LEX NUSANTARA: Jurnal Lex Syar'i and Positive Law
Vol. 1, No. 1, pp: 01-10
DOI: https://doi.org/10.62667/lexnusantara.v1i1.123
E-ISSN: 0000-0000
https://berugakbaca.org/index.php/lexnusantara

Penerapan Alat Bukti Digital dalam Penanganan Kasus Kejahatan Siber di Wilayah Kepolisian Daerah Papua Barat

Wiwid Irianti Septiyaninigsih
Ilmu Hukum,Universitas Terbuka

History Article

Article history:

Received 01 July 2026
Revision 01 July 2026
Approved 01 July 2026

Keywords:

Kejahatan, digital,Siber

,

ABSTRACT

Penelitian ini mengkaji penerapan alat bukti digital dalam penanganan kasus kejahatan siber di wilayah Polda Papua Barat. Pendekatan yang efektif sangatlah dibutuhkan untuk kumpulkan dan analisis bukti elektronik sebab kini keberadaan kejahatan siber sangatlah rumit sehingga untuk analisisnya butuh pendekatan efektif agar hasilnya sesuai yang diinginkan. Metode deskriptif dipakai di studi ini ditambah berfokus ke kendala yang ada, efisiensi penanganan kasus beserta dengan manfaat dan dampak pemakaian alat bukti digital sehingga didapatkan informasi lengkap untuk dukung studi yang dilakukan. Studi didapatkan hasil pemakaian alat bukti digital lebih cepat merespons kejahatan siber, membuat penyelidikan tambah cepat dan hasil analisis yang tepat dan cepat sehingga penggunaan alat bukti digital ini berdampak baik untuk memberi edukasi masyarakat akan kejahatan siber beserta dengan tingkatkan keberhasilan penegakan hukum. Tapi ada kendala yang butuh dicari solusinya seperti keterbatasan SDM ataupun teknologi di tengah-tengah kejahatan siber yang tambah rumit untuk itu studi ini soroti pentingnya pelatihan penyidik, kolaborasi antar instansi ditambah dengan keseimbangan penegakan HAM, privasi dan hukum agar didapatkan solusi untuk kendala yang timbul terkhusus yang ada kaitannya dengan kasus kejahatan siber. Sehingga harapannya lewat hasil studi yang dilakukan bisa memberi kontribusi baik untuk bisa pahami cara menangani kejahatan siber terkhusus di wilayah Kepolisian Daerah Papua Barat lewat pemanfaatan alat bukti digital.

*Corresponding author email: wiwidirianti@gmail.com

PENDAHULUAN

Penyebaran informasi palsu ditambah serangan siber terkoordinasi dan pencurian data pribadi tergolong kasus kejahatan siber yang bertambah banyak jumlahnya di tengah perkembangan teknologi digital kini sehingga kejahatan siber jadi ancaman serius untuk banyak orang di dunia sebab membawa kerugian besar. Menurut Saeful Bahri (2020), kejahatan siber, yang umumnya dikenali sebagai tindak pidana siber, merujuk pada tindakan kejahatan yang menggunakan jaringan komputer dani kemudahani teknologi, termasuki melalui media sosiali seperti Facebook, Tiktok, Instagram, Twitter, dan SMS (short message service). Postingan atau iklan di grub medsos jadi contohnya kejahatan siber semacam ini.

Kejahatan di dunia maya jadi masalah serius misalnya penyebaran informasi yang merusak, terorisme ditambah hacking dan carding seperti diterangkan Prasetiyo & Mukhtar Zuhdy (2020) sebab kurangnya regulasi pemakaian teknologi informasi dan komunikasi di banyak bidang sehingga menyebabkan kejahatan dunia maya bertambah rumit. Regulasi yang lebih kuat sangatlah dibutuhkan untuk atasi masalah kejahatan siber sebab tingkat kejahatan siber di dunia maya bertambah banyak sehingga regulasi aturan yang lebih baik tentu saja dibutuhkan agar bisa pastikan keamanan di dunia maya dan bisa atasi masalah kejahatan siber.

Ada dua kategori kejahatan siber seperti diterangkan Barda Nawawi Arif dalam artian luas (kejahatan terhadap pemakaian sarana komputer dan kejahatan terhadap sistem komputer) ditambah dengan artian sempit (kejahatan terhadap sistem komputer) yang pada kenyataannya banyak pihak sesuai pemahamannya sudah berupaya definisikan kejahatan siber itu. Istilahistilah itu seperti diterangkan Barda Nawawi Arif belum memberi gambaran akurat secara penuh walau masih tetap dipakai istilah semacam "*crime related to computer*" atau kejahatan yang berhubungan dengan komputer, "*crime utilizing computers*" atau kejahatan memakai komputer beserta dengan "*crime directed at computer*" atau kejahatan terhadap komputer.

Dalam konteks ini, penelitian ini akan mencoba menjawab dua rumusan masalah utama yaitu bagaimana penerapan alat bukti digital berkontribusi dalam peningkatan efisiensi penanganan kasus kejahatan siber di Wilayah Kepolisian Daerah Papua Barat dan apa saja kendala dan tantangan yang dihadapi oleh Polda Papua Barat dalam mengimplementasikan alat bukti digital dalam penanganan kasus kejahatan siber? Penelitian ini bertujuan untuk Menganalisis peran dan kontribusi alat bukti digital dalam peningkatan efisiensi penanganan kasus kejahatan siber di Wilayah Polda Papua Barat. Tujuan studi ini identifikasi tantangan beserta dengan kendala yang Polda Papua Barat hadapi terkhusus sewaktu memakai alat bukti digital untuk tangani kasus kejahatan siber sehingga bisa didapat informasi sesuai keinginan tujuan studi.

Tulisan ini fokusnya ke pemakaian alat bukti digital untuk tangani kasus kejahatan siber terkhusus di Wilayah Polda Papua Barat ditambah fokus ke teknologi digital yang dipakai, peran alat bukti digital beserta dengaan tantangannya untuk itu harapannya lewat studi ini bias beri manfaat pemahaman lebih banyak atas topik studi ini sehingga hasil studi ini bisa dipakai untuk perbaikan berikutnya.

Ada keterbatasan sewaktu susun tulisan ini sehingga perlu diperhitungkan sebab keterbatasan yang timbul bisa jadi hambatan untuk menyusun tulisan ini dan hasilnya menjadi tidak sesuai yang diharapkan di tujuan studi. Keterbatasan-keterbatasan ini mencakup Keterbatasan akses ke data internal Polda Papua Barat, yang dapat mempengaruhi tingkat kedalaman analisis dalam penelitian ini, Terbatasnya waktu dan sumber daya untuk melibatkan berbagai pihak terkait, seperti praktisi hukum, penegak hukum, dan ahli keamanan siber, Dengan memahami keterbatasan-keterbatasan ini, penelitian ini tetap diharapkan dapat

memberikan kontribusi yang bermanfaat dalam pemahaman tentang penerapan alat bukti digital dalam penanganan kasus kejahatan siber di Wilayah Polda Papua Barat.

METODE PENELITIAN

Penelitian ini menggunakan metode deskriptif untuk mendalami pemahaman tentang Penerapan Alat Bukti Digital dalam Penanganan Kasus Kejahatan Siber di Wilayah Kepolisian Daerah Papua Barat. Teknik pengumpulan data yang digunakan adalah studi pustaka, yang merupakan metode yang diarahkan pada pencarian data dan informasi melalui berbagai dokumen, baik tertulis, foto-foto, gambar, peraturan, maupun dokumen elektronik yang mendukung proses penulisan.

Studi pustaka ini akan melibatkan sejumlah perusahaan atau organisasi yang menggunakan Alat Bukti Digital dalam Penanganan Kasus Kejahatan Siber. Selain itu, kasuskasus konkret akan dianalisis dalam penelitian ini. Data kualitatif yang terkumpul akan dianalisis menggunakan analisis tematik, di mana data akan disusun, dikodekan, dan kategori tematik akan dikembangkan untuk mengidentifikasi pola-pola dan temuan-temuan utama yang berkaitan dengan Penerapan Alat Bukti Digital dalam Penanganan Kasus Kejahatan Siber.

Adapun beberapa keterbatasan yang perlu diakui dalam penelitian ini yaitu, penelitian ini terbatas pada konteks geografis tertentu dan mungkin tidak mencakup semua variasi dalam Penerapan Alat Bukti Digital dalam Penanganan Kasus Kejahatan Siber di berbagai negara, waktu yang terbatas mungkin membatasi jumlah responden dan kasus yang dapat diinvestigasi secara mendalam, analisis data kualitatif dapat dipengaruhi oleh subyektivitas peneliti, meskipun upaya maksimal akan dilakukan untuk meminimalkan bias, beberapa informasi yang relevan mungkin tidak dapat diakses karena batasan kerahasiaan atau kendala lainnya. Hasil dari studi ini harapannya bisa beri wawasan luas lebih-lebih yang ada hubungannya dengan topik studi ini sehingga pembaca memiliki pemahaman yang tambah baik walau tentu saja ada keterbatasan di studi ini.

