuktian elektronik, penelitian ini berupaya menempatkan alat bukti digital dalam kerangka hukum acara pidana yang adaptif terhadap perkembangan teknologi. Fokus kajian diarahkan pada penilaian kesesuaian antara ketentuan normatif dan praktik penegakan hukum, khususnya dalam menjamin keabsahan, keandalan, dan keterkaitan alat bukti digital dengan perbuatan pidana yang didakwakan.

Dengan demikian, penelitian ini diharapkan mampu memberikan gambaran yang sistematis mengenai batasan dan standar penggunaan alat bukti digital dalam perkara kejahatan siber, sekaligus menawarkan landasan konseptual bagi penguatan sistem pembuktian pidana yang responsif terhadap tantangan kejahatan berbasis teknologi informasi.

Berdasarkan uraian pada pendahuluan, maka rumusan masalah dalam penelitian ini adalah:

1. Apakah pengaturan hukum terkait alat bukti digital dalam sistem pidana di Indonesia khususnya dalam pembuktian tindak *cyber* seperti *phantom hacker scam*?
2. Apa kriteria keabsahan dan kekuatan pembuktian alat bukti digital dalam mengungkapkan tindak pidana *phantom hacker scam*?

B. PEMBAHASAN

1. Pengaturan Hukum Terkait Alat Bukti Digital dalam Sistem Pidana di Indonesia Khususnya dalam Pembuktian Tindak *Cyber* Seperti *Phantom Hacker Scam*

Pengaturan hukum terkait alat bukti digital dalam sistem peradilan pidana di Indonesia telah mengalami perkembangan signifikan, terutama setelah berlakunya Undang-Undang Informasi dan Transaksi Elektronik beserta peraturan pelaksananya. Berdasarkan hasil penelusuran terhadap peraturan perundang-undangan, alat bukti digital secara normatif diakui sebagai alat bukti yang sah dan memiliki kedudukan hukum yang setara dengan alat bukti konvensional, sepanjang memenuhi persyaratan tertentu. Dalam konteks pembuktian tindak pidana siber seperti *phantom hacker scam*, alat bukti digital menjadi instrumen utama karena karakteristik kejahatan yang sepenuhnya berlangsung dalam ruang siber. Data yang diperoleh dari analisis dokumen hukum menunjukkan bahwa sistem pembuktian pidana Indonesia telah membuka ruang penggunaan informasi dan dokumen elektronik, termasuk hasil cetaknya, sebagai alat bukti yang sah, meskipun pengaturannya masih memerlukan penafsiran yang cermat dalam praktik peradilan.

Pengakuan normatif terhadap alat bukti digital belum sepenuhnya diimbangi dengan keseragaman penerapan di tingkat praktik peradilan. Masih ditemukan perbedaan pandangan aparat penegak hukum dan hakim dalam menilai keabsahan, kekuatan pembuktian, serta relevansi alat bukti digital dengan unsur tindak pidana yang didakwakan. Hal ini terutama berkaitan dengan aspek teknis seperti proses perolehan alat bukti, pemeliharaan integritas data, dan pembuktian keterkaitan antara bukti digital dengan pelaku kejahatan. Dalam kasus *phantom hacker scam*, kompleksitas pembuktian semakin meningkat karena pelaku kerap memanfaatkan teknologi penyamaran identitas, lintas yurisdiksi, serta infrastruktur digital yang sulit dilacak. Akibatnya, alat bukti digital sering kali membutuhkan dukungan keterangan ahli forensik digital untuk memperkuat nilai pembuktiannya di persidangan. Oleh karena itu, penelitian ini menegaskan pentingnya penguatan kerangka hukum dan pedoman teknis yang lebih rinci, guna memastikan alat bukti digital dapat digunakan secara optimal, konsisten, dan berkeadilan dalam sistem peradilan pidana Indonesia.

Keabsahan alat bukti digital dalam pengungkapan tindak pidana *phantom hacker scam* sangat ditentukan oleh proses perolehan dan pengelolaannya. Berdasarkan analisis terhadap literatur hukum dan putusan pengadilan yang relevan, alat bukti digital dinyatakan sah apabila diperoleh secara legal, tidak melanggar hak privasi, serta dijaga keutuhan dan keasliannya sejak tahap penyidikan hingga persidangan. Data observasi terhadap praktik penegakan hukum menunjukkan bahwa aparat penegak hukum umumnya menggunakan alat bukti berupa rekaman transaksi elektronik, jejak alamat protokol internet, data komunikasi digital, dan hasil analisis forensik digital. Namun, penelitian menemukan bahwa tidak seluruh alat bukti tersebut secara otomatis memiliki kekuatan pembuktian yang kuat apabila tidak disertai dengan penjelasan teknis dan keterangan ahli yang mampu menghubungkan data digital dengan perbuatan dan pelaku tindak pidana.

