QUANTUM JURIS: JURNAL HUKUM MODERN
Volume 08, No. 1, Januari 2026
https://journalversa.com/s/index.php/jhm

ANALISIS PERAN DIGITAL FORENSIK DALAM PENINDAKAN TINDAK PIDANA TERORISME

Mario Marco[1], Saupi Hasbi[2], Slamet Tri Wahyudi[3]

[1,2,3]Universitas Pembangunan Nasional "Veteran" Jakarta

mmsimatupang@gmail.com[1], saupihasbi.law@gmail.com[2], slamettriwahyudi@upnvj.ac.id[3]

***ABSTRACT**; The development of information and communication technology has transformed the modus operandi of criminal acts of terrorism. Terrorist groups now intensively utilize cyberspace for planning, recruitment, propaganda, and financing. This condition necessitates a new investigative approach capable of uncovering the perpetrators' digital footprints. The fundamental role of Digital Forensics as an essential discipline in supporting the legal enforcement process against terrorism offenses spans from the investigation stage to judicial proof in court. This research employs a qualitative-descriptive approach, analyzing legal literature, case studies, and Digital Forensics concepts, focusing on the collection, preservation, and analysis of admissible digital evidence.The analysis results indicate that Digital Forensics plays a vital role in: (1) Identifying and securing digital evidence from various devices used by perpetrators, including encrypted or deleted data. (2) Uncovering secret networks and communications among terrorist members, including radicalization patterns and following the money in terrorist financing. (3) Providing scientific evidence and crucial expert testimony to strengthen prosecution in court. However, its implementation faces challenges such as the rapid evolution of perpetrator technology and the need to strengthen human resource capacity and infrastructure. Ultimately, Digital Forensics is an inseparable instrument of law enforcement in counteracting modern terrorism (cyber-terrorism). Strengthening Digital Forensics capabilities, including cross-sectoral collaboration, is key to the effectiveness of prosecuting terrorism offenses in Indonesia.*
***Keywords**: Digital Forensics, Terrorism, Digital Evidence, Law Enforcement, Cyber-terrorismsystem.*

ABSTRAK; Perkembangan teknologi informasi dan komunikasi telah mengubah modus operandi tindak pidana terorisme. Kelompok teroris kini secara intensif memanfaatkan ruang siber untuk perencanaan, perekrutan, propaganda, dan pendanaan. Kondisi ini menuntut adanya pendekatan investigasi baru yang mampu mengungkap jejak digital pelaku. Peran fundamental Digital Forensik sebagai disiplin ilmu yang esensial dalam mendukung proses penindakan hukum terhadap tindak pidana terorisme, mulai dari tahap penyelidikan hingga pembuktian di pengadilan. Penelitian ini menggunakan pendekatan kualitatif-deskriptif dengan analisis terhadap literatur hukum, studi kasus, dan konsep ilmu Digital Forensik, difokuskan pada pengumpulan, preservasi, dan analisis bukti digital yang sah. Hasil analisis menunjukkan bahwa Digital Forensik memainkan peran vital dalam: (1) Mengidentifikasi dan mengamankan bukti digital dari berbagai perangkat yang digunakan pelaku, termasuk data yang terenkripsi atau telah dihapus. (2)

Mengungkap jaringan dan komunikasi rahasia antar anggota teroris, termasuk pola radikalisasi dan follow the money dalam pendanaan terorisme. (3) Menyediakan alat bukti ilmiah dan keterangan ahli yang krusial untuk memperkuat tuntutan di pengadilan. Namun, implementasinya menghadapi tantangan seperti cepatnya evolusi teknologi pelaku dan perlunya penguatan kapasitas sumber daya manusia serta infrastruktur. Digital Forensik adalah instrumen penegakan hukum yang tidak terpisahkan dalam menanggulangi terorisme modern (cyber-terrorism). Penguatan kapabilitas Digital Forensik, termasuk kolaborasi lintas sektoral, menjadi kunci untuk efektivitas penindakan tindak pidana terorisme di Indonesia.
Kata Kunci: Digital Forensik, Terorisme, Bukti Digital, Penindakan Hukum, Cyber-terrorism.

PENDAHULUAN

Perkembangan pesat teknologi informasi dan komunikasi (TIK) telah membawa konsekuensi ganda bagi keamanan global, ditandai dengan metamorfosis ancaman terorisme. Kelompok-kelompok ekstremis telah secara fundamental mengubah *modus operandi* mereka, bergeser dari serangan fisik konvensional menuju pemanfaatan ruang siber secara intensif. Internet dan media sosial kini berfungsi sebagai infrastruktur penting bagi mereka untuk menyebarkan propaganda, melaksanakan radikalisasi, dan merekrut anggota baru, seringkali menyasar generasi muda yang rentan[1]. Fenomena ini menciptakan bentuk kejahatan baru yang dikenal sebagai **Terorisme Siber** (*Cyber-terrorism*), yang memiliki karakter tanpa batas (*borderless*) dan sulit dideteksi, sehingga menimbulkan tantangan signifikan bagi aparat penegak hukum.

Pergeseran operasional terorisme ke ranah digital menghasilkan jejak kejahatan yang tidak lagi kasat mata, melainkan tersimpan dalam bentuk data elektronik yang kompleks, mudah dihapus, atau terenkripsi secara canggih. Hal ini menjadikan metode investigasi dan alat bukti konvensional yang diatur dalam Kitab Undang-Undang Hukum Acara Pidana (KUHAP) tidak lagi memadai untuk membuktikan unsur-unsur tindak pidana terorisme secara material[2]. Oleh karena itu, diperlukan suatu pendekatan investigasi yang khusus, ilmiah, dan adaptif terhadap teknologi digital untuk menemukan kebenaran. Kebutuhan inilah yang menempatkan Digital Forensik sebagai disiplin ilmu yang esensial dan mutlak dalam proses penegakan hukum kontemporer terhadap kejahatan berbasis teknologi.

[1] BNPT, *Laporan Perkembangan Ancaman Terorisme di Ruang Siber 2024*, (Jakarta: BNPT Press, 2024).
[2] N. F. Adnan, "Kekuatan Pembuktian Bukti Elektronik dalam Sistem Peradilan Pidana Indonesia," *Jurnal Hukum Pidana dan Kriminologi*, Vol. 4, No. 1 (2021), hlm. 55

Digital Forensik didefinisikan sebagai aplikasi ilmu komputer untuk kepentingan pembuktian hukum, khususnya dalam mengumpulkan, mengamankan, menganalisis, dan melaporkan bukti yang tersimpan pada perangkat digital secara metodologis[3]. Dalam konteks penindakan terorisme, peran Digital Forensik adalah fundamental, dimulai dari tahap penyelidikan hingga pembuktian di pengadilan. Analisis Digital Forensik memungkinkan penegak hukum (seperti Densus 88 Antiteror Polri) untuk: (1) Mengidentifikasi dan mengamankan bukti digital yang terenkripsi dan tersembunyi; (2) Mengungkap jaringan rahasia dan komunikasi koordinasi; dan (3) Melacak aliran dana terorisme (*follow the money*) yang menggunakan skema digital, termasuk *cryptocurrency*[4]. Ketiga peran ini secara kolektif membentuk fondasi bagi konstruksi hukum yang kuat terhadap para pelaku.

Meskipun memiliki peran yang vital, implementasi Digital Forensik dalam kasus terorisme menghadapi sejumlah tantangan serius. Tantangan utama berasal dari evolusi teknologi pelaku yang bergerak cepat, ditandai dengan penggunaan *enkripsi end-to-end* yang kuat dan pemanfaatan *dark web*, yang seringkali melampaui kemampuan perangkat dan regulasi forensik yang ada. Selain itu, terdapat kendala internal terkait keterbatasan sumber daya manusia (SDM) ahli yang bersertifikasi dan infrastruktur forensik yang memadai. Secara hukum, sifat kejahatan terorisme yang transnasional juga menimbulkan masalah yurisdiksi, mempersulit akuisisi bukti digital yang tersimpan di server luar negeri[5].

Dengan mempertimbangkan pergeseran ancaman dan kompleksitas pembuktian, analisis mengenai peran Digital Forensik menjadi sangat penting untuk dipublikasikan. Digital Forensik adalah instrumen penegakan hukum yang tidak terpisahkan dalam menanggulangi terorisme modern (*cyber-terrorism*). Efektivitas penindakan tindak pidana terorisme di Indonesia sangat bergantung pada sejauh mana kapabilitas Digital Forensik nasional dapat diperkuat, termasuk melalui investasi berkelanjutan, pengembangan Standar Operasional Prosedur (SOP) yang adaptif, dan kolaborasi lintas sektoral (misalnya, dengan Badan Siber dan Sandi Negara) untuk memastikan bukti digital yang dikumpulkan dapat menjerat pelaku secara sah dan tuntas di pengadilan

[3] M. Nuh Al-Azhar, *Digital Forensics: Panduan Praktis Investigasi Komputer*, (Jakarta: Elex Media Komputindo, 2012), hlm. 12
[4] R. S. Dewi, "Digital Forensik dan Penelusuran Dana Terorisme Melalui Mata Uang Kripto," *Jurnal Kajian Hukum dan Teknologi*, Vol. 3, No. 2 (2023), hlm. 101.
[5] A. S. Prayoga, "Tantangan Hukum Pembuktian Lintas Yurisdiksi dalam Kasus *Cyber-terrorism*," *Jurnal Hukum Internasional*, Vol. 15, No. 1 (2022), hlm. 78

Rumusan Masalah :

1) Bagaimana kekuatan Pembuktian digital forensik didalam penanganan tindak pidana terorisme?
2) Bagaimana pandangan hakim terhadap validitas dan reliabilitas bukti digital yang diperoleh melalui digital forensik dalam perkara terorisme?

Tujuan Penulisan

Tujuan dari penelitian ini adalah untuk memahami dan menganalisis sejauh mana kekuatan alat bukti digital forensik dalam penindakan tindak pidana terorisme. Secara lebih rinci, tujuan penelitian ini meliputi:

1) Mengidentifikasi Pergeseran Modus Operandi Terorisme: Menganalisis bagaimana perkembangan teknologi informasi dan komunikasi telah mengubah tindak pidana terorisme menjadi aktivitas berbasis siber (*cyber-terrorism*) yang menuntut pendekatan investigasi khusus.
2) Menganalisis Peran Fundamental Digital Forensik: Merumuskan dan menjelaskan peran esensial Digital Forensik dalam mendukung upaya penindakan hukum terhadap tindak pidana terorisme, terutama dalam mengungkap jejak digital pelaku.
3) Menguraikan Kontribusi Digital Forensik dalam Pembuktian: Menguraikan kontribusi spesifik Digital Forensik dalam menghasilkan alat bukti digital yang sah dan terpercaya, yang meliputi proses:
    - Pengamanan dan pemulihan data terenkripsi atau terhapus.
    - Pengungkapan jaringan komunikasi rahasia antar anggota teroris.
    - Pelacakan aliran pendanaan terorisme (*follow the money*).
4) Mengidentifikasi Tantangan dan Hambatan Implementasi: Mengidentifikasi dan menganalisis tantangan utama (baik teknis, regulasi, maupun sumber daya manusia) yang dihadapi oleh penegak hukum di Indonesia dalam menerapkan Digital Forensik untuk kasus terorisme.
5) Merumuskan Rekomendasi Penguatan Kapabilitas: Memberikan rekomendasi strategis dan praktis bagi penegak hukum dan instansi terkait (seperti BNPT dan BSSN) mengenai upaya penguatan kapabilitas Digital Forensik nasional guna meningkatkan efektivitas penindakan tindak pidana terorisme di masa depan.

METODE PENELITIAN

Penelitian ini merupakan penelitian hukum normatif, yaitu penelitian yang bertumpu pada kajian terhadap norma-norma hukum yang tertulis, baik yang terdapat dalam peraturan perundang-undangan maupun dalam literatur hukum yang relevan. Penelitian hukum normatif berfokus pada analisis terhadap kaidah hukum sebagai suatu sistem yang bersifat preskriptif, yakni menjelaskan tentang apa yang seharusnya dilakukan dalam konteks hukum tertentu.

Pendekatan yang digunakan dalam penelitian ini mencakup beberapa pendekatan hukum, yaitu:

Pendekatan Perundang-undangan (Statute Approach)

Pendekatan ini dilakukan dengan menelaah peraturan perundang-undangan yang mengatur secara langsung maupun tidak langsung mengenai alat bukti dalam sistem hukum pidana, khususnya yang berkaitan dengan alat bukti forensik dalam KUHAP dan peraturan pelaksana lainnya.

Pendekatan Konseptual (Conceptual Approach)

Pendekatan ini digunakan untuk memahami konsep-konsep yuridis yang berkaitan dengan alat bukti forensik, kedudukannya dalam sistem pembuktian hukum acara pidana, serta relevansinya dengan asas-asas hukum seperti asas keadilan, asas legalitas, dan asas due process of law.

Pendekatan Kasus (Case Approach)

Penelitian ini juga menggunakan pendekatan kasus, yaitu dengan mengkaji dan menganalisis putusan-putusan pengadilan yang berkaitan dengan penggunaan alat bukti forensik dalam perkara pidana, untuk melihat bagaimana bukti digital forensik digunakan dalam praktik didalam penegakan tindak pidana terorisme.

HASIL DAN PEMBAHASAN

1) Kekuatan Pembuktian digital forensik didalam penanganan tindak pidana terorisme.

Kekuatan pembuktian Digital Forensik dalam perkara terorisme bersandar pada landasan yuridis yang telah diakui, terutama melalui Undang-Undang Informasi dan Transaksi Elektronik (UU ITE). UU ITE secara eksplisit mengakui Informasi Elektronik dan/atau

Dokumen Elektronik sebagai alat bukti hukum yang sah[6]. Namun, pengakuan ini bersifat bersyarat: bukti digital harus memiliki integritas, otentisitas, dan ketersediaan yang terjamin, sebuah prinsip yang dikenal sebagai *admissibility*[7]. Digital Forensik bertindak sebagai jembatan antara teknologi dan hukum, menggunakan metodologi ilmiah untuk mengubah data mentah yang tersimpan dalam perangkat komunikasi teroris menjadi bukti yang memenuhi syarat hukum. Tanpa proses Digital Forensik yang ketat, bukti digital—sekalipun substansinya kuat—dapat dianggap cacat prosedur dan ditolak di pengadilan.

Kekuatan pembuktian Digital Forensik yang paling mendasar adalah kemampuannya menjamin integritas data melalui penggunaan teknik ilmiah. Seluruh proses akuisisi data dilakukan dengan prinsip write-blocker untuk mencegah modifikasi pada data asli[8]. Selanjutnya, data yang diambil akan dihitung nilai hash (seperti SHA-256) untuk menghasilkan kode unik digital. Nilai hash ini, yang dicatat pada berita acara penyitaan, berfungsi sebagai verifikasi bahwa salinan data (forensic image) yang dianalisis sama persis dengan data yang disita dari perangkat pelaku. Jaminan bahwa bukti tidak diubah (*tamper-proof*) ini sangat krusial, khususnya dalam kasus terorisme di mana pembuktian harus tanpa keraguan (*beyond a reasonable doubt*) dan sering melibatkan data sensitif yang terenkripsi.

Digital Forensik memberikan kekuatan pembuktian yang superior dalam mengungkap dimensi kejahatan yang tidak terlihat, terutama niat jahat (mens rea) dan pola radikalisasi. Analisis terhadap riwayat pencarian (misalnya, instruksi pembuatan bom, target serangan), komunikasi rahasia, atau keanggotaan dalam grup daring terenkripsi, secara jelas dapat membuktikan perencanaan dan kesamaan niat kolektif[9]. Selain itu, dengan melacak jejak metadata dan log koneksi, Digital Forensik mampu memetakan seluruh jaringan teroris, mengidentifikasi donatur dana, dan mengungkap pola follow the money yang menggunakan sistem pembayaran digital atau mata uang kripto. Bukti-bukti ini menyediakan rantai komando dan kontrol yang konkret, yang sangat diperlukan untuk menjerat pelaku utama maupun pendukung terorisme.

[6] Pasal 5 ayat (1) dan (2) Undang-Undang Nomor 19 Tahun 2016 tentang Perubahan atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik.
[7] M. Nuh Al-Azhar, *Digital Forensics: Panduan Praktis Investigasi Komputer*, (Jakarta: Elex Media Komputindo, 2012), hlm. 25.
[8] P. R. Adhikari, "Standard Operating Procedures in Digital Forensics and Evidence Management," International Journal of Computer Science, Vol. 12, No. 3 (2015), hlm. 109
[9] R. S. Dewi, "Digital Forensik dan Penelusuran Dana Terorisme Melalui Mata Uang Kripto," *Jurnal Kajian Hukum dan Teknologi*, Vol. 3, No. 2 (2023), hlm. 105

Kekuatan pembuktian Digital Forensik tidak akan sempurna tanpa kehadiran Keterangan Ahli di persidangan. Ahli forensik digital bertindak sebagai penerjemah temuan ilmiah ke dalam bahasa hukum yang dapat dipahami oleh Majelis Hakim[10]. Melalui kesaksiannya, ahli memastikan bahwa: (a) Prosedur forensik yang digunakan telah sesuai dengan standar yang berlaku; (b) Hasil analisis (seperti pemulihan data yang dihapus atau dekripsi komunikasi) memiliki dasar ilmiah yang valid; dan (c) Bukti digital tersebut relevan secara kontekstual dengan unsur-unsur tindak pidana terorisme yang didakwakan. Dengan demikian, keterangan ahli mengeliminasi keraguan hakim terhadap validitas dan keabsahan bukti digital yang dihasilkan.

Kekuatan pembuktian Digital Forensik adalah pilar utama dalam penindakan tindak pidana terorisme di era digital. Proses DF yang memastikan integritas data, dikombinasikan dengan kemampuan mengungkap jaringan tersembunyi, menjadikan bukti digital sebagai tulang punggung untuk mencapai kebenaran materiil di pengadilan. Penguatan berkelanjutan terhadap kapabilitas Digital Forensik baik melalui regulasi, peralatan, maupun pelatihan sumber daya manusia mutlak diperlukan agar kekuatan pembuktian ini dapat dipertahankan dan ditingkatkan untuk melawan ancaman cyber-terrorism yang terus berevolusi.

2) pandangan hakim terhadap validitas dan reliabilitas bukti digital yang diperoleh melalui digital forensik dalam perkara terorisme

Dalam praktik persidangan di Indonesia, hakim menilai bukti digital melalui dua lensa utama, yakni aspek formil dan materiil. Aspek formil mencakup keabsahan dan prosedur perolehan bukti seperti otentikasi, rantai penguasaan (*chain of custody*), serta legalitas penyadapan atau akses terhadap data. Sedangkan aspek materiil menitikberatkan pada sejauh mana bukti digital tersebut mampu meyakinkan hakim mengenai kebenaran suatu fakta. Landasan yuridis mengenai penerimaan bukti elektronik diatur dalam Undang-Undang Nomor 19 Tahun 2016 tentang Perubahan atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (UU ITE), yang menyatakan bahwa dokumen atau informasi elektronik dapat dijadikan alat bukti hukum yang sah sepanjang dapat dibuktikan

[10] E. Y. Utami, "Peran Ahli Digital Forensik dalam Pembuktian Tindak Pidana Siber," *Prosiding Seminar Nasional Hukum dan Teknologi*, (2021), hlm. 47.

keaslian dan integritasnya. Karena itu, hakim tidak serta-merta menerima file digital tanpa bukti yang menunjukkan proses perolehannya secara sah dan terjamin integritasnya.[11]

Keterangan saksi ahli digital forensik memegang peran sentral dalam pembentukan keyakinan hakim terhadap reliabilitas bukti digital. Menurut Eoghan Casey, seorang pakar forensik digital dalam bukunya *Digital Evidence and Computer Crime*, hakim akan memberikan bobot lebih pada bukti digital ketika ahli dapat menjelaskan secara rinci metode yang digunakan seperti pembuatan *image* bit-by-bit, penggunaan hash kriptografis, dan dokumentasi *chain of custody*. Ahli juga harus menunjukkan bahwa prosedur yang digunakan mengikuti standar ilmiah yang dapat diuji ulang (*reproducible*). Penjelasan yang dapat dipahami oleh hakim yang bukan ahli teknis menjadi penting, karena transparansi dalam metode analisis merupakan kunci bagi hakim untuk menilai tingkat keandalan bukti digital.[12]

Selain keterangan ahli, hakim juga menilai validitas bukti digital berdasarkan pemenuhan standar dan pedoman internasional. Lembaga seperti ENFSI (*European Network of Forensic Science Institutes*) dan NIST (*National Institute of Standards and Technology*) telah menetapkan standar pemeriksaan forensik digital yang banyak dijadikan acuan di berbagai negara. Ketika laporan forensik menunjukkan kesesuaian dengan pedoman tersebut, seperti *Best Practice Manual for the Forensic Examination of Digital Technology* yang diterbitkan ENFSI, maka kepercayaan hakim terhadap hasil analisis meningkat karena prosesnya memiliki dasar ilmiah dan prosedural yang teruji.[13]

Hakim menghadapi sejumlah kendala dalam menilai bukti digital pada perkara terorisme. Salah satunya adalah variasi kualitas laporan forensik yang kadang terlalu teknis atau sebaliknya terlalu sederhana, sehingga menyulitkan hakim memahami maknanya. Selain itu, keterbatasan kemampuan teknis hakim membuat mereka sering kali bergantung pada kredibilitas ahli. Di sisi lain, persoalan yuridiksi dan akses terhadap data yang disimpan di luar negeri juga kerap menimbulkan keraguan atas keutuhan bukti. Hal-hal ini menyebabkan hakim meski menerima bukti elektronik secara formal, belum tentu menganggapnya kuat secara materiil tanpa dukungan bukti lain yang memperkuat konteks fakta hukum.[14]

---

[11] Undang-Undang Republik Indonesia Nomor 19 Tahun 2016 tentang Perubahan atas UU No.11 Tahun 2008 tentang Informasi dan Transaksi Elektronik.
[12] Eoghan Casey, *Digital Evidence and Computer Crime: Forensic Science, Computers and the Internet*, 3rd Edition, Academic Press, 2011.
[13] ENFSI, *Best Practice Manual for the Forensic Examination of Digital Technology*, 2015.
[14] Mahkamah Agung Republik Indonesia, *Pedoman Pemeriksaan Alat Bukti Elektronik dalam Perkara Pidana*, Jakarta, 2020.

Pada perspektif ilmu forensik modern, prinsip yang paling berpengaruh dalam penerimaan bukti digital oleh hakim adalah transparansi metode dan keterulangan hasil. Para ahli forensik menekankan pentingnya dokumentasi yang lengkap, seperti penyimpanan *image* forensik, log hash, dan catatan langkah analisis yang memungkinkan pihak lain melakukan verifikasi ulang. Menurut pedoman SWGDE (*Scientific Working Group on Digital Evidence*), kemampuan untuk mereplikasi hasil pemeriksaan dengan hasil yang konsisten merupakan ukuran utama reliabilitas bukti digital. Dengan demikian, bukti yang dihasilkan dari prosedur yang transparan dan dapat diuji ulang memiliki legitimasi ilmiah yang lebih kuat di hadapan hakim.[15]

Implikasinya bagi penegakan hukum terhadap tindak pidana terorisme adalah bahwa penyidik dan penuntut harus memastikan bukti digital yang diajukan ke persidangan tidak hanya sah secara hukum, tetapi juga reliabel secara teknis. Laporan forensik harus disusun dengan bahasa yang jelas dan disertai uraian metodologi yang dapat dipahami hakim. Selain itu, peningkatan kapasitas hakim melalui pendidikan dan pelatihan singkat tentang dasar-dasar digital forensik perlu dilakukan agar mereka dapat menilai kekuatan pembuktian secara lebih kritis. Dengan kombinasi kepatuhan prosedural, validasi ilmiah, dan literasi teknis, bukti digital akan semakin diterima sebagai alat bukti yang valid dan meyakinkan dalam perkara terorisme.

KESIMPULAN DAN SARAN

Kesimpulan

Digital forensik memiliki peran yang sangat strategis dan tidak terpisahkan dalam proses penindakan tindak pidana terorisme di era digital. Melalui pendekatan ilmiah terhadap data elektronik, digital forensik mampu menjembatani antara teknologi dan hukum dalam mengungkap kebenaran materiil suatu perkara. Bukti digital yang diperoleh dari hasil analisis forensik tidak hanya membantu mengidentifikasi pelaku, jaringan, serta pola komunikasi teroris, tetapi juga menjadi alat bukti yang sah di pengadilan sebagaimana diatur dalam Undang-Undang Informasi dan Transaksi Elektronik (UU ITE). Dengan demikian, digital forensik berfungsi sebagai fondasi ilmiah dalam proses pembuktian dan memperkuat tuntutan hukum terhadap pelaku terorisme.Pandangan hakim terhadap validitas dan reliabilitas bukti digital menunjukkan bahwa aspek prosedural dan teknis menjadi faktor kunci dalam

[15] SWGDE, *Best Practices for Computer Forensics*, Scientific Working Group on Digital Evidence, 2018.

penerimaan bukti di pengadilan. Hakim akan menilai bukti digital berdasarkan keabsahan proses perolehannya, integritas data, serta kesesuaian dengan standar ilmiah dan hukum yang berlaku. Kejelasan laporan forensik serta kemampuan ahli menjelaskan metodologi yang digunakan secara transparan turut menentukan tingkat kepercayaan hakim terhadap hasil analisis digital forensik. Oleh karena itu, hubungan sinergis antara ahli forensik, penyidik, dan aparat peradilan menjadi penting untuk menjamin keabsahan dan kekuatan pembuktian bukti digital di persidangan.

Secara umum, penerapan digital forensik telah memberikan terobosan signifikan dalam sistem penegakan hukum terhadap tindak pidana terorisme. Namun demikian, tantangan masih muncul dalam bentuk keterbatasan sumber daya manusia, infrastruktur laboratorium forensik digital, serta perbedaan tingkat pemahaman aparat peradilan terhadap aspek teknis bukti elektronik. Untuk itu, peningkatan kapabilitas teknis dan koordinasi lintas sektor diperlukan agar digital forensik dapat berfungsi lebih efektif dan efisien dalam menanggulangi ancaman terorisme siber yang terus berkembang.

Saran

penguatan kapasitas sumber daya manusia di bidang digital forensik dan peradilan perlu dilakukan secara berkelanjutan. Aparat penegak hukum, termasuk penyidik, jaksa, dan hakim, harus dibekali dengan pemahaman dasar mengenai prinsip kerja digital forensik, integritas data, serta validasi alat bukti elektronik agar tidak terjadi kesalahan dalam menilai kekuatan pembuktian.pemerintah dan lembaga penegak hukum perlu memperkuat infrastruktur laboratorium digital forensik nasional yang berstandar internasional. Hal ini mencakup peningkatan fasilitas teknis, sertifikasi alat dan tenaga ahli, serta penerapan prosedur kerja yang sesuai dengan pedoman dari lembaga internasional seperti ENFSI, NIST, dan SWGDE, sehingga hasil pemeriksaan memiliki legitimasi ilmiah di tingkat global.

Perlunya pembaruan kebijakan hukum acara pidana agar lebih adaptif terhadap dinamika perkembangan teknologi informasi. KUHAP sebagai dasar hukum acara pidana perlu direvisi dengan memasukkan ketentuan yang secara eksplisit mengatur mekanisme pemeriksaan, penyitaan, dan pembuktian alat bukti elektronik agar tidak terjadi kekosongan norma di masa depan. Dengan langkah-langkah tersebut, digital forensik dapat menjadi pilar utama dalam sistem peradilan pidana modern untuk menanggulangi kejahatan terorisme di era digital secara efektif dan berkeadilan.

DAFTAR PUSTAKA

N. F. Adnan, "Kekuatan Pembuktian Bukti Elektronik dalam Sistem Peradilan Pidana Indonesia," *Jurnal Hukum Pidana dan Kriminologi*, Vol. 4, No. 1 (2021).

M. Nuh Al-Azhar, *Digital Forensics: Panduan Praktis Investigasi Komputer*, (Jakarta: Elex Media Komputindo, 2012).

R. S. Dewi, "Digital Forensik dan Penelusuran Dana Terorisme Melalui Mata Uang Kripto," *Jurnal Kajian Hukum dan Teknologi*, Vol. 3, No. 2 (2023).

A. S. Prayoga, "Tantangan Hukum Pembuktian Lintas Yurisdiksi dalam Kasus *Cyber-terrorism*," *Jurnal Hukum Internasional*, Vol. 15, No. 1 (2022).

M. Nuh Al-Azhar, *Digital Forensics: Panduan Praktis Investigasi Komputer*, (Jakarta: Elex Media Komputindo, 2012).

P. R. Adhikari, "Standard Operating Procedures in Digital Forensics and Evidence Management," International Journal of Computer Science, Vol. 12, No. 3 (2015).

BNPT, *Laporan Perkembangan Ancaman Terorisme di Ruang Siber 2024*, (Jakarta: BNPT Press, 2024).

ENFSI, *Best Practice Manual for the Forensic Examination of Digital Technology*, 2015.

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

R. S. Dewi, "Digital Forensik dan Penelusuran Dana Terorisme Melalui Mata Uang Kripto," *Jurnal Kajian Hukum dan Teknologi*, Vol. 3, No. 2 (2023).

E. Y. Utami, "Peran Ahli Digital Forensik dalam Pembuktian Tindak Pidana Siber," *Prosiding Seminar Nasional Hukum dan Teknologi*.