LEGAL: Journal of Law
Vol. 4 No. 2, November 2025, 53-66 / ISSN 2829-6672

Implementasi Penggunaan Forensik Digital dalam Penyelidikan dan Penyidikan Tindak Pidana di Polres Wajo

Ismail Ali[1], Yustiana[2], Rusdi Kadir[3], Herianti[4], Besse Nur Fatimah[5]
[1-2-3-4-5]Institut Ilmu Hukum dan Ekonomi Lamaddukelleng

Abstrak
Forensik digital merupakan penggunaan teknik analisis dan investigasi untuk melakukan identifikasi, pengumpulan, pemeriksaan dan penyimpanan bukti atau informasi yang disimpan atau dikodekan pada komputer atau media penyimpanan digital sebagai bagian dari alat bukti yang sah dalam suatu tindak pidana. Forensik digital juga dapat diartikan sebagai penerapan ilmu dan teknologi informasi yang bertujuan untuk membuktikan suatu tindak pidana atau pembuktian kejahatan. Tindakan ini dilakukan oleh perangkat komputer guna mendapatkan bukti digital yang dapat digunakan untuk menangkap pelaku kejahatan. untuk membahas penelitian tersebut maka diajukan permasalahan yaitu Bagaimana implementasi penggunaan forensik digital dalam penyelidikan dan penyidikan tindak pidana di Polres Wajo. Apakah hambatan yang terjadi dalam penerapan teknologi forensik digital dalam penyelidikan dan penyidikan tindak pidana di Polres Wajo beserta upaya yang dilakukan untuk mengatasi hambatan tersebut. Penelitian ini menggunakan metode teknik analisis data berupa empiris kualitatif artinya analisis data pada penelitian ini berdasarkan pada data-data yang telah peneliti kumpulkan secara non-numerik guna memahami fenomena. Fenomena dan fakta yang diperoleh berdasarkan data konkrit yang didapatkan dalam penelitian empiris. Hasil penelitian Berdasarkan ulasan tentang perkembangan peradaban manusia di atas diketahui bahwa seiring perkembangan jaman ilmu teknologi berkembang dengan pesat. Perkembangan teknologi komputer dan internet memberikan dampak terhadap pengaturan atau dan regulasi dalam hukum siber serta terhadap perkembangan kejahatan dalam ruang siber *(cyberspace)*.

Kata Kunci: *Forensik Digital, Penyidikan, Penyelidikan, kejahatan siber*

Abstract
Digital forensics is the use of analytical and investigative techniques to identify, collect, examine, and store evidence or information stored or encoded on a computer or digital storage media as part of valid evidence in a crime. Digital forensics can also be defined as the application of information science and technology aimed at proving a crime or proving a crime. This action is carried out by a computer device to obtain digital evidence that can be used to catch the perpetrator of the crime. To discuss this research, the problem is proposed: How is the implementation of the use of digital forensics in the investigation and investigation of criminal acts at the Wajo Police? What are the obstacles that occur in the application of digital forensic technology in the investigation and investigation of criminal acts at the Wajo Police and the efforts made to overcome these obstacles. This study uses a qualitative empirical data analysis technique method, meaning that the data analysis in this study is based on data that researchers have collected non-numerically to understand the phenomenon. The phenomena and facts obtained are based on concrete data obtained in empirical research. Research Results Based on the review of the development of human civilization above, it is known that along with the development of the era, technological science is developing rapidly. The development of computer and internet technology has an impact on the arrangement and regulation of cyber law as well as on the development of

crime in cyberspace.

Keywords**:** *Digital Forensics, Investigation, Inquiry, Cyber Crime*

PENDAHULUAN

Forensik digital adalah disiplin ilmu yang berfokus pada pengumpulan, analisis, dan penyajian bukti digital yang dapat digunakan dalam proses hukum. Dalam konteks penyelidikan dan penyidikan tindak pidana, forensik digital menjadi sangat penting karena banyaknya kejahatan yang melibatkan teknologi informasi, seperti penipuan online, pencurian identitas, dan kejahatan siber lainnya. Menurut laporan dari Cybersecurity & Infrastructure Security Agency (CISA) pada tahun 2021, lebih dari 50% kejahatan siber yang dilaporkan melibatkan unsur digital, yang menunjukkan pentingnya penerapan forensik digital dalam penegakan hukum (CISA, 2021).

Forensik digital mencakup berbagai aspek, mulai dari pemulihan data yang terhapus, analisis perangkat keras dan perangkat lunak, hingga pengumpulan bukti dari jaringan komputer. Proses ini tidak hanya melibatkan teknologi, tetapi juga memerlukan pemahaman mendalam tentang hukum dan prosedur yang berlaku. Sebagai contoh, dalam kasus pencurian data yang melibatkan perusahaan besar, analisis forensik dapat mengungkap jejak digital yang mengarah pada pelaku kejahatan, yang sering kali sulit ditemukan tanpa metode yang tepat.

Salah satu tantangan dalam forensik digital adalah cepatnya perkembangan teknologi. Setiap tahun, muncul perangkat dan aplikasi baru yang dapat digunakan oleh pelaku kejahatan untuk menyembunyikan jejak digital mereka. Oleh karena itu, para profesional di bidang forensik digital harus terus memperbarui pengetahuan dan keterampilan mereka agar tetap relevan. Menurut sebuah studi yang dilakukan oleh *International Journal of Cyber Criminology*, 70% ahli forensik digital merasa perlu untuk mengikuti pelatihan tambahan setiap tahun untuk mengatasi tantangan baru yang muncul dalam dunia digital (Bada et al., 2020).

Contoh nyata dari penerapan forensik digital dapat dilihat dalam kasus penyelidikan terhadap serangan *ransomware* yang mengincar rumah sakit di Amerika Serikat. Tim forensik digital berhasil mengidentifikasi sumber serangan dan memulihkan data yang telah dienkripsi oleh pelaku. Keberhasilan ini tidak hanya mengurangi kerugian finansial bagi rumah sakit, tetapi juga menyelamatkan nyawa pasien yang bergantung pada akses data medis mereka (FBI, 2021).

Indonesia merupakan negara yang secara tegas menempatkan hukum sebagai landasan utama dalam setiap aspek kehidupan bernegara. Hal ini tercermin dalam Pasal 1 ayat (3) Undang-Undang Dasar Negara Republik Indonesia Tahun 1945 yang menyatakan bahwa Indonesia adalah negara hukum. Konsekuensinya, setiap bentuk pelanggaran atau kejahatan yang terjadi di masyarakat harus diselesaikan melalui proses hukum yang berlaku. Terutama apabila kejahatan tersebut membahayakan keselamatan orang banyak atau mengancam keberlangsungan hidup sumber daya alam.