Selain aspek keabsahan, bahwa kekuatan pembuktian alat bukti digital dalam perkara *phantom hacker scam* sangat bergantung pada keterkaitannya dengan alat bukti lain. Berdasarkan hasil telaah putusan pengadilan, alat bukti digital jarang berdiri sendiri, melainkan harus didukung oleh keterangan saksi,

keterangan ahli forensik digital, serta alat bukti lain yang relevan untuk membentuk keyakinan hakim. Temuan ini menunjukkan bahwa meskipun alat bukti digital memiliki peran sentral dalam mengungkap kejahatan siber, sistem pembuktian pidana Indonesia masih menganut prinsip pembuktian yang menekankan pada keterpaduan antaralat bukti. Dengan demikian, hasil penelitian menegaskan bahwa keberhasilan pembuktian tindak pidana *phantom hacker scam* tidak hanya ditentukan oleh keberadaan alat bukti digital, tetapi juga oleh kualitas, keabsahan, dan integrasi alat bukti tersebut dalam keseluruhan proses pembuktian di persidangan.

Implikasi dari temuan tersebut adalah perlunya pendekatan pembuktian yang komprehensif dan holistik dalam penanganan perkara *phantom hacker scam*. Alat bukti digital harus diposisikan sebagai bagian dari satu rangkaian pembuktian yang saling melengkapi, bukan sebagai satu-satunya dasar penentuan kesalahan terdakwa. Oleh karena itu, peran keterangan ahli forensik digital menjadi sangat strategis untuk menjelaskan proses perolehan, analisis, dan validitas data elektronik agar dapat dipahami secara rasional oleh hakim. Selain itu, sinkronisasi antara alat bukti digital dengan alat bukti lain, seperti dokumen pendukung, rekam jejak transaksi, serta keterangan saksi yang relevan, menjadi faktor penentu dalam membangun konstruksi pembuktian yang kuat. Dengan demikian, penelitian ini menegaskan bahwa optimalisasi pembuktian dalam perkara *phantom hacker scam* menuntut tidak hanya pengakuan normatif terhadap alat bukti digital, tetapi juga peningkatan kualitas penilaian dan integrasi pembuktian dalam praktik peradilan pidana.

2. Kriteria Keabsahan dan Kekuatan Pembuktian Alat Bukti Digital dalam Mengungkapkan Tindak Pidana *Phantom Hacker Scam*

Dalam sistem hukum acara pidana Indonesia, penilaian terhadap keabsahan dan kekuatan pembuktian alat bukti merupakan kewenangan hakim yang didasarkan pada ketentuan Kitab Undang-Undang Hukum Acara Pidana (KUHAP). Pasal 184 KUHAP menyebutkan bahwa alat bukti yang sah terdiri dari keterangan saksi, keterangan ahli, surat, petunjuk, dan keterangan terdakwa. Namun perkembangan teknologi informasi menyebabkan munculnya alat bukti baru berupa informasi elektronik dan/atau dokumen elektronik yang diakui

sebagai alat bukti yang sah berdasarkan Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik sebagaimana telah diubah dengan Undang-Undang Nomor 19 Tahun 2016. Meskipun demikian, pengakuan secara normatif tersebut belum sepenuhnya diikuti dengan pengaturan teknis yang rinci dalam KUHAP mengenai tata cara penilaian alat bukti digital, sehingga dalam praktik peradilan hakim memiliki peran yang sangat menentukan dalam menilai keabsahan alat bukti elektronik.

Berdasarkan Pasal 183 KUHAP, hakim tidak boleh menjatuhkan pidana kepada seseorang kecuali apabila dengan sekurang-kurangnya dua alat bukti yang sah ia memperoleh keyakinan bahwa suatu tindak pidana benar-benar terjadi dan terdakwalah yang bersalah melakukannya. Ketentuan ini menunjukkan bahwa kekuatan pembuktian tidak hanya ditentukan oleh jenis alat bukti, tetapi juga oleh keyakinan hakim yang dibangun melalui penilaian terhadap keaslian, relevansi, dan keterkaitan alat bukti dengan peristiwa pidana. Dalam konteks alat bukti digital, hakim harus menilai apakah data elektronik diperoleh secara sah, apakah data tersebut tidak mengalami perubahan sejak pertama kali diperoleh, serta apakah terdapat hubungan yang jelas antara data tersebut dengan pelaku tindak pidana. Oleh karena itu, keabsahan alat bukti digital sangat bergantung pada penerapan prinsip *chain of custody*, yaitu rangkaian prosedur yang menjamin bahwa alat bukti sejak ditemukan, disimpan, dianalisis, hingga diajukan di persidangan tetap dalam kondisi utuh dan dapat dipertanggungjawabkan.

Permasalahan menjadi lebih kompleks dalam kasus *phantom hacker scam*, karena pelaku menggunakan teknik anonimitas, pemalsuan identitas digital, penggunaan server luar negeri, serta manipulasi data elektronik untuk menghilangkan jejak. Dalam kondisi demikian, alat bukti digital sering kali menjadi satu-satunya alat bukti yang dapat digunakan untuk mengungkap tindak pidana. Namun apabila proses perolehan alat bukti tidak sesuai dengan prosedur hukum, maka alat bukti tersebut dapat dinyatakan tidak sah dan tidak memiliki kekuatan pembuktian. Oleh karena itu, kewenangan hakim dalam menilai keabsahan alat bukti menjadi sangat penting, karena hakim harus mempertimbangkan keseimbangan antara kepentingan penegakan hukum dan perlindungan hak asasi manusia, sesuai dengan prinsip *due process of law*.