HASIL DAN PEMBAHASAN

HASIL

Studi ini didapatkan hasil kejahatan siber sejarahnya sudah semenjak seabad lalu sewaktu sistem telepon negara dirusak para remaja di tahun 1870-an lewat cara merubah otoritas jaringan telekomunikasi sehingga memperlihatkan aktivitas hacking yang tergolong kejahatan siber sudah berlangsung semenjak dulu.

Orang yang bisa buat program yang fungsinya bisa melampaui fungsi awal program itu sendiri disebut hacker atau disebutkan peretas dan fenomena hacker itu sudah ada semenjak lama di tahun 1870-an lalu kemudian tahun 1960-an para peretas lakukan eksperimen di laboratorium kecerdasan buatan fasilitas universitas yang mempunyai komputer dengan ukuran besar.

Studi didapatkan hasil bila bertambah banyak jenis kejahatan siber contohnya serangan ke pemerintah, pelanggaran hak cipta ditambah serangan ke individu beserta kejahatan muri yang betul-betul dilakukan sehingga memperlihatkan bila para hacker pada

kenyataannya di lapangan berkembang jadi pelaku kejahatan komputer yang memakai perangkat ilegal di aksinya.

Sedang hasil studi bila dilihat lewat sudut pandang hukum pidana memperlihatkan tindak pidana terkhusus di Indonesia dasar utamanya peraturan khusus ditambah KUHP yang tergolong hukum publik yang isinya bahas hubungan individu dengan negara. Studi didapatkan hasil penyidik dalam proses kasus kejahatan siber memakai rujukan hukum UU ITE dimana BAB XI aturannya berisikan ketentuan pidana sedang Pasal 27 – 37 isinya perbuatan yang tidak diperbolehkan sehingga rujukan itu bisa dipakai untuk jadi dasar yang legal agar bisa menangani kejahatan siber.

Studi didapatkan hasil ada ciri-ciri alat bukti di kejahatan siber yang tentu saja tidak sama dengan tindak pidana umum contohnya bukti digital dimana bila penyidik tidak segera amankan bukti digital itu sangatlah mudah disembunyikan atau dihapus dan dirubah oleh oknum yang tak bertanggung jawab. Dalam penyelesaian perkara pidana kejahatan siber ada batasan untuk alat bukti yang dipakai seperti diterangkan KUHAP Pasal 184 ayat (1) alat bukti yang sah ada lima seperti keterangan terdakwa, petunjuk dan surat ditambah keterangan ahli beserta keterangan saksi sehingga alat bukti penyelesaian perkaranya dibatasi lima itu.

Studi didapatkan hasil proses pemeriksaan atau penyidikan bekas perkara susah dilakukan sebab di kasus kejahatan siber pelakunya banyak ada di luar daerah lebih-lebih di luar negeri sehingga jejak digital semacam alamat IP susah dilacak yang menjadi hambatan sewaktu mencari pelakunya.

PEMBAHASAN

Kejahatan siber yang tambah banyak dikarenakan perkembangan teknologi yang berubah-ubah sangatlah menarik dijadikan bahasan utama di studi ini mengingat perkembangan teknologi dampaknya besar ke hidup manusia. Kompleksitas sistem digital membuka peluang bagi pelaku untuk mengeksploitasi celah keamanan dengan berbagai teknik.Kecepatan perubahan teknologi menuntut penyidik untuk memiliki kemampuan forensik digital yang memadai. Bukti digital bersifat *volatile* sehingga membutuhkan penanganan cepat dan prosedural agar tidak kehilangan keasliannya.

Pemanfaatan fasilitas umum seperti warnet oleh pelaku menjadi bentuk adaptasi mereka dalam menyembunyikan identitas digital. Minimnya regulasi terhadap fasilitas tersebut memperbesar tantangan aparat dalam menelusuri jejak aktivitas kejahatan. Minimnya saksi dalam kasus *cyber crime* memperlihatkan bahwa bukti digital menjadi komponen utama pembuktian. Tanpa dukungan saksi, penyidik harus mengandalkan rekaman digital, log aktivitas, alamat IP, dan data elektronik lain yang dapat menghubungkan pelaku dengan perbuatan.

Penundaaan pemeriksaan saksi atau keterbatasan lokasi saksi dapat menyebabkan berkas perkara dinilai tidak lengkap oleh penuntut umum. Hal ini berdampak pada risiko bebasnya terdakwa jika bukti digital tidak diperkuat dengan bukti lain. Pembahasan memperjelas bahwa keterbatasan alat dan SDM menjadi hambatan serius dalam implementasi bukti digital. Penyidik harus dibekali pelatihan terkait prosedur forensik, teknik pengamanan data, dan metode analisis digital. Alat bukti digital memberikan kontribusi besar dalam efektivitas penyelidikan. Ketepatan analisis data digital memungkinkan penyidik memahami

pola serangan dan identitas pelaku secara lebih komprehensif. Dampak lain dari penggunaan bukti digital adalah meningkatnya keberhasilan penegakan hukum. Bukti elektronik yang valid dan dapat diverifikasi membantu memperkuat dakwaan di pengadilan.

Penerapan bukti digital juga bersifat preventif karena masyarakat dan pelaku potensial menyadari bahwa aktivitas digital meninggalkan jejak yang dapat ditelusuri aparat. Keseluruhan pembahasan menekankan pentingnya kolaborasi antarinstansi, khususnya antara kepolisian, penyedia layanan internet, instansi pemerintah, dan lembaga keamanan siber. Dalam pemakaian ataupun pengumpulan bukti haruslah tetap perhitungkan privasi digital beserta dengan hak asasi manusia sebab tiap-tiap manusia punya hak dilindungi privasinya terkhusus informasi pribadinya sehingga hak asasi itu haruslah diutamakan sewaktu kumpulkan bukti agar tidak rugikan orang lain.

SIMPULAN

Ada dampak nyata pemakaian alat bukti digital untuk tangani kasus kejahatan siber terkhusus di Wilayah Kepolisian Daerah Papua Barat sebab proses penyelidikan tambah cepat lewat adanya alat bukti digital sehingga mudahkan kepolisian sewaktu bekerja untuk ungkap kejahatan siber walau tentu saja ada hambatan sewaktu pelaksanaannya contohnya sumber daya terbatas ditambah dengan kejahatan yang tambah rumit.

Agar masalah yang timbul bisa diatasi butuh usaha bersama sebab pemakaian alat bukti digital bisa berhasil sewaktu ada kerja sama antar institusi beserta keselarasan penegakan HAM, privasi dan hukum sehingga lewat cara ini bisa berdampak baik jaga keamanan siber.

DAFTAR PUSTAKA

Aryyaguna, A. D. (2017). *Tinjauan kriminologis terhadap kejahatan penipuan*. Makassar:Fakultas Hukum Universitas Hasanuddin.

Bahri, I. S. (2020). *Cyber crime dalam sorotan hukum pidana*. Bahasa Rakyat, 159.

Chrisendo, L., & A. T. M. S. (2023). Juridical analysis of law enforcement against fraud with job vacancies mode through social media. *Jurnal Penelitian dan Pengabdian Masyarakat*, 3210.

Margo Hadi Pura, D. N. (2021). *Pembuktian teknologi informasi dan komunikasi (TIK) dalam tahap penyidikan melalui bukti petunjuk melalui ilmu komputer digital forensic di Kepolisian Resort Karawang*. Jurnal Pengabdian Hukum Indonesia.

Prasetiyo, M. Z. (2020). Penegakan hukum oleh aparat penyidik cyber crime dalam kejahatan dunia maya (cyber crime) di wilayah hukum Polda DIY. *Indonesian Journal of Criminal Law and Criminology*, .

Prastini, E. (2018). *Kebijakan kriminal pemerintah terhadap kejahatan dunia maya (cybercrime) di Indonesia.* Jurnal Surya Kencana Dua, 599–600.

Umam. (2022). *Pengertian media sosial, sejarah, fungsi, jenis, manfaat, dan perkembangannya*. Gramedia Blog. https://www.gramedia.com/literasi/pengertianmedia-sosial/

Yahya, H. M. (2015). *Pembahasan permasalahan dan penerapan KUHAP (Pemeriksaan Sidang Pengadilan, Banding, Kasasi dan Peninjauan Kembali)* (Edisi ke-2). Jakarta: Sinar Grafika.

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