Sebagai negara hukum, Indonesia mewajibkan seluruh aktivitas masyarakat maupun pemerintahan untuk berjalan sesuai dengan norma dan aturan yang ditetapkan melalui peraturan perundang-undangan. Tujuan dari aturan hukum ini adalah untuk menciptakan keadilan, ketertiban, dan keamanan dalam kehidupan sosial. Maka dari itu, seluruh elemen masyarakat memiliki kewajiban untuk menaati hukum, demi tercapainya masyarakat yang tertib dan damai.

Namun dalam praktiknya, penerapan hukum tidak selalu berjalan ideal. Masih banyak masyarakat yang belum sepenuhnya sadar hukum, sehingga kejahatan tetap

terjadi di berbagai bentuk, baik secara konvensional seperti perampokan, pembunuhan, maupun kejahatan modern yang berbasis teknologi informasi, seperti *cyber crime*.

Perubahan zaman telah membawa masyarakat menuju era digital yang penuh ketergantungan pada teknologi. Teknologi telah menjadi bagian dari hampir seluruh aspek kehidupan, termasuk komunikasi yang kini lebih mengandalkan telepon genggam dan internet dibandingkan cara-cara tradisional. Seiring dengan kemajuan teknologi tersebut, muncul pula bentuk-bentuk kejahatan baru yang memanfaatkan kecanggihan internet. Kejahatan ini dikenal sebagai tindak pidana siber *(cyber crime).*

Cyber crime memiliki karakteristik yang berbeda dari kejahatan konvensional. Jika kejahatan biasa cukup diatur melalui KUHP, maka kejahatan digital memerlukan pengaturan hukum khusus, salah satunya adalah Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik, sebagaimana telah diubah dengan Undang-Undang Nomor 19 Tahun 2016.

Penanganan kasus *cyber crime* juga membutuhkan pendekatan berbeda, terutama dalam hal pembuktian dan penelusuran data. Dalam konteks ini, forensik digital menjadi metode penting yang digunakan oleh aparat penegak hukum. Forensik digital merupakan ilmu yang digunakan untuk mengidentifikasi, mengumpulkan, memeriksa, dan menganalisis data digital guna menemukan bukti dan mengungkap pelaku kejahatan.

Kabupaten Wajo, salah satu wilayah di Provinsi Sulawesi Selatan dengan jumlah penduduk sekitar 379.396 jiwa, turut mengalami perkembangan kejahatan siber. Oleh karena itu, Polres Kabupaten Wajo mulai menerapkan teknologi forensik digital dalam upaya penyelidikan dan penyidikan tindak pidana yang berkaitan dengan dunia maya.

Namun, terdapat kesenjangan antara *das sollen* (apa yang seharusnya menurut hukum) dan *das sein* (apa yang terjadi di lapangan). Undang-Undang Nomor 8 Tahun 1981 tentang KUHAP masih menjadi dasar hukum utama dalam proses penyelidikan dan penyidikan, namun belum sepenuhnya menyesuaikan dengan kebutuhan penegakan hukum di era digital. Oleh karena itu, aparat penegak hukum dituntut untuk mampu mengintegrasikan metode konvensional dengan pendekatan modern melalui penerapan forensik digital.

Penelitian ini dilakukan untuk menganalisis secara mendalam bagaimana implementasi forensik digital diterapkan dalam proses penyelidikan dan penyidikan tindak pidana siber di Polres Wajo. Fokus penelitian diarahkan pada efektivitas penggunaan teknologi forensik digital dalam membantu aparat mengungkap kasus, serta tantangan-tantangan yang dihadapi dalam proses penerapannya

METODE PENELITIAN

Penelitian ini dilaksanakan di Kepolisian Resor (Polres) Kabupaten Wajo yang berlokasi di Jalan Rusa, Kelurahan Bulu Pabbulu, Kecamatan Tempe, Kabupaten Wajo, Sulawesi Selatan. Waktu pelaksanaan penelitian berlangsung selama kurang lebih lima bulan, yaitu dari bulan Maret hingga Juli 2025.

Jenis data yang digunakan dalam penelitian ini terdiri dari data primer dan data sekunder. Data primer diperoleh melalui wawancara terstruktur dengan narasumber yang berasal dari kalangan penyelidik dan penyidik Polres Wajo. Sementara itu, data sekunder diperoleh dari berbagai literatur yang relevan, seperti peraturan perundang-undangan, buku-buku hukum, jurnal ilmiah, skripsi, tesis, serta sumber dari internet yang berkaitan dengan implementasi forensik digital dalam proses penyelidikan dan penyidikan.

Bahan hukum yang digunakan dalam penelitian ini terbagi menjadi tiga, yaitu: bahan hukum primer yang meliputi Undang-Undang Dasar Negara Republik Indonesia Tahun 1945, Undang-Undang Nomor 8 Tahun 1981 tentang Hukum Acara Pidana (KUHAP), serta Undang-Undang Nomor 11 Tahun 2008 beserta perubahannya yaitu Undang-Undang Nomor 19 Tahun 2016 tentang Informasi dan Transaksi Elektronik. Bahan hukum sekunder terdiri dari referensi buku, jurnal, skripsi, dan tesis yang relevan dengan topik penelitian. Adapun bahan hukum tersier diperoleh dari sumber-sumber internet yang mendukung topik penelitian.

Teknik pengumpulan data dilakukan melalui dua pendekatan, yaitu studi pustaka dan penelitian lapangan. Studi pustaka dilakukan dengan menelaah berbagai literatur dan dokumen hukum yang relevan. Sementara itu, penelitian lapangan dilakukan melalui wawancara langsung dengan penyelidik dan penyidik menggunakan metode wawancara terstruktur dan bebas terpimpin, yang memungkinkan pertanyaan berkembang sesuai konteks pembicaraan.

Populasi dalam penelitian ini adalah seluruh penyelidik dan penyidik yang bertugas di Polres Kabupaten Wajo. Pengambilan sampel dilakukan dengan metode *purposive sampling*, yaitu teknik pengambilan sampel berdasarkan pertimbangan dan kriteria tertentu yang ditentukan oleh peneliti, sehingga sampel yang diambil benar-benar mewakili kebutuhan data primer penelitian ini.

Teknik analisis data yang digunakan dalam penelitian ini adalah analisis data kualitatif empiris, yang berarti data dianalisis secara deskriptif berdasarkan fakta dan fenomena yang ditemukan di lapangan maupun dari sumber kepustakaan. Langkah-langkah analisis data mencakup proses pengumpulan data, reduksi data untuk menyaring dan mengorganisir informasi, serta pengolahan data melalui deskripsi dan interpretasi untuk menjawab permasalahan dalam penelitian.