Dalam perspektif kriminologi modern, kejahatan siber seperti *phantom hacker scam* dapat dianalisis menggunakan teori *Routine Activity Theory*, yang menyatakan bahwa kejahatan terjadi karena adanya pertemuan antara pelaku yang termotivasi, target yang rentan, dan lemahnya pengawasan. Perkembangan teknologi digital menyebabkan pengawasan menjadi semakin sulit sehingga peluang terjadinya kejahatan meningkat. Selain itu, teori *Cybercrime Theory* dalam kriminologi modern menjelaskan bahwa pelaku kejahatan siber memanfaatkan anonimitas, kecepatan, dan jangkauan global internet untuk menghindari deteksi, sehingga proses pembuktian membutuhkan pendekatan forensik digital yang lebih ketat dibandingkan kejahatan konvensional. Teori *Social Engineering* juga relevan dalam kasus *phantom hacker scam*, karena pelaku tidak hanya menggunakan teknologi, tetapi juga memanipulasi psikologis korban melalui rekayasa identitas digital.

Berdasarkan analisis hukum acara pidana dan teori kriminologi modern, dapat disimpulkan bahwa kriteria keabsahan alat bukti digital dalam kasus *phantom hacker scam* harus memenuhi beberapa unsur, yaitu diperoleh melalui prosedur yang sah, dijaga keutuhan dan keasliannya melalui prinsip *chain of custody*, dianalisis menggunakan metode forensik digital yang dapat dipertanggungjawabkan secara ilmiah, serta memiliki keterkaitan yang jelas dengan pelaku tindak pidana. Selain itu, hakim memiliki kewenangan penuh untuk menilai kekuatan pembuktian alat bukti berdasarkan keyakinan yang didukung oleh sekurang-kurangnya dua alat bukti yang sah sebagaimana diatur dalam KUHAP. Dengan demikian, efektivitas pembuktian dalam perkara kejahatan siber sangat bergantung pada kemampuan aparat penegak hukum dalam mengelola alat bukti digital serta kecermatan hakim dalam menilai keabsahan dan kekuatan pembuktiannya.

Pengaturan hukum terkait alat bukti digital dalam sistem peradilan pidana Indonesia menunjukkan adanya upaya adaptasi hukum terhadap perkembangan teknologi informasi. Keberadaan informasi dan dokumen elektronik sebagai alat bukti yang sah mencerminkan pengakuan negara bahwa kejahatan modern, khususnya kejahatan siber seperti *phantom hacker scam*, tidak dapat lagi dibuktikan hanya dengan instrumen konvensional. Adapun dalam konteks ini,

hukum pembuktian pidana mengalami perluasan makna alat bukti yang bersifat dinamis dan fungsional, tanpa menghilangkan prinsip kehati-hatian dalam menjamin kepastian dan keadilan hukum[6]. Pengakuan normatif tersebut sekaligus menunjukkan bahwa tujuan penelitian, yakni mengkaji dasar hukum penggunaan alat bukti digital, telah tercapai melalui penelusuran dan penafsiran sistematis terhadap peraturan yang berlaku.

Lebih lanjut, efektivitas penerapan alat bukti digital sangat bergantung pada kemampuan aparat penegak hukum dalam memahami karakteristik bukti elektronik yang berbeda dengan bukti konvensional. Bukti digital memiliki sifat mudah berubah, mudah disalin, dan sangat bergantung pada sistem teknologi tertentu, sehingga memerlukan prosedur khusus dalam proses pengumpulan, penyimpanan, serta penyajiannya di persidangan. Oleh karena itu, keberadaan standar forensik digital dan keahlian penyidik menjadi faktor penting agar alat bukti elektronik dapat dipertanggungjawabkan secara hukum. Tanpa adanya pemahaman teknis yang memadai, alat bukti digital berpotensi dipersoalkan keabsahannya dan justru melemahkan proses pembuktian.

Di sisi lain, meskipun regulasi telah mengakui kedudukan alat bukti elektronik, masih terdapat tantangan yuridis dalam implementasinya. Beberapa permasalahan yang sering muncul antara lain terkait keaslian data, rantai penguasaan barang bukti (*chain of custody*), serta yurisdiksi hukum ketika pelaku kejahatan berada di luar wilayah Indonesia. Kasus *phantom hacker scam* menjadi contoh nyata bahwa pembuktian tindak pidana siber memerlukan koordinasi lintas lembaga, baik antara kepolisian, penyedia layanan digital, maupun otoritas internasional. Hal ini menunjukkan bahwa pengaturan hukum yang ada perlu terus diperkuat dengan kebijakan teknis dan kerja sama kelembagaan yang lebih terintegrasi.

Analisis menunjukkan bahwa pengaturan alat bukti digital tidak hanya bersumber dari Undang-Undang Informasi dan Transaksi Elektronik, tetapi juga berkaitan erat dengan ketentuan dalam Kitab Undang-Undang Hukum Acara Pidana serta putusan-putusan pengadilan yang mulai mengakomodasi

[6] Dino Rizka Afdhali dan Handar Subhandi Bakhtiar, *Tinjauan Yuridis Pengaturan Pembuktian Ilmiah dalam Produk Hukum Positif di Indonesia*, Indonesian Journal of Law, Vol.1, No.10 (Oktober 2024), p.267–73.

perkembangan teknologi informasi. Penafsiran sistematis terhadap norma-norma tersebut memperlihatkan adanya upaya harmonisasi antara hukum acara pidana konvensional dan kebutuhan pembuktian modern berbasis digital. Dengan demikian, dasar hukum penggunaan alat bukti digital dapat dipahami secara komprehensif, baik dari aspek formil maupun materil, sehingga memberikan kepastian hukum bagi aparat penegak hukum dalam proses penyidikan, penuntutan, dan pemeriksaan di persidangan. Temuan ini sekaligus menegaskan bahwa meskipun kerangka hukum telah tersedia, diperlukan pemahaman yang mendalam dan konsisten agar penerapan alat bukti digital benar-benar selaras dengan tujuan keadilan dan perlindungan hukum dalam penanganan tindak pidana siber.

Namun demikian, pembahasan memperlihatkan bahwa pengakuan normatif saja belum cukup untuk menjamin efektivitas pembuktian dalam perkara *phantom hacker scam*. Kejahatan ini memiliki karakteristik khas berupa rekayasa identitas digital dan manipulasi data elektronik yang berpotensi mengaburkan hubungan antara pelaku dan perbuatan pidana. Oleh karena itu, keabsahan alat bukti digital tidak hanya ditentukan oleh bentuknya sebagai informasi elektronik, tetapi juga oleh proses perolehan, pengelolaan, dan penyajiannya di persidangan.[7] Aspek ini menegaskan bahwa tujuan penelitian untuk menilai sejauh mana kekuatan pembuktian alat bukti digital tercapai melalui analisis terhadap standar prosedural dan teknis yang harus dipenuhi.

Lebih jauh lagi, proses pembuktian dalam perkara *phantom hacker scam* menuntut adanya penerapan prinsip kehati-hatian yang tinggi, mengingat bukti digital sangat rentan terhadap perubahan, penghapusan, maupun pemalsuan. Setiap tahapan penanganan bukti mulai dari penyitaan perangkat elektronik, ekstraksi data, hingga analisis forensik, harus dilakukan sesuai dengan prosedur yang dapat dipertanggungjawabkan secara hukum. Apabila proses tersebut tidak memenuhi standar yang ditetapkan, maka alat bukti digital berpotensi kehilangan nilai pembuktiannya di hadapan hakim.

---

[7] Mohamad Azhan Yahya, Ahmad Azam dan Mohd Shariff, *Application Of Principles Of Chain Of Evidence And Chain Of Custody During Storage And Forensic Examination Of Electronic Documentary Evidence In Shariah Criminal Cases In Malaysia*, Ilmu Law Journal, Vol.31, No.1 (November 2023), p.145–66.

Hal ini menunjukkan bahwa keberhasilan pembuktian tidak hanya ditentukan oleh kecanggihan teknologi, tetapi juga oleh kepatuhan terhadap prosedur hukum acara pidana yang mengatur tata cara perolehan, pengelolaan, serta penyajian alat bukti digital di persidangan. Setiap tahapan proses pembuktian harus dilakukan secara transparan, akuntabel, dan sesuai dengan prinsip-prinsip legalitas agar alat bukti elektronik yang diajukan memiliki kekuatan hukum yang sah dan meyakinkan. Tanpa kepatuhan terhadap prosedur tersebut, bukti digital yang secara teknis akurat sekalipun dapat kehilangan nilai pembuktiannya karena dianggap cacat secara formil. Penerapan prosedur hukum acara pidana yang konsisten juga berfungsi untuk melindungi hak-hak para pihak dalam proses peradilan, baik tersangka, korban, maupun masyarakat secara umum. Dengan adanya mekanisme yang jelas dan terukur, potensi penyalahgunaan kewenangan dalam pengumpulan dan pemanfaatan data elektronik dapat diminimalisasi. Oleh karena itu, keseimbangan antara penggunaan teknologi modern dan penghormatan terhadap asas-asas hukum acara pidana menjadi faktor utama dalam menjamin bahwa pembuktian perkara kejahatan siber dapat berlangsung secara adil dan dapat dipertanggungjawabkan.

Selain itu, kompleksitas pembuktian juga muncul dari fakta bahwa pelaku *phantom hacker scam* sering kali menggunakan teknik enkripsi, akun anonim, serta jaringan komunikasi berlapis untuk menyembunyikan jejak digitalnya. Kondisi ini menyebabkan hubungan kausal antara bukti elektronik dengan identitas pelaku menjadi sulit dibuktikan secara langsung. Oleh sebab itu, pembuktian perkara semacam ini memerlukan kombinasi antara bukti digital, keterangan ahli, serta alat bukti pendukung lainnya agar dapat membentuk konstruksi pembuktian yang utuh. Tanpa adanya keterpaduan tersebut, hakim akan kesulitan memperoleh keyakinan yang cukup untuk menjatuhkan putusan. Dapat dipahami bahwa tantangan utama dalam pembuktian perkara *phantom hacker scam* terletak pada bagaimana menjamin integritas dan autentisitas alat bukti digital sejak tahap penyidikan hingga persidangan. Penelitian ini menunjukkan bahwa diperlukan pedoman teknis yang lebih rinci, peningkatan kapasitas forensik digital, serta harmonisasi antara regulasi hukum dan perkembangan teknologi.

Upaya tersebut menjadi sangat penting agar sistem pembuktian pidana Indonesia mampu menjawab dinamika kejahatan siber secara lebih efektif, adil, dan memberikan kepastian hukum bagi para pencari keadilan menunjukkan bahwa kriteria keabsahan alat bukti digital harus dipahami secara multidimensional, meliputi aspek yuridis dan teknis. Dari sisi yuridis, alat bukti digital harus diperoleh secara sah dan tidak melanggar hak asasi manusia, khususnya hak atas privasi. Dari sisi teknis, keandalan alat bukti sangat bergantung pada integritas data, rantai penguasaan (*chain of custody*), serta dukungan keterangan ahli forensik digital[8]. Tanpa pemenuhan aspek-aspek tersebut, alat bukti digital berpotensi kehilangan kekuatan pembuktiannya, meskipun secara normatif telah diakui sebagai alat bukti yang sah.

Sistem pembuktian pidana Indonesia masih menempatkan alat bukti digital sebagai bagian dari konstruksi pembuktian yang bersifat komplementer. Artinya, alat bukti digital tidak berdiri sendiri, melainkan harus dikaitkan dengan alat bukti lain untuk membentuk keyakinan hakim. Pendekatan ini sejalan dengan asas pembuktian yang menitikberatkan pada kualitas dan keterpaduan alat bukti, bukan semata-mata pada kecanggihan teknologi yang digunakan[9]. Dengan demikian, pembuktian perkara *phantom hacker scam* menuntut sinergi antara instrumen hukum, kemampuan teknis aparat penegak hukum, dan pemahaman hakim terhadap karakteristik kejahatan siber.

Dalam praktiknya, sinergi tersebut diwujudkan melalui pemanfaatan berbagai jenis alat bukti seperti keterangan saksi, keterangan ahli, petunjuk, serta barang bukti elektronik yang saling menguatkan satu sama lain. Bukti digital seperti rekaman aktivitas transaksi, jejak alamat IP, riwayat percakapan daring, maupun data log sistem hanya akan memiliki kekuatan pembuktian yang optimal apabila didukung oleh keterangan ahli forensik digital yang mampu menjelaskan proses perolehan dan keasliannya.

---

[8] Vina Putri Afisako, dkk., *Analisis Normatif terhadap Kekosongan Pengaturan Pedoman Teknis Alat Bukti Elektronik dalam Penanganan Kasus Kekerasan Seksual di Indonesia*, Jurnal Kajian Hukum dan Pendidikan Kewarganegaraan, Vol.2, No.1 (Oktober-Desember 2025), p.228–37.

[9] I Made Dwi Krisnanda, Madiasa Ablisar dan Mahmud Mulyadi, *Analisis Yuridis Bukti Digital (Digital Evidence) dalam Pembuktian Perkara Tindak Pidana Ujaran Kebencian pada Putusan Pengadilan Negeri Medan No. 3168/PID.SUS/2018/PN.MDN*, Res Nullius Law Journal, Vol.3, No.2 (Juli 2021), p.98–117.

Tanpa dukungan tersebut, alat bukti digital berpotensi dipandang lemah karena sifatnya yang sangat teknis dan rentan terhadap manipulasi. Oleh sebab itu, pembuktian perkara kejahatan siber menuntut pendekatan multidisipliner yang menggabungkan aspek hukum dan teknologi secara seimbang.

Selain itu, hakim sebagai pihak yang berwenang menilai alat bukti juga dituntut untuk memiliki pemahaman yang memadai mengenai karakteristik bukti elektronik. Kompleksitas perkara *phantom hacker scam* sering kali melibatkan metode kejahatan yang canggih, seperti penggunaan identitas palsu, penyamaran lokasi akses, hingga pemanfaatan perangkat lunak berbahaya. Kondisi ini mengharuskan hakim tidak hanya berpegang pada teks hukum semata, tetapi juga mampu memahami konstruksi teknis yang melatarbelakangi terjadinya tindak pidana. Dengan pemahaman tersebut, hakim dapat menilai relevansi, keabsahan, dan kekuatan pembuktian alat bukti digital secara lebih objektif dan proporsional.

Pembuktian yang bersifat komplementer ini juga menunjukkan pentingnya profesionalisme aparat penegak hukum sejak tahap penyidikan. Kesalahan prosedur dalam pengumpulan dan pengamanan bukti elektronik dapat berakibat fatal terhadap keseluruhan proses pembuktian di persidangan. Oleh karena itu, diperlukan pedoman operasional yang jelas mengenai tata cara penanganan bukti digital, mulai dari proses penyitaan, analisis forensik, hingga penyajian di muka persidangan. Dengan adanya standar prosedur yang baku, alat bukti digital dapat dihadirkan secara sah dan meyakinkan untuk mendukung terungkapnya kebenaran materiil. Dapat disimpulkan bahwa pembuktian perkara *phantom hacker scam* menuntut keterpaduan antara norma hukum, kemampuan teknis, serta integritas proses peradilan. Alat bukti digital memang memiliki peran yang semakin penting dalam mengungkap kejahatan siber, namun kedudukannya tetap harus ditempatkan dalam kerangka pembuktian yang menyeluruh dan berimbang. Pendekatan yang komprehensif ini diharapkan mampu menjamin tercapainya tujuan utama hukum pidana, yaitu menegakkan keadilan, kepastian hukum, dan perlindungan bagi masyarakat dari ancaman kejahatan berbasis teknologi informasi.

Lebih lanjut, dalam praktik peradilan, alat bukti digital seperti rekaman log aktivitas, riwayat transaksi elektronik, alamat IP, maupun data percakapan daring sering kali memerlukan dukungan keterangan ahli agar dapat dipahami secara utuh oleh hakim. Tanpa adanya penjelasan dari ahli forensik digital, bukti elektronik berpotensi hanya dipandang sebagai data mentah yang sulit diinterpretasikan secara hukum. Oleh karena itu, peran ahli menjadi sangat krusial untuk menerjemahkan aspek teknis ke dalam bahasa hukum yang dapat dipertanggungjawabkan. Hal ini menunjukkan bahwa pembuktian tindak pidana siber tidak hanya bertumpu pada keberadaan bukti, tetapi juga pada validitas proses pengolahannya.

Selain itu, karakter lintas batas (*borderless*) dari kejahatan *phantom hacker scam* juga menimbulkan tantangan tersendiri dalam proses pembuktian. Banyak pelaku kejahatan siber beroperasi dari luar negeri dengan menggunakan server asing, jaringan privat virtual (VPN), maupun teknik penyamaran identitas lainnya. Kondisi ini menyebabkan alat bukti digital sering kali berada di luar yurisdiksi hukum Indonesia sehingga membutuhkan kerja sama internasional melalui mekanisme bantuan hukum timbal balik (*mutual legal assistance*). Tanpa dukungan mekanisme tersebut, proses pembuktian dapat terhambat dan berdampak pada sulitnya penegakan hukum secara optimal.

Dengan demikian, dapat dipahami bahwa keberhasilan pembuktian dalam perkara *phantom hacker scam* tidak hanya ditentukan oleh kelengkapan regulasi, tetapi juga oleh kesiapan infrastruktur hukum dan sumber daya manusia yang memadai. Diperlukan peningkatan kompetensi aparat penegak hukum di bidang forensik digital, penguatan koordinasi antarinstansi, serta pembaruan prosedur pembuktian yang lebih adaptif terhadap perkembangan teknologi. Melalui langkah-langkah tersebut, diharapkan sistem peradilan pidana Indonesia mampu memberikan perlindungan hukum yang lebih efektif bagi masyarakat dari ancaman kejahatan siber yang semakin kompleks.

Berdasarkan analisis tersebut, pembahasan ini menunjukkan bahwa tujuan penelitian untuk memberikan pemahaman komprehensif mengenai keabsahan dan kekuatan pembuktian alat bukti digital tercapai. Pembuktian kejahatan *phantom hacker scam* tak hanya memerlukan pengakuan hukum terhadap alat bukti digital,

tetapi juga standar operasional yang jelas dan konsisten dalam praktik penegakan hukum. Oleh karena itu, pembahasan ini menegaskan pentingnya penguatan kapasitas forensik digital dan harmonisasi penerapan hukum acara pidana agar mampu merespons tantangan kejahatan siber secara efektif dan berkeadilan. Penguatan tersebut mencakup peningkatan kompetensi aparat penegak hukum dalam memahami karakteristik bukti elektronik, penyusunan pedoman teknis yang terstandarisasi, serta penyediaan infrastruktur forensik digital yang memadai. Dengan langkah-langkah tersebut, proses pengumpulan, analisis, dan penyajian alat bukti digital dapat dilakukan secara lebih profesional, akurat, dan dapat dipertanggungjawabkan di hadapan hukum.

Selain itu, harmonisasi penerapan hukum acara pidana juga diperlukan untuk memastikan bahwa pemanfaatan alat bukti digital tetap sejalan dengan prinsip-prinsip perlindungan hak asasi manusia dan asas peradilan yang adil. Setiap tindakan penegakan hukum, mulai dari penyitaan perangkat elektronik hingga pemeriksaan data pribadi, harus dilakukan berdasarkan prosedur yang jelas agar tidak menimbulkan pelanggaran hak tersangka maupun korban. Dengan demikian, keseimbangan antara kepentingan penegakan hukum dan perlindungan hak individu dapat tetap terjaga dalam penanganan perkara kejahatan siber. Upaya penguatan tersebut perlu didukung oleh kerja sama yang erat antara lembaga penegak hukum, akademisi, praktisi teknologi informasi, serta pembuat kebijakan. Kolaborasi lintas sektor akan membantu menciptakan standar pembuktian digital yang lebih komprehensif dan adaptif terhadap perkembangan modus kejahatan siber. Melalui sinergi tersebut, diharapkan sistem peradilan pidana Indonesia mampu menghadirkan mekanisme pembuktian yang lebih modern, kredibel, dan responsif terhadap dinamika kejahatan berbasis teknologi.

Dengan demikian, pembahasan ini menegaskan bahwa keberhasilan pembuktian perkara seperti *phantom hacker scam* tidak hanya bergantung pada keberadaan alat bukti digital semata, tetapi juga pada kesiapan sistem hukum secara keseluruhan. Penguatan kapasitas forensik digital, pembaruan regulasi, serta konsistensi praktik penegakan hukum merupakan elemen penting untuk mewujudkan proses peradilan yang efektif, berkeadilan, dan mampu memberikan kepastian hukum bagi masyarakat di era digital.

Pembahasan ini menekankan bahwa penguatan pembuktian digital harus dipahami sebagai bagian dari pembaruan sistem peradilan pidana secara menyeluruh, bukan sekadar penyesuaian teknis. Kejelasan standar prosedural dalam perolehan, pengelolaan, dan penyajian alat bukti digital menjadi prasyarat penting untuk menjamin perlindungan hak tersangka sekaligus kepentingan korban dan masyarakat. Dalam konteks tersebut, konsistensi penafsiran hakim terhadap alat bukti digital serta sinergi antara aparat penegak hukum, ahli forensik, dan pembentuk kebijakan sangat diperlukan agar proses pembuktian tidak menimbulkan ketidakpastian hukum. Dengan demikian, penelitian ini tidak hanya memberikan kontribusi akademik dalam pengembangan teori pembuktian pidana, tetapi juga menawarkan arah kebijakan praktis untuk memperkuat efektivitas penegakan hukum terhadap kejahatan siber, khususnya *phantom hacker scam*, di Indonesia.

Penguatan tersebut juga perlu diiringi dengan pembaruan regulasi yang lebih responsif terhadap dinamika teknologi informasi. Perkembangan modus operandi kejahatan siber yang semakin kompleks menuntut adanya norma hukum yang adaptif, termasuk pedoman teknis yang lebih rinci mengenai tata cara penanganan bukti elektronik. Tanpa adanya pembaruan kebijakan yang berkelanjutan, aparat penegak hukum akan selalu tertinggal selangkah dibandingkan dengan para pelaku kejahatan. Oleh karena itu, diperlukan kerangka hukum yang tidak hanya mengatur pengakuan alat bukti digital, tetapi juga mekanisme operasional yang menjamin keabsahan, integritas, dan akuntabilitas proses pembuktiannya. Di samping aspek regulasi, peningkatan kapasitas sumber daya manusia menjadi faktor kunci dalam keberhasilan pembuktian perkara *phantom hacker scam*. Penyidik, jaksa, dan hakim harus dibekali dengan pemahaman yang memadai mengenai teknologi informasi dan forensik digital agar mampu menilai bukti elektronik secara tepat. Pelatihan berkelanjutan, sertifikasi keahlian, serta penyediaan laboratorium forensik digital yang memadai merupakan langkah strategis yang perlu diprioritaskan. Tanpa dukungan kapasitas teknis yang kuat, keberadaan aturan hukum yang baik tidak akan dapat diimplementasikan secara optimal di lapangan.

Selain itu, koordinasi antarlembaga juga menjadi elemen penting dalam memperkuat sistem pembuktian digital. Penanganan perkara *phantom hacker scam* sering kali melibatkan berbagai pihak seperti kepolisian, otoritas perbankan, penyedia layanan internet, hingga lembaga internasional. Oleh karena itu, mekanisme kerja sama yang terstruktur dan efektif mutlak diperlukan agar proses pengumpulan dan verifikasi alat bukti dapat berjalan dengan cepat dan akurat. Sinergi kelembagaan ini akan membantu mengatasi kendala teknis maupun yuridis yang kerap muncul dalam penanganan kejahatan siber lintas batas. Dengan demikian, dapat dipahami bahwa efektivitas pembuktian digital tidak hanya bergantung pada keberadaan alat bukti elektronik semata, tetapi juga pada kesiapan sistem hukum secara keseluruhan. Pembaruan regulasi, peningkatan kompetensi aparat, penguatan infrastruktur forensik, serta koordinasi kelembagaan merupakan satu kesatuan yang tidak dapat dipisahkan. Melalui langkah-langkah strategis tersebut, diharapkan penegakan hukum terhadap kejahatan *phantom hacker scam* di Indonesia dapat berlangsung lebih profesional, transparan, dan berkeadilan, sehingga mampu memberikan perlindungan hukum yang nyata bagi masyarakat di era digital.

C. PENUTUP

Pengaturan hukum mengenai alat bukti digital dalam sistem peradilan pidana Indonesia telah memberikan landasan normatif yang memadai untuk digunakan dalam pembuktian tindak pidana siber, termasuk kasus *phantom hacker scam*. Pengakuan terhadap informasi dan dokumen elektronik sebagai alat bukti yang sah menunjukkan adanya adaptasi hukum terhadap perkembangan teknologi informasi. Namun demikian, efektivitas pengaturan tersebut sangat bergantung pada kemampuan aparat penegak hukum dan peradilan dalam menerapkan ketentuan hukum secara tepat dan konsisten, khususnya dalam menghadapi karakteristik kejahatan siber yang bersifat kompleks dan anonim.

Keabsahan dan kekuatan pembuktian alat bukti digital tidak hanya ditentukan oleh pengakuan normatif, tetapi juga oleh terpenuhinya persyaratan prosedural dan persyaratan teknis. Alat bukti digital harus diperoleh secara sah,

dijaga keutuhan dan keasliannya, serta didukung oleh keterangan ahli yang kompeten agar memiliki nilai pembuktian yang kuat di persidangan. Dalam konteks pembuktian tindak pidana *phantom hacker scam*, alat bukti digital pada umumnya tidak berdiri sendiri, melainkan harus dikaitkan dengan alat bukti lain untuk membentuk keyakinan hakim. Oleh karena itu, penguatan kapasitas forensik digital dan pemahaman hukum pembuktian berbasis teknologi menjadi kebutuhan penting guna mewujudkan sistem peradilan pidana yang efektif, adil, dan responsif terhadap perkembangan kejahatan siber.

DAFTAR PUSTAKA

Publikasi

Afdhali, Dino Rizka dan Handar Subhandi Bakhtiar. *Tinjauan Yuridis Pengaturan Pembuktian Ilmiah dalam Produk Hukum Positif di Indonesia*. Indonesian Journal of Law. Vol.1. No.10 (Oktober 2024).

Afisako, Vina Putri, dkk.. *Analisis Normatif terhadap Kekosongan Pengaturan Pedoman Teknis Alat Bukti Elektronik dalam Penanganan Kasus Kekerasan Seksual di Indonesia*. Jurnal Kajian Hukum dan Pendidikan Kewarganegaraan. Vol.2. No.1 (Oktober-Desember 2025).

Aini, Nurul dan Fauziah Lubis. *Tantangan Pembuktian dalam Kasus Kejahatan Siber*. Jurnal Hukum. Vol.5. No.2 (Juli 2024).

Dewi, Ni Made Trisma dan Reido Lardiza Fahrial. *Suatu Kajian Yuridis terhadap Penggunaan Alat Bukti Elektronik dalam Kejahatan Cyber dalam Sistem Penegakan Hukum*. Jurnal Hukum Saraswati (JHS). Vol.3. No.2 (September 2021).

Kencono, Pramukhtiko Suryo dan Ajeng Dwi Wahyuni. *Keabsahan Perolehan Alat Bukti Elektronik sebagai Konsep Perluasan Objek Praperadilan*. Fairness and Justice : Jurnal Ilmiah Ilmu Hukum. Vol.23. No.1 (Mei 2025).

Krisnanda, I Made Dwi, Madiasa Ablisar dan Mahmud Mulyadi. *Analisis Yuridis Bukti Digital (Digital Evidence) dalam Pembuktian Perkara Tindak Pidana Ujaran Kebencian pada Putusan Pengadilan Negeri Medan No. 3168/PID.SUS/2018/PN.MDN*. Res Nullius Law Journal. Vol.3. No.2 (Juli 2021).

Permana, Arya Made dan I Putu Rasmadi Arsha Putra. *Upaya Peningkatan Akses Keadilan terhadap Penerima Bantuan Hukum di Indonesia Melalui Paralegal*. Jurnal Ilmiah Kebijakan Hukum. Vol.17. No.22 (Januari-Juni 2023).

Tanoto, Elvina, Jesslyn Tandy dan Ricky Banke. *Kekuatan Alat Bukti Elektronik dalam Proses Pembuktian di Peradilan Pidana*. Jurnal Ilmu Hukum. Vol.2. No.1 (Oktober 2024).

Yahya, Mohamad Azhan, Ahmad Azam dan Mohd Shariff. *Application Of Principles Of Chain Of Evidence And Chain Of Custody During Storage And Forensic Examination Of Electronic Documentary Evidence In Shariah Criminal Cases In Malaysia*. Ilmu Law Journal. Vol.31. No.1 (November 2023).

Sumber Hukum

Kitab Undang-Undang Hukum Acara Pidana.

Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik.

Undang-Undang Nomor 19 Tahun 2016 tentang Perubahan Atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik.