Jurnal Penelitian Nusantara
Volume 1 ; Nomor 9 ; Oktober 2025 ; Page 359-368
Doi : https://doi.org/10.59435/menulis.v1i10.696
Website : https://padangjurnal.web.id/index.php/menulis
E-ISSN : 3088-988X

Jejak Digital Di Balik Investigasi Kriminal: Studi Atas Pengelolaan Bukti Oleh Kepolisian Samarinda

M. Ilham Maulana Firdaus

Mahasiswa Program Studi Ilmu Hukum, Fakultas Hukum, Ilmu Sosial, dan Ilmu Politik,
Universitas Terbuka
Email: *Ilhammuhammd123456@gmail.com*

ABSTRAK

Kemajuan teknologi digital dalam beberapa tahun terakhir telah menghadirkan tantangan yang signifikan dalam investigasi kriminal, terutama terkait pengelolaan bukti digital. Penelitian ini bertujuan untuk menganalisis proses pengelolaan bukti digital dalam investigasi kriminal di Kepolisian Samarinda. Penelitian ini juga mengidentifikasi tantangan yang dihadapi, seperti keterbatasan personel terlatih dan sumber daya teknologi yang memadai. Metode yang digunakan adalah pendekatan yuridis normatif dengan menganalisis norma hukum serta melakukan wawancara mendalam dengan penyidik yang bertugas di Satuan Reserse Kriminal Polresta Samarinda. Hasil penelitian menunjukkan bahwa pengelolaan bukti digital mencakup tahapan identifikasi, pengumpulan, penyimpanan, dan analisis yang membutuhkan alat serta protokol khusus untuk menjaga integritas bukti. Tantangan seperti kurangnya keahlian forensik digital dan regulasi hukum yang belum jelas juga dibahas, dengan solusi berupa peningkatan pelatihan dan pembaruan regulasi hukum. Studi ini menekankan pentingnya kolaborasi antara penegak hukum dan penyedia teknologi untuk meningkatkan kemampuan investigasi.

Kata kunci: Bukti digital, investigasi kriminal, kerangka hukum, teknologi forensik

PENDAHULUAN

Perkembangan teknologi informasi dan komunikasi dalam beberapa tahun terakhir telah menghadirkan tantangan baru dalam proses penegakan hukum. Salah satu tantangan tersebut adalah munculnya bukti digital, yang menjadi elemen krusial dalam investigasi kriminal. Bukti digital ini meliputi data elektronik yang diperoleh dari perangkat elektronik seperti komputer, smartphone, dan jaringan internet, yang dapat digunakan sebagai alat bukti dalam proses peradilan (Mohamed et al., 2020). Bukti digital tidak hanya terkait dengan kasus-kasus yang melibatkan kejahatan siber, tetapi juga kejahatan konvensional yang semakin sering melibatkan teknologi digital, seperti pencurian, penipuan, dan perdagangan manusia (Rahman & Kurniawan, 2021).

Kepolisian di berbagai wilayah, termasuk Samarinda, menghadapi kebutuhan mendesak untuk mengelola bukti digital secara efektif dan efisien. Pengelolaan ini mencakup proses identifikasi, pengumpulan, penyimpanan, dan pemulihan data yang relevan dengan kasus kriminal (Zhang, 2020). Dalam konteks Kepolisian Samarinda, pengelolaan bukti digital ini memainkan peran penting dalam memastikan bahwa bukti tersebut dapat diterima di pengadilan dan tidak mengalami kerusakan atau modifikasi selama proses investigasi (Setiawan & Nurul, 2022). Hal ini menuntut peningkatan kemampuan teknis penyidik dalam menangani bukti digital, serta peningkatan perangkat dan infrastruktur teknologi yang mendukung proses investigasi tersebut.

Namun, pengelolaan bukti digital di Kepolisian Samarinda tidak terlepas dari tantangan, termasuk keterbatasan sumber daya manusia yang terlatih dalam *digital forensics* serta terbatasnya anggaran untuk pengadaan perangkat lunak dan perangkat keras yang mendukung proses tersebut (Widodo & Saputra, 2022). Selain itu, aspek hukum terkait bukti digital juga masih perlu diperjelas, terutama dalam hal regulasi tentang privasi data dan tata cara penggunaan bukti digital di pengadilan (Hartanto, 2021). Hal ini

menunjukkan bahwa tantangan teknis dan hukum dalam pengelolaan bukti digital di Kepolisian Samarinda memerlukan perhatian yang serius dan solutif.

Pengelolaan bukti digital merupakan bagian dari proses forensik digital, yang mencakup berbagai tahapan mulai dari identifikasi hingga penyimpanan dan analisis bukti. Menurut Mohamed et al. (2020), *forensik digital* merupakan metode yang digunakan untuk mengumpulkan, menganalisis, dan menyimpan informasi elektronik yang dapat dijadikan sebagai bukti dalam pengadilan. Metode ini telah menjadi standar dalam banyak investigasi, terutama ketika teknologi memainkan peran penting dalam tindak pidana. Dalam konteks Kepolisian Samarinda, penerapan forensik digital telah membantu dalam menangani berbagai kasus kriminal yang melibatkan teknologi informasi (Rahman & Kurniawan, 2021).

Tantangan dalam pengelolaan bukti digital di Kepolisian Samarinda juga meliputi masalah teknis dan regulasi hukum. Berdasarkan penelitian Setiawan dan Nurul (2022), salah satu kendala utama dalam pengelolaan bukti digital adalah kurangnya pelatihan bagi penyidik dalam menggunakan perangkat lunak forensik yang dapat memproses bukti digital dengan standar yang dapat diterima di pengadilan. Selain itu, masalah integritas bukti digital juga menjadi perhatian utama. Sebagai contoh, bukti digital dapat dengan mudah dirusak atau dimodifikasi tanpa disadari jika tidak ada protokol yang tepat dalam pengelolaannya (Widodo & Saputra, 2022).

Menurut Hartanto (2021), regulasi terkait penggunaan bukti digital di Indonesia masih memerlukan penguatan, terutama dalam hal undang-undang yang mengatur tentang privasi data dan prosedur penggunaan data elektronik sebagai alat bukti di pengadilan. Di Kepolisian Samarinda, regulasi ini menjadi penting mengingat banyaknya kasus yang melibatkan data pribadi dalam bentuk digital, baik itu dalam kejahatan siber maupun kejahatan konvensional yang menggunakan perangkat digital sebagai sarana komunikasi. Oleh karena itu, kepastian hukum terkait penggunaan bukti digital sangat diperlukan untuk menghindari konflik dalam proses penegakan hukum.

Untuk mengatasi berbagai tantangan tersebut, penelitian yang dilakukan oleh Zhang (2020) menunjukkan bahwa kolaborasi antara kepolisian dengan sektor swasta, seperti penyedia layanan teknologi dan ahli *forensik digital*, dapat menjadi solusi yang efektif. Peningkatan investasi dalam pelatihan sumber daya manusia serta pengadaan perangkat forensik yang lebih mutakhir akan meningkatkan kemampuan Kepolisian Samarinda dalam mengelola bukti digital secara optimal. Selain itu, penyesuaian regulasi yang lebih jelas dan tegas terkait bukti digital juga akan memberikan kerangka kerja yang lebih baik bagi para penyidik dalam menjalankan tugasnya.

Pengelolaan bukti digital dalam investigasi kriminal memiliki peran strategis di tengah meningkatnya kejahatan yang melibatkan teknologi digital. Menurut Yulianto dan Prasetyo (2021), pengelolaan bukti digital harus dilakukan secara hati-hati dan sesuai dengan standar internasional untuk menjaga integritas bukti tersebut. Misalnya, dalam kasus pencurian identitas atau penipuan daring, data yang diperoleh dari perangkat pelaku atau server dapat digunakan sebagai bukti forensik yang penting untuk dihadirkan di pengadilan. Di Kepolisian Samarinda, penerapan standar tersebut masih dalam tahap pengembangan, meskipun sudah ada beberapa penyidik yang dilatih secara khusus untuk menangani bukti digital (Wahyuni, 2022).

Tantangan lain yang dihadapi dalam pengelolaan bukti digital adalah masalah teknis terkait kompatibilitas perangkat lunak forensik dengan berbagai perangkat elektronik yang berbeda. Sebagaimana diungkapkan oleh Pratama (2021), perangkat lunak yang digunakan untuk memproses bukti digital sering kali tidak dapat mengakses data tertentu jika perangkat tersebut menggunakan sistem operasi atau teknologi keamanan yang berbeda. Misalnya, enkripsi pada perangkat smartphone modern menjadi tantangan tersendiri bagi penyidik untuk membuka dan mendapatkan data yang relevan. Ini menunjukkan bahwa pengelolaan bukti digital membutuhkan perangkat lunak yang fleksibel dan terintegrasi untuk memastikan data yang diperlukan dapat diakses dengan mudah, tanpa melanggar aturan privasi yang berlaku.

Di sisi lain, aspek hukum pengelolaan bukti digital di Indonesia, termasuk di Samarinda, masih menjadi topik yang perlu diperjelas. Menurut Saragih (2021), undang-undang terkait cybercrime dan penggunaan bukti digital di Indonesia masih relatif baru dan belum sepenuhnya teruji dalam kasus-kasus besar. Banyak perdebatan muncul terkait validitas bukti digital di pengadilan, terutama terkait dengan manipulasi atau pemalsuan data elektronik yang sulit dilacak jika tidak menggunakan teknologi yang canggih. Dalam beberapa kasus, bukti digital ditolak di pengadilan karena dianggap tidak memenuhi syarat-

syarat hukum yang berlaku di Indonesia, seperti tidak adanya prosedur yang jelas dalam proses pengumpulan bukti (Rahmawati & Hidayat, 202).

Hal ini semakin memperkuat urgensi untuk membangun kerangka hukum yang lebih kuat dan jelas dalam mengelola bukti digital. Widodo (2022) menegaskan bahwa regulasi yang mengatur privasi data dan prosedur pengumpulan bukti digital harus segera diperbarui agar sejalan dengan perkembangan teknologi dan kebutuhan investigasi kriminal modern. Di Kepolisian Samarinda, masalah ini menjadi fokus utama, terutama dalam menghadapi kasus-kasus yang semakin kompleks dan melibatkan banyak pihak yang berada di luar yurisdiksi hukum setempat. Dengan demikian, diperlukan regulasi yang tidak hanya berlaku secara lokal, tetapi juga memiliki daya jangkau yang lebih luas dalam menghadapi kejahatan lintas negara yang sering kali menggunakan teknologi sebagai alat utama.

Selain itu, penguatan kerjasama dengan sektor swasta dan lembaga internasional juga sangat diperlukan untuk meningkatkan kapasitas pengelolaan bukti digital di Indonesia. Berdasarkan penelitian Maulana (2023), kepolisian di negara-negara maju sudah mulai menerapkan kolaborasi dengan perusahaan teknologi untuk membantu memecahkan kasus-kasus yang melibatkan bukti digital. Kolaborasi ini memungkinkan penggunaan teknologi terbaru dalam memproses bukti digital, seperti analisis data besar (*big data analytics*) dan penggunaan kecerdasan buatan (*artificial intelligence*) untuk mempercepat proses investigasi.

Dengan kolaborasi semacam ini, Kepolisian Samarinda diharapkan dapat memanfaatkan teknologi terbaru untuk meningkatkan efektivitas penanganan kasus kriminal yang melibatkan bukti digital. Selain itu, peningkatan pelatihan dan pengadaan perangkat teknologi yang lebih canggih juga menjadi salah satu kunci keberhasilan dalam mengelola bukti digital secara optimal (Hasan, 2023). Tidak hanya itu, penyidik juga harus memahami prosedur hukum yang berlaku untuk memastikan bahwa bukti yang diperoleh melalui metode digital dapat diterima di pengadilan tanpa menimbulkan masalah hukum.

Berbagai penelitian sebelumnya telah mengangkat isu seputar pengelolaan bukti digital dalam konteks penegakan hukum. Penelitian terdahulu yang dilakukan oleh Zhang (2020) menyoroti pentingnya manajemen bukti digital dalam era *digital forensics*, terutama dalam kaitannya dengan kebutuhan standarisasi prosedur yang digunakan oleh aparat penegak hukum di berbagai negara. Zhang menjelaskan bahwa proses identifikasi, pengumpulan, dan analisis bukti digital perlu dilakukan secara sistematis dengan protokol yang ketat agar integritas bukti tetap terjaga sejak awal hingga tahap persidangan. Ia juga menekankan bahwa tanpa standarisasi dan panduan yang jelas, kemungkinan besar bukti digital akan diragukan keabsahannya di hadapan hukum, terutama ketika terjadi perbedaan sistem hukum antarnegara. Dalam konteks tersebut, Zhang mendorong adanya kolaborasi lintas negara untuk membangun kerangka hukum dan teknologi yang saling mendukung dalam penanganan kejahatan berbasis teknologi.

Selanjutnya, Rahman dan Kurniawan (2021) melalui penelitiannya mengangkat isu maraknya kejahatan siber di Indonesia dan pentingnya bukti digital sebagai alat pembuktian utama dalam kasus-kasus tersebut. Mereka memaparkan bahwa data dari media sosial, riwayat perpesanan elektronik, hingga aktivitas pengguna di platform daring kini menjadi jejak digital yang sangat penting dalam pembuktian tindak pidana. Namun, mereka juga menekankan bahwa belum semua aparat penegak hukum di tingkat daerah mampu mengelola bukti digital secara maksimal karena keterbatasan teknis dan sumber daya. Studi ini menjadi pijakan penting dalam memahami transformasi alat bukti dari bentuk fisik ke digital dalam dunia hukum kontemporer.

Di sisi lain, Hartanto (2021) memfokuskan kajiannya pada aspek regulasi hukum terkait bukti digital di Indonesia. Dalam penelitiannya, ia mengungkapkan bahwa masih terdapat banyak celah hukum dalam Undang-Undang Informasi dan Transaksi Elektronik (UU ITE), khususnya terkait dengan standar prosedural pengumpulan dan penyimpanan bukti digital. Menurutnya, hal ini kerap kali menimbulkan kebingungan di kalangan penyidik, terlebih dalam menentukan batas antara penegakan hukum dan pelanggaran hak privasi individu. Hartanto pun menyarankan perlunya revisi dan harmonisasi regulasi agar tidak terjadi tumpang tindih hukum yang dapat merugikan proses peradilan.

Sementara itu, Widodo dan Saputra (2022) menyoroti tantangan teknis yang dihadapi aparat penegak hukum dalam menangani bukti digital, terutama di tingkat kepolisian daerah. Melalui penelitian lapangan, mereka menemukan bahwa banyak penyidik yang belum mendapatkan pelatihan khusus dalam bidang forensik digital, sehingga sering kali kesulitan dalam mengoperasikan perangkat lunak dan perangkat keras yang digunakan untuk analisis bukti digital. Mereka juga mencatat bahwa keterbatasan anggaran menjadi

kendala utama dalam pengadaan teknologi forensik mutakhir, yang sangat diperlukan dalam menangani kasus-kasus kejahatan berbasis teknologi tinggi.

Penelitian terakhir yang relevan datang dari Maulana (2023), yang menawarkan pendekatan solutif melalui kolaborasi antara institusi penegak hukum dan sektor swasta, khususnya perusahaan teknologi. Ia menjelaskan bahwa banyak negara maju telah mulai bekerja sama dengan penyedia layanan *cloud*, pengembang perangkat lunak forensik, serta analis data profesional untuk mempercepat dan menyempurnakan proses investigasi berbasis bukti digital. Menurut Maulana, Indonesia juga perlu mulai menjalin kemitraan strategis semacam ini, karena akan sangat membantu dalam menjawab tantangan keterbatasan sumber daya manusia maupun teknologi yang sering dialami institusi kepolisian di daerah.

Berbeda dari lima penelitian terdahulu yang lebih bersifat teoritis, umum, atau berskala nasional dan internasional, penelitian ini mengambil fokus yang lebih sempit namun mendalam, yakni pada proses pengelolaan bukti digital dalam konteks lokal Kepolisian Samarinda. Dengan pendekatan yuridis normatif yang dilengkapi data empiris dari wawancara langsung, penelitian ini tidak hanya membahas teori atau regulasi semata, tetapi juga menyentuh persoalan teknis dan prosedural yang benar-benar dihadapi oleh penyidik di lapangan. Kontribusi utama dari penelitian ini adalah usulan solusi yang bersifat kontekstual, realistis, dan aplikatif, seperti pelatihan berkelanjutan, pembaruan regulasi hukum, penguatan kolaborasi lintas sektor, serta peningkatan sistem keamanan digital secara lokal. Dengan pendekatan ini, penelitian menjadi lebih relevan dan responsif terhadap dinamika penegakan hukum di daerah-daerah yang sering kali belum tersentuh oleh kebijakan nasional.

Berdasarkan paparan diatas maka Rumusan Masalah dalam penelitian ini ialah sebagai berikut: 1. Bagaimana proses pengelolaan *bukti digital* dalam investigasi kriminal di Kepolisian Samarinda? Dan 2. Apa saja tantangan yang dihadapi dalam pengelolaan *bukti digital* di Kepolisian Samarinda, dan bagaimana solusi yang dapat diterapkan untuk mengatasinya?

Adapun Tujuan Penelitian ialah untuk: Menganalisis proses pengelolaan *bukti digital* dalam investigasi kriminal di Kepolisian Samarinda dan Mengidentifikasi tantangan dan solusi dalam pengelolaan *bukti digital* guna meningkatkan efektivitas investigasi kriminal di Kepolisian Samarinda.

METODE PENELITIAN

Metode penelitian yang digunakan dalam penelitian ini adalah pendekatan yuridis normatif, yaitu pendekatan yang mengkaji peraturan perundang-undangan, doktrin hukum, serta asas-asas hukum yang relevan dengan pengelolaan bukti digital dalam investigasi kriminal. Penelitian ini bertujuan untuk memahami sejauh mana norma hukum yang ada diterapkan dalam praktik di lapangan, khususnya oleh aparat penegak hukum.

Jenis data yang digunakan terdiri dari data sekunder dan data primer. Data sekunder diperoleh melalui studi kepustakaan, meliputi literatur berupa buku, jurnal ilmiah, dan peraturan perundang-undangan seperti Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (UU ITE) dan peraturan pelaksanaannya. Sementara itu, data primer diperoleh melalui wawancara mendalam dengan penyidik yang bertugas di Satuan Reserse Kriminal Polresta Samarinda, guna mendapatkan informasi empiris tentang praktik pengelolaan bukti digital dalam proses investigasi kriminal di tingkat kepolisian daerah.

Teknik analisis data yang digunakan adalah analisis deskriptif-analitis, yakni dengan mendeskripsikan fakta dan norma hukum yang ada, kemudian menganalisisnya secara sistematis untuk merumuskan kesimpulan serta rekomendasi yang dapat diterapkan guna mengatasi permasalahan yang ditemukan di lapangan.

HASIL DAN PEMBAHASAN

1. Proses Pengelolaan Bukti Digital dalam Investigasi Kriminal di Kepolisian Samarinda

Pengelolaan *bukti digital* dalam investigasi kriminal di Kepolisian Samarinda mencakup serangkaian tahapan yang dimulai dari identifikasi bukti, pengumpulan, penyimpanan, hingga analisis bukti tersebut.

Pengelolaan bukti digital ini sangat berbeda dengan bukti konvensional karena sifatnya yang elektronik dan rentan terhadap modifikasi, penghapusan, atau kerusakan. Oleh karena itu, proses pengelolaan harus dilakukan secara hati-hati untuk memastikan integritas bukti tetap terjaga selama penyelidikan dan proses peradilan (Hartanto, 2021).

Tahap pertama dalam pengelolaan bukti digital adalah identifikasi bukti digital, yang mencakup upaya untuk menemukan dan mengenali data elektronik yang relevan dengan kasus kriminal yang sedang diselidiki. Identifikasi ini dilakukan melalui berbagai alat dan metode yang sesuai dengan standar forensik digital. Menurut Prasetyo (2020), identifikasi bukti digital harus dilakukan dengan metode yang terstandarisasi untuk meminimalkan risiko hilangnya data atau modifikasi yang tidak disengaja. Pada tahap ini, penyidik di Kepolisian Samarinda bekerja sama dengan ahli forensik digital untuk menemukan data-data penting yang tersimpan di perangkat elektronik milik tersangka, seperti *smartphone*, komputer, atau server. Pada beberapa kasus, bukti digital dapat berupa pesan teks, email, riwayat panggilan, atau aktivitas media sosial yang berhubungan dengan tindakan kriminal.

Setelah bukti digital berhasil diidentifikasi, langkah berikutnya adalah pengumpulan bukti digital. Tahap ini melibatkan proses pengambilan data dari perangkat digital menggunakan perangkat lunak khusus yang dirancang untuk mengumpulkan bukti tanpa merusak integritas data. Menurut Widodo dan Saputra (2022), pengumpulan bukti digital harus dilakukan dengan hati-hati, mengingat bukti ini rentan terhadap kerusakan atau pengubahan jika tidak diproses dengan benar. Di Kepolisian Samarinda, perangkat lunak *forensik digital* digunakan untuk menyalin data yang relevan dari perangkat tersangka ke dalam media penyimpanan khusus, yang kemudian dapat dianalisis lebih lanjut. Setiap tindakan yang diambil selama proses pengumpulan bukti harus dicatat secara rinci untuk membuktikan bahwa bukti tersebut tetap utuh dan tidak dimanipulasi.

Penyimpanan bukti digital juga merupakan aspek penting dalam pengelolaan bukti di Kepolisian Samarinda. Bukti yang telah dikumpulkan harus disimpan dalam lingkungan yang aman dan terjamin agar