PEMBAHASAN

Urgensi Pengaturan Tata Cara Pembuktian Tindak Pidana

Toffler (1981) menjelaskan tentang tiga hal perubahan kebudayaan sosial masyarakat yang mengubah peradaban manusia secara umum, yang *pertama* berkembangnya masyarakat agraris yang menghapus kebudayaan masyarakat nomaden yang hanya mengandalkan sumber daya alam untuk hidup. Yang *kedua* dimulai sejak revolusi industri yang dimulai pada akhir abad 17 sampai dengan pertengahan abad 20, masa ini ditandai dengan standardinasi, spesialisasi, konsentrasi keuangan, energi, dan kekuasaan, serta produksi, distribusi dan konsumsi yang di lakukan secara masal. Pada era ini muncul teknologi-teknologi yang menggantikan tenaga manusia. *Ketiga* disebut dengan *post-industrial society* yang dimulai sejak akhir yahun 1950-an menekankan pada informasi dan bukan tenaga, era ini disebut juga dengan era informasi atau pengetahuan yang bergantung pada komputer. Era ini ditandai dengan berkembangnya ilmu pengetahuan seperti teori informasi serta teori ruang, dan teknologi-teknologi seperti *biology molecular*, dan *electronic quantum*. Selain itu, peningkatan produktivitas dimungkinkan melalui komputer dan proses data.

Berdasarkan ulasan tentang perkembangan peradaban manusia di atas diketahui bahwa seiring perkembangan jaman ilmu teknologi berkembang dengan pesat. Perkembangan teknologi komputer dan internet memberikan dampak terhadap pengaturan atau dan regulasi dalam hukum siber serta terhadap perkembangan kejahatan dalam *cyberspace* (ruang siber). Lipson H. F (2021) berpendapat bahwa internet pada awalnya tidak pernah dirancang untuk *tracking* dan *tracing user behavior*,

tetapi dirancang untuk kebutuhan militer dalam menghadapi perang dunia selain itu pada awal dibentuknya internet berada dalam satu *control administrator*.

Sistem kontrol administrator ini mengatur secara penuh sistem perangkat lunak jaringan dan sistem perangkat keras komputer. Pengguna awal internet adalah anggota komunitas yang dapat diidentifikasi sehingga dalam hal pengguna melakukan penyalahgunaan jaringan atau perangkat, sistem administrator dapat segera mengetahuinya. Akan tetapi saat internet dilepas ke publik dan bisa diakses semua masyarakat maka bermunculan bermacam sistem administrator baik berupa organisasi maupun individu dari berbagai domain internet. Ketika jaringan dilepaskan ke publik dan NSFNET dinonaktifkan pada tahun 1995, kontrol terpusat awal menghilang, memungkinkan munculnya berbagai administrator jaringan swasta dan publik (Abbate, 1999). Administrasi internet yang pada awalnya berada di bawah kendali tunggal ARPA dan kemudian NSFNET, mengalami desentralisasi kontrol yang signifikan seiring munculnya berbagai domain dan penyedia layanan swasta (Mueller, 2010). Pola sistem administrasi sentral telah diubah dengan sistem administrasi dan desentralisasi. Hal ini berakibat aparat penegak hukum kesulitan dalam menangani pelaku tindak pidana.

Di samping berbagai kemudahan dan manfaat yang diberikan teknologi internet dan komputer, internet juga menimbulkan dampak dan berbagai permasalahan hukum seperti transaksi *online* yang mudah dapat menimbulkan keraguan terhadap keamanan informasi, karena teknologi informasi yang bisa diakses orang lain tanpa diketahui para pihak, semakin berkurangnya saksi yang melihat secara langsung suatu kejadian dalam internet serta kebebasan anonimitas yang diterapkan dalam transaksi elektronik juga mengakibatkan sulitnya aparat penegak hukum dalam mencari dan menemukan pelaku tindak kejahatan siber.

Membicarakan tindak kejahatan siber tentunya tidak lepas dari penegakan hukum yang mengaturnya. Hukum pada dasarnya merupakan pengaturan yang dibuat untuk mengatur perilaku seseorang di dalam masyarakat terhadap suatu pelanggaran dan dikenakan sanksi oleh negara. Meskipun dunia siber ialah dunia maya, hukum tetap diperlukan untuk mengatur sikap masyarakat, karena masyarakat yang ada di dunia maya adalah masyarakat yang hidup di dunia nyata yang memilki nilai dan kepentingan baik secara sendiri-sendiri maupun secara bersama-sama yang harus dilindungi dan hal yang terjadi di dunia maya kerap kali berhubungan dengan dunia nyata dan berakibat langsung bagi masyarakat seperti, transaksi yang dilakukan oleh masyarakat memiliki pengaruh dalam dunia nyata, baik secara ekonomis maupun non ekonomis.

Di dalam dunia siber kejahatan bisa bertambah semakin kompleks dan beraneka ragam jenisnya dibanding di dunia nyata karena jutaan orang mengunjunginya tanpa batasan ruang dan waktu. Membicarakan tentang urgensi tata cara pembuktian tindak pidana siber *(cybercrime)* berarti membicarakan mengenai seberapa pentingnya tata cara pembuktian tersebut harus ada.

Alat Bukti Elektronik Mempunyai Sifat Mudah Rusak

Menurut Alan M Gahtan (1999) bukti elektronik adalah bukti informasi yang tersimpan secara elektronik dalam bentuk komputer dalam suatu tindakan hukum. Penjelasan tersebut menerangkan bahwa untuk kepentingan tindakan hukum bukti elektronik yang didapat berasal dari data elektronik, dan disebut bukti elektronik apabila bukti tersebut tersimpan secara elektronik dalam suatu mesin penyimpanan data. Data elektronik komputer adalah data yang dapat dibaca menggunakan bantuan mesin elektronik yang dapat berupa data *base36, source code, object code*, data yang tersimpan dalam file komputer, data yang tersimpan dalam metode penyimpanan

elektronik seperti *flashdisk*, CD atau alat lain. Karakteristik bukti elektronik berbeda dengan bukti konvensional, bukti elektronik berupa bukti perangkat lunak *(software)*. Sesuai dengan pasal 1 ayat 1 Undang-Undang Nomor 11 Tahun 2008 Tentang Informasi Dan Transaksi Elektronik (UUITE) dan juga pasal 1 ayat 4 UUITE.

Bukti elektronik tidak terbatas pada tulisan, gambar, atau foto tetapi juga berupa kode, simbol dan grafik yang diolah melalui komputer, oleh sebab itu bukti elektronik bisa dikatakan khusus dan bersifat mudah rusak karena sifatnya yang tidak tetap yang tak terbatas. Karakteristik tersebut adalah yang pertama data elektronik mudah untuk menyimpannya serta mudah untuk dibawa dan dihilangkan. Serta data elektronik mudah untuk diubah dan dirusak dan dengan bahkan perusakan tersebut dapat ditutupi.

Salah satu karakteristik khusus bukti elektronik bentuknya yang disimpan dalam media elektronik, di samping itu bukti elektronik dapat dengan mudah direkayasa sehingga sering diragukan validitasnya. Salah satu contohnya Seperti halnya dengan salah satu aplikasi chat saat ini yang dapat diunduh bebas di perangkat *handphone* yaitu line dari Line Corporation, pada fitur terbarunya line menyajikan fitur khusus untuk kontrol obrolan dalam durasi tertentu yakni pada durasi satu jam, enam jam, dan dua puluh empat jam, jadi bukti elektronik bisa hapus dengan sendirinya, di mana apabila dikaitkan pada proses pembuktian hal ini menjadi kelehaman juga untuk obrolan yang digunakan sebagai alat bukti karena dengan mudahnya secara otomatis di hapus oleh aplikasi line itu sendiri, jadi hilangnya alat bukti tidak harus dari pelaku secara manual karena bisa diatur secara otomatis.

Sebagai Acuan Penyidik Dalam Memperlakukan Barang Bukti Elektronik

Dalam memperlakukan barang bukti elektronik penyidik tidak boleh sembarangan dalam melakukan penyidikan, oleh sebab itu harus ada acuannya karena data elektronik mempunyai resiko mudah hancur. Penyidik harus memiliki panduan tentang cara memperkenalkan bukti komputer ke pengadilan dengan menggunakan standar yang berlaku sesuai dengan undang-undang. Adanya peraturan mengenai tata cara melakukan pembuktian tindak pidana siber dapat melindungi data yang telah diamankan dan juga berguna untuk mengamankan jaringan komputer, menangkap suatu informasi penting yang berguna untuk menangkap tersangka yang berkelompok. Kejahatan yang melibatkan perangkat elektronik beraneka ragam mulai dari pornografi, terorisme, hingga pencurian data pribadi bahkan data suatu pemerintahan. Penyidik harus memiliki keahlian di bidang teknologi informasi dan perangkat elektronik yang memadai yang tepat untuk digunakan mengungkap suatu kejahatan.

Suatu file komputer mungkin telah dihapus, rusak dan hilang akan tetapi hal tersebut bisa dipulihkan kembali dengan keahlian khusus. Dalam prakteknya pejabat yang berwenang melakukan autentifikasi untuk memperkuat validitas bukti elektronik, untuk mempermudahnya suatu arsip elektronik akan meliputi:

1. Validitas substansi informasi ditentukan oleh proses pengolahan informasi dan identitas hukum para pihak *(legal identity).*
2. Format formasi akan ditentukan oleh kepentingan para pihak dan atau sesuai dengan konteks komunikasi yang terjadi, khususnya kepada siapa informasi itu ditujukan.
3. Tanggung jawab para pihak, baik sebagai si penyampai informasi *(originators)* dan si penerima atau tujuan infomasi *(recipient)*, sebenarnya dipengaruhi oleh kaedah-kaedah hukum yang berlaku, baik secara etis maupun berdasarkan peraturan perundang-undangan.

4. Validitas informasi sebagai output, secara teknis dan yuridis semestinya ditentukan oleh validitas sistem informasi dan komunikasi yang ada.

Autentifikasi adalah melakukan sebuah proses untuk menjamin keaslian dokumen elektronik, karena bukti elektronik mudah dipalsukan dan dihapus. Autentikasi bukti elektronik dapat ditampilkan dalam bentuk cetak *hard copy* dari komputer atau alat penyimpanan data elektronik yang disalin langsung dari alat penyimpanan asli (original). Dalam kejahatan siber seringkali aparat penegak hukum penyidik, penuntut umum, hakim dan pengacara dihadapkan pada kesulitan menentukan kebenaran bukti- bukti elektronik ketika menangani hal tersebut. Hal ini disebabkan katena mayoritas bukti elektronik yang ada berupa catatan-catatan elektronik yang tersimpan dalam alat penyimpanan data maupun yang dicetak dari komputer tersebut.

Dan tidak semua orang bisa membaca data dalam komputer hanya sebagian orang tertentu seperti ahli di bidang teknologi informasi saja, oleh karena itu aparat penegak hukum seperti penyidik, pengacara, penuntut umum, dan hakim harus mempunyai keahlian khusus dibidang teknologi informasi dan juga mempunuai acuan dasar di dalam undang-undang untuk melakukan pembuktian yang baik dan benar. Dalam proses pembuktian di persidangan, yang diperlukan hanya hasil cetakannya *(printout)* alat bukti surat elektronik dan tidak diperlukan bentuk aslinya *(soft copy).* Hal ini mengacu kepada Pasal 5 ayat (1) UndangUndang No.11 Tahun 2008. Mengenai aspek keaslian dari hasil cetakan *(printout)* surat elektronik, dikatakan sebagai alat bukti yang sah apabila telah memenuhi aspek keaslian sebagai alat bukti, dalam pengadilan hakim akan bertanya kepada terdakwa atau korban tentang surat elektronik tersebut, apakah terdapat perbedaan dari bentuk aslinya atau tidak, jika terdakwa atau korban mengakui bahwa surat elektronik tersebut sama dengan aslinya atau tidak terdapat perbedaan maka surat elektronik tersebut sah. Apabila salah satu pihak tidak mengakui maka diperlukan keterangan ahli untuk menentukan sah atau tidaknya hasil cetak dari surat elektronik tersebut, dan keterangan ahli tersebut akan menjadi dasar pertimbangan hakim dalam menentukan sah atau tidaknya hasil cetak *(printout)* surat elektronik sebagai alat bukti dalam persidangan.

Adapun tata cara pembuktian tindak pidana siber di indonesia selama ini dengan cara melakukan *digital forensic* dengan menggunakan bantuan ahli komputer. Karena permasalahan yang ada di dalam komputer sangat komplek oleh sebab itu dibutuhkan ahli di bidang komputer untuk memeriksa data rahasia, data yang sudah dihapus dan diubah.

Kredibilitas Barang Bukti Elektronik Dapat Dipertanggungjawabkan di Persidangan

Untuk mencari dan menangani bukti elektronik dengan baik dan benar digunakan metode penanganan khusus yaitu dengan melakukan forensik digital, Secara garis besar, forensik digital adalah salah satu cabang ilmu Informatika untuk menganalisa barang bukti elektronik yang disebut juga forensik digital yang memiliki pemahaman yang sama dengan forensik pada umumnya. Didalam istilah hukum Indonesia forensik artinya suatu ilmu pengetahuan yang menggunakan multi disiplin ilmu yaitu dengan menerapkan ilmu pengetahuan alam seperti kimia, fisika, biologi, psikologi, kedokteran, psikologi dan kriminologi yang bertujuan membuat terang suatu perkara pidana dan membuktikan ada tidaknya kejahatan atau pelanggaran dengan memeriksa barang bukti fisik dalam perkara tersebut.

Forensik adalah proses penggunaan pengetahuan ilmiah untuk mengumpulkan, menganalisis, dan menyajikan bukti ke pengadilan (NIST dan DOJ). Definisi forensik

didasarkan pada prinsip bahwa bukti ilmiah harus dapat dipertanggungjawabkan dalam persidangan hukum (Widodo, 2017). Kata forensik berarti *membawa ke pengadilan*.

Metodologi digital forensik terdiri dari serangkaian langkah sistematis yang dirancang untuk memastikan bahwa bukti digital dapat diperoleh, dianalisis, dan disajikan dengan cara yang sah dan dapat diterima di pengadilan. Langkah-langkah ini biasanya meliputi identifikasi, pengambilan, analisis, dan pelaporan. Setiap langkah memiliki tujuan dan teknik spesifik yang harus diikuti untuk menjaga integritas bukti digital. Menurut National Institute of Standards and Technology (NIST), mengikuti metodologi yang tepat sangat penting untuk memastikan bahwa bukti yang diperoleh dapat dipertanggungjawabkan di hadapan hukum (NIST, 2006).

Forensik terutama berkaitan dengan pemulihan dan analisis bukti yang tidak terlihat (laten). Bukti laten dapat mengambil banyak bentuk, dari sidik jari yang tertinggal di jendela sampai bukti DNA pulih dari noda darah ke file pada *hard drive*. Berdasarkan hasil wawancara yang dilakukan bersama Bripka Hermansyah beliau mengatakan bahwa implementasi penggunaan forensik digital khususnya melalui analisis sidik jari, merupakan langkah penting dalam memperkuat pembuktian .ia menilai bahwa penggunaan teknologi digital untuk memindai, mencocokkan, dan mengidentifikasi sidik jari tersangka secara cepat dan akurat sangat membantu dalam mempercepat proses pengungkapan kasus, meskipun masih diperlukan peningkatan alat dan pelatihan personel guna memaksimalkan hasil pemerikasaan forensik tersebut.

Itu sebabnya mengapa hasil analisa dari forensik digital harus bisa dipertanggungjawabkan di sidang pengadilan. Forensik digital tidak hanya diperlukan untuk menganalisa kasus tindak pidana siber tetapi juga di perlukan untuk semua kasus tindak pidana karena saat ini semua kasus memiliki bukti digital karena diakibatkan dari pengaruh perkembangan zaman yang modern. Forensik digital sangat diperlukan di dalam semua kasus tindak pidana karena mampu menemukan data yang sulit dicari sekalipun.

Melakukan forensik digital seharusnya menerapkan prosedur untuk mengumpulkan dan mengamankan bukti digital. Terdapat dua jenis data dasar yang dapat dikumpulkan dalam komputer forensik. Data yang persisten adalah data yang tersimpan pada *hard drive* lokal (atau media lain) dan dipelihara saat komputer dimatikan. Data volatil adalah data yang tersimpan dalam memori, atau ada dalam transit, yang akan hilang saat komputer kehilangan daya atau dimatikan. Data volatil berada pada *register*, *cache*, dan *random access memory* (RAM).

Karena data volatil bersifat sementara, sangat penting penyidik mengetahui cara yang andal untuk menangkapnya. Administrator sistem dan petugas keamanan juga harus memiliki pemahaman dasar tentang bagaimana tugas rutin komputer dan jaringan dapat mempengaruhi proses forensik (kemungkinan diterimanya bukti di pengadilan) dan kemampuan untuk memulihkan data yang mungkin penting untuk identifikasi dan analisis.

Adapun di Indonesia sendiri untuk memperoleh dan memperlakukan bukti elektronik aparat penegak hukum juga melakukan forensik digital dengan tahapan-tahapan sebagai berikut.

1. *Pengambilan bukti digital*. Mengingat sifatnya yang dapat diubah, dirusak, atau dihilangkan apabila tidak ditangani dengan tepat, pengambilan informasi atau dokumen elektronik harus dilakukan dengan menjaga dan melindungi keutuhan atau integritasnya. Tahap ini dimaksudkan untuk mengambil dan mengamankan alat bukti elektronik (orijinal). Cara atau prosedur pengambilan alat bukti elektronik

original dapat didasarkan pada kondisi awal ditemukannya alat bukti elektronik atau alat perangkat yang menyimpan alat bukti elektronik tersebut.

Alat penyimpanan yang bisa dijadikan sebagai barang bukti mencakup sebuah sistem komputer, media penyimpanan seperti *handphone, flash disk, hard disk, pen drive, smart card,* atau *CD- ROM), PDA, e-mail, sms, cookies, source code, windows registry, document, web browser bookmark, chat loglog file*, atau bahkan sederetan paket yang berpindah dalam jaringan komputer.

2. *Kewajiban menyimpan dokumen elektronik*. Ada kalanya hukum mengharuskan pihak tertentu untuk menyimpan data atau dokumen untuk jangka waktu tertentu, misalnya untuk keperluan akuntansi atau pajak. Akan tetapi, suatu data elektronik tidak selamanya dapat diharapkan disimpan dalam bentuknya yang asli mengingat tidak jarang data tersebut disimpan dalam bentuk yang sudah dipendekkan, atau diubah bentuk dan format dan sebagainya.

   Oleh karena itu, jika data atau dokumen tersebut merupakan data elektronik, maka kewajiban data atau dokumen tersebut harus dianggap telah memenuhi persyaratan hukum jika, (a) Informasi dalam dokumen elektronik tersebut masih dapat diakses untuk masa selanjutnya; (b) Informasi tersebut disimpan tetapi masih dapat diidentifikasi keasliannya dan tujuannya, dan dapat pula ditentukan waktu data tersebut diterima atau dikirim; (c) Informasi disimpan dalam format asli ketika disimpan, dikirim, atau diterima, atau dalam format yang dapat ditunjukkan bahwa data tersebut merepresentasikan secara akurat terhadap informasi yang disimpan, dikirim, atau diterima tersebut.

   Namun demikian, kewajiban menyimpan data tersebut tentunya tidak berlaku terhadap data atau informasi yang mempunyai tujuan hanya untuk dikirim atau diterima, Penyimpanan dan penyiapan bukti-bukti yang ada, termasuk melindungi bukti-bukti dari kerusakan, perubahan dan penghilangan oleh pihak-pihak tertentu.

   Bukti harus benar-benar steril artinya belum mengalami proses apapun ketika diserahkan kepada ahli forensik digital untuk diteliti. Karena bukti digital bersifat sementara *(volatile)*, mudah rusak, berubah dan hilang, maka pengetahuan yang mendalam dari seorang ahli forensik digital mutlak diperlukan. Kesalahan kecil pada penanganan bukti digital dapat membuat barang bukti digital tidak diakui di pengadilan. Bahkan menghidupkan dan mematikan komputer dengan tidak hati-hati bisa saja merusak atau mengubah barang bukti tersebut. Karena saat komputer dihidupkan terjadi beberapa perubahan pada temporari file, waktu akses, dan seterusnya. Sekali file-file ini telah berubah ketika komputer dihidupkan dan tidak ada cara untuk mengembalikan *(recover)* file-file tersebut kepada keadaan semula. Karena komputer dalam kondisi hidup juga tidak bisa sembarangan dimatikan, sebab jika komputer dimatikan data-data yang ada bisa terhapus oleh program komputer.

   Oleh sebab itu seorang ahli forensik digital harus menguasai langkah-langkah tertentu dalam mematikan atau menghidupkan komputer agar tidak merusak atau menghilangkan barang bukti yang ada di dalamnya. Aturan utama pada tahap ini adalah bukti asli tidak boleh di ikutkan dalam penyidikan karena dikhawatirkan akan dapat merubah isi dan struktur yang ada didalamnya. Untuk mengatasi hal ini maka dilakukan penyalinan *copy* data secara *bitstream image* dari bukti asli ke media penyimpanan lainnya. Dengan kata lain, setiap biner digit demi digit disalin secara utuh dalam media baru. Teknik ini umumnya diistilahkan dengan *cloning* atau *imaging*. Data hasil cloning inilah yang selanjutnya menjadi objek penelitian

dan penyelidikan.

3. *Pemeriksaan alat bukti.* Pemeriksaan terhadap alat bukti elektronik original umumnya menggunakan perangkat keras dan perangkat lunak yang khusus dibuat untuk kepentingan forensik digital. Pada tahap ini, pemeriksa melakukan ekstraksi, yaitu mengambil seluruh data dari media di mana data tersebut mengambil seluruh data dari media di mana data tersebut tersimpan, termasuk data yang telah terhapus sebelumnya. Pemeriksa juga perlu menggunakan *write blocker*, yaitu alat yang digunakan untuk mencegah penulisan terhadap data original. Selain itu, dalam melakukan pengambilan data, pemeriksa juga perlu menentukan nilai dari keseluruhan data yang diambil *(hash).*

   Nilai *(hash)* dari data original akan sama dengan nilai dari hasil ekstraksi. Sehingga, apabila diperlukan pemeriksaan ulang oleh pemeriksa yang berbeda (misalnya pemeriksa dari advikat tersangka), nilai dari alat bukti elektronik tersebut akan sama. Setelah alat bukti elektronik harus dilakukan dengan membuat salinan dari informasi atau dokumen elektronik yang asli. Pengambilan informasi atau dokumen elektronik dilakukan, tahap selanjutnya ialah pemeriksaan dan analisa terhadap alat selanjutnya ialah pemeriksaan dan analisa terhadap alat bukti elektronik. Pemeriksaan dilakukan terhadap salinan dari alat bukti elektronik yang asli. Pemeriksa juga dapat membuat salinan dari alinan alat bukti elektronik sebagai bahan kerja. Pada tahap ini, pemeriksa juga melakukan analisa, yaitu adalah mengintepretasikan informasi yang telah diekstraksi dan menentukan informasi atau data yang relevan dengan tindak pidana.

   Tergantung dari jenis tindak pidana, dalam tahap ini, pemeriksa mencari informasi elektronik atau dokumen elektronik yang menunjukan adanya tindak pidana atau menunjukan pelaku tindak pidana. Misalnya, dalam tindak pidana penyebaran pornografi, pemeriksa harus menemukan adanya file-file pornografi dalam komputer, laptop, atau USB pelaku. Untuk membuktikan adanya penyebaran, pemeriksa dapat mencari rekaman email yang masih tersimpan dalam komputer pelaku dari rekaman email tersebut, pemeriksa dapat mengetahui penerima email. Dalam tindak pidana akses illegal, pemeriksa harus menemukan adanya rekaman aktivitas transaksi elektronik *log file* yang menunjukan bahwa pelaku, dengan menggunakan IP tertentu, berhasil mengakses sesuatu website secara ilegal.
4. *Dokumentasi dan presentasi*. Setiap tindakan yang dilakukan dalam pengumpulan dan pemeriksaan alat bukti elektronik harus didokumentasikan secara akurat dan menyuluruh. Tindak hanya tindakan dalam melakukan digital forensk, tetapi juga tindakan yang terkait dengannya, misalnya serah terima komputer dari petugas yang mengambil barang di tempat kejadian perkara kepada pemeriksa forensik. Laporan dapat memuat proses dan tahapan yang dilakukan dalam pemeriksaan, termasuk alat dan perangkat yang digunakan. Selain itu, laporan juga perlu memuat informasi mengenai keseluruhan data yang diperoleh serta yang relevan dengan tindak pidana. Penanganan yang tidak tepat terhadap komputer yang menyala dapat menghilangkan informasi elektronik yang sifatnya tidak stabil.
5. Tindak diberikannya label terhadap komponen serta kabel atau port dari alat dan perangkat yang telah dipreteli di tempat kejadian perkara dapat menyulitkan analisis forensik digital untuk menyusun kembali perangkat tersebut di laboratorium forensik. Demikian juga pencatatan yang tidak lengkap dapat menimbulkan keraguan hakim atau pengacara terhadap hasil forensik yang dilakukan. Dalam pengumpulan alat bukti elektronik, penyidik akan menemukan

berbagai informasi, baik yang relevan dengan tindak pidana, maupun yang tidak relevan. Terkait dengan hal ini, penyidik harus menjaga kerahasiaan informasi, khususnya informasi terkait privasi seseorang yang tidak relevan dengan tindak pidana. Semua informasi yang tidak relevan tidak boleh diungkap di pengadilan.

Menghindari Kekosongan Yuridis mengenai Pengaturan Tata Cara Pembuktian Tindak Pidana Siber

Sistem peradilan pidana dibentuk untuk menanggulangi kejahatan di masyarakat yaitu terdapat serangkaian subsistem pendukung yang saling berkaitan yakni kepolisian, kejaksaan, pengadilan dan lembaga pemasyarakatan yang secara keseluruhan membentuk kesatuan lembaga penegak hukum. Tugas dan wewenang lembaga penegak hukum masingmasing secara garis besar adalah sebagai berikut.

1. Kepolisian.
   Tugas kepolisian di bidang penyidikan, melakukan penyidikan tambahan, berperan sebagai koordinator dan pengawas Penyidik Pegawai Negeri Sipil adalah kewenangan kepolisian. KUHAP ini mengatur cara mengenai dapat atau tidaknya dilakukan penyidikan dgn mencari tahu dan menemukan suatu peristiwa yang diduga sebagai tindak pidana yg merupakan ruang lingkup penyelidikan.
2. Kejaksaan.
   Lembaga kejaksaan bertugas melakukan penuntutan terhadap suatu tindak pidana. Kejaksaan bertugas sebagai lembaga penuntut dan pelaksana dari putusan pengadilan pidana dari semua tingkat pengadilan. Tugas-tugasnya adalah melaksanakan putusan-putusan pengadilan pidana mempertahankan ketentuan undang-undang, melakukan penuntutan tindak-tindak pidana pelanggaran dan kejahatan melakukan penyidikan dan penyidikan lanjutan. Di dalam Undang-undang Nomor 16 tahun 2004 Tentang Kejaksana Republik Indonesia pasal 2 menyatakan bahwa Kejaksaan adalah lembaga pemerintahan yang melaksanakan kekuasaan negara di bidang penuntutan serta kewenangan lain berdasarkan undang-undang.
3. Pengadilan.
   Lembaga pengadilan adalah pelaksanaan atau penerapan hukum terhadap suatu perkara dengan suatu putusan hakim yang bersifat melihat, putusan mana dapat berupa pemidanaan, pembebasan maupun pelepasan dari hukuman terhadap pelaku tindak pidana. Di sini lembaga pengadilan adalah lembaga penegak hukum yang paling penting dikarenakan untuk menentukan terdakwa tersebut bersalah atau tidak. Hakim memiliki peranan yang sangat besar untuk menentukan pelaksanaan sistem peradilan pidana hakim tidak boleh pandang bulu dalam melaksanakan putusan. Dalam hal pembuktain tindak pidana siber dibutuhkan penelitian lebih lanjut mengenai pengaturan pembuktian tindak pidana siber secara konvensional di Indonesia.

   Kejahatan siber merupakan perbuatan melawan hukum yang dilakukan dengan memakai komputer sebagai sarana, alat atau komputer sebagai objek, baik untuk memperoleh keuntungan ataupun tidak, dengan merugikan pihak lain. *Cyber crime* di sisi lain, bukan hanya menggunakan kecanggihan teknologi komputer, akan tetapi juga melibatkan teknologi telekomunikasi di dalam pengoperasiannya. Pembuktian bertujuan untuk mengetahui tentang cara meletakkan hasil pembuktian terhadap perkara yang sedang diperiksa, beberapa sistem pembuktian sebagai berikut:
   a. Sistem atau teori pembuktian berdasarkan undang-undang secara positif.
   b. Sistem atau teori pembuktian berdasarkan keyakinan hakim.

c. Sistem atau teori pembuktian berdasar keyakinan atas alasan yang logis *(laconviction raisonnee).*
d. Teori pembuktian berdasarkan undang-undang secara negatif *(negatief wettelijk)* Pembuktian yang dianut oleh Indonesia adalah pembuktian menurut undang-undang secara negatif. Sistem pembuktian ini merupakan gabungan dari sistem pembutian menurut undang-undang secara positif dan sistem pembuktian berdasarkan keyakinan hakim melulu *(conviction intime)*.

Agar suatu transaksi elektronik dalam pengadilan pidana dapat diterima menjadi bukti terdapat beberapa cara, antara lain:

1. *The real evidence route*. Bukti elektronik sebagai suatu alat bukti yang sah dan yang berdiri sendiri *(real evidencce)* tentunya suatu rekaman atau salinan data *(data recording)* harus dapat memberikan jaminan berjalan sesuai dengan prosedur yang berlaku (telah diprogram) sedemikian rupa sehingga dalam pembuktian suatu kasus hasil print out suatu data dapat diterima.
2. *The statutory route*. Suatu bukti elektronik dapat diterima sebagai alat bukti di pengadilan jika suatu data *(statutory route)* sudah di tetapkan dan dikatakan sah. Contohnya dalam suatu kasus dengan mempertimbangakan suatu dokumen merupakan dokumen publik maka mengedepankan salinan dokumen berupa ijazah.

   Dokumen atau data tersebut disahkan oleh negara atau pengadilan yang merupakan pihak yang memiliki kewenangan dan dalam hal pembuktian suatu kasus, keabsahan data dokumen tidak harus tercetak di atas kertas tapi juga termasuk data atau informasi yang ada dalam sebuah disket, dokumen yang diterima dengan menggunakan komputer melalui fasilitas telekomunikasi (fax,e-mail) sepanjang dapat dibuktikan data informasi itu asli (original) atau hasil fotokopi yang otentik, kemungkinan data atau informasi tersebut dapat diterima. Pada kategorisasi ini yang ditetapkan adalah data atau informasi yang ada di dalamnya, atau data tersebut dinyatakan otentik.
3. *The expert witness*. Selanjutnya dalam peranan saksi ahli *(the expert witness)* adalah bahwa keterangan seorang ahli dapat dijadikan alat bukti terhadap suatu kasus, dimana keterangan yang diberikan berdasarkan pada pengetahuan dan pengalaman. Hakin akan mempertimbangkan kesaksian seorang ahli terutama mengenai kekuatan pembuktian suatu alat bukti dan memberikan suatu standar keakuratan dan keobjektifan bekerjanya suatu sistem komputer. Seorang ahli dapat dipanggil jika terjadi suatu kasus penggunaan komputer secara ilegal maka di dalam suatu persidangan kemudian saksi tersebut memberikan keterangan mengenai cara kerja dan sistem komputer.

SIMPULAN

Kejahatan dunia maya merupakan masalah serius yang memerlukan penanganan data elektronik secara cermat. Kejahatan ini melibatkan penggunaan perangkat lunak komputer untuk melindungi informasi sensitif dan menjaga identitas hukum. Kejahatan dunia maya dapat melibatkan berbagai bentuk data elektronik, seperti pornografi, terorisme, dan perlindungan data pribadi. Pelaku kejahatan dunia maya harus memiliki pengetahuan tentang teknologi informasi dan sistem elektronik untuk melindungi data mereka. Digital forensik tidak hanya diperlukan untuk menganalisa kasus tindak pidana siber *(cybercrime)* tetapi juga di perlukan untuk semua kasus tindak pidana karena saat ini semua kasus memiliki bukti digital karena diakibatkan dari pengaruh perkembangan zaman yang modern. Digital forensik sangat diperlukan di dalam semua kasus tindak

pidana karena mampu menemukan data yang sulit dicari sekalipun.

Dan saat melakukan digital forensik seharusnya menerapkan prosedur untuk mengunpulkan dan mengamankan bukti digital. Terdapat dua jenis data dasar yang dapat dikumpulkan dalam komputer forensik, Data yang persisten adalah data yang tersimpan pada *hard drive* lokal (atau media lain) dan dipelihara saat komputer dimatikan. Data volatil adalah data yang tersimpan dalam memori, atau ada dalam transit, yang akan hilang saat komputer kehilangan daya atau dimatikan. Data volatil berada *pada register, cache,* dan *random access memory* (RAM).

Karena data volatil bersifat sementara, sangat penting penyidik mengetahui cara yang andal untuk menangkapnya. Administrator sistem dan petugas keamanan juga harus memiliki pemahaman dasar tentang bagaimana tugas rutin komputer dan jaringan dapat mempengaruhi proses forensik (kemungkinan diterimanya bukti di pengadilan) dan kemampuan untuk memulihkan data yang mungkin penting untuk identifikasi dan analisis. Polres wajo telah melakukan tahap pengembangan dan belum sepenuhnya optimal, digital forensik digunakan untuk mendukung pembuktian dalam tindak pidana yang melibatkan perangkat digital seperti kejahatan siber, penipuan online, serta beberapa tindak pidana yang memiliki bukti digital.

DAFTAR PUSTAKA

Abbate, J. (1999). *Inventing the Internet*. Cambridge: MIT Press.

Alan M. Gahtan. (1999). *Electronic Evidence*. Toronto: Carswell.

Andi Bau Mallarangeng, Andi Wahyuddin Nur, Martono, & Muhammad Syahbana. (2025). Penegakan Hukum Terhadap Penyebarluasan Foto Vulgar di Media Sosial Disertai Pemerasan dan Pengancaman di Kabupaten Wajo. *Legal Journal of Law*, 4(1), 65–76. Diambil dari https://jurnal.lamaddukelleng.ac.id/index.php/legal/article/view/128

Bada, A., & Sasse, M. A. (2020). The Role of Digital Forensics in Cyber Crime Investigation. *International Journal of Cyber Criminology*, 14(1), 1-16.

CISA. (2021). *Cybersecurity & Infrastructure Security Agency Annual Report*. Washington, DC: Cybersecurity & Infrastructure Security Agency.

FBI. (2013). *FBI Arrests Silk Road Operator.* Washington, DC: Federal Bureau of Investigation.

Indonesia. (2008). *Undang-Undang Republik Indonesia Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik. Lembaran Negara Republik Indonesia Tahun 2008 Nomor 58*. Jakarta: Sekretariat Negara.

Ismail Ali, Besse Muqita Dewi, Andi Wahyuddin Nur, & Andi Wira Saputra. (2023). Tinjauan Sosio Yuridis Terhadap Penerapan Sistem Digital Id Berbasis Aplikasi Pada Dinas Kependudukan Dan Pencatatan Sipil Kabupaten Wajo. *Legal Journal of Law*, 2(2), 25–35. Diambil dari https://jurnal.lamaddukelleng.ac.id/index.php/legal/article/view/70.

Kepolisian Negara Republik Indonesia. (2010). *Peraturan Kepala Kepolisian Negara Republik Indonesia Nomor 10 Tahun 2010 tentang Tata Cara Pengelolaan Barang Bukti Digital*. Jakarta: Kepolisian Negara Republik Indonesia.

Lipson, H. F. (2021, Mei). *The inherent vulnerabilities of the internet's original design*.

CISA Webinar.

Martono, Muharawati, & Besse Astria Devi. (2024). Pertimbangan Penyidik dalam Penghentian Penyidikan dalam Delik Culpa. *Legal Journal of Law*, 3(1), 43–52. Retrieved from https://jurnal.lamaddukelleng.ac.id/index.php/legal/article/view/25.

Mueller, M. L. (2010). *Networks and States: The global politics of internet governance*. Cambridge: MIT Press.

Muharawati, Hardian Kumala, Ramadhani, W. S., Nurfadillah, Yuswan, M., Sunarti, & Alfarizy, A. (2024). Analisis Fenomena Anak Sebagai Pelaku Kejahatan Penipuan Online di Kabupaten Wajo dari Perspektif Kriminologis. *Legal Journal of Law*, 3(2), 41–49. Diambil dari https://jurnal.lamaddukelleng.ac.id/index.php/legal/article/view/33.

Munir, R. (2012). *Forensik Digital: Metode dan Analisis Bukti Elektronik*. Bandung: Informatika Bandung.

National Institute of Standards and Technology. (n.d.). *Forensic Science*. Diakses dari www.nist.govU.S. Department of Justice. (n.d.). *Forensic Science*. Diakses dari nij.ojp.gov.

NIST. (2014). *Guidelines on Multimedia Evidence Collection, Analysis, and Exchange.* National Institute of Standards and Technology (NIST Interagency Report 800-89).

NIST. (2006). *Guide to Integrating Forensic Techniques into Incident Response*. National Institute of Standards and Technology. (NIST SP 800-86). U.S. Department of Commerce.

Nur, A. W., Firsan, M. ., Syahbana, M. S., Ramadandi, Sefiani, AU, S. Z., & Masse, N. H. (2024). Transaksi Jual Beli Online Menurut Undang-Undang Perlindungan Konsumen. *Legal Journal of Law*, 3(2), 14–20. Diambil dari https://jurnal.lamaddukelleng.ac.id/index.php/legal/article/view/35

Sulaeman, Yustiana, Martono, & Herawati. (2025). Perlindungan Hukum Terhadap Penyerbarluasan Data Pribadi Pelaku Pinjaman Online di Kabupaten Wajo. Legal *Journal of Law*, 4(1), 55–64. Diambil dari https://jurnal.lamaddukelleng.ac.id/index.php/legal/article/view/127

Toffler, A. (1981). *Kejutan masa depan* (Terjemahan: Ali Shahab). Jakarta: PT Gramedia.

Widodo, W. (2017). *Pengantar Ilmu Forensik untuk Penegakan Hukum*. Semarang: UPT Undip.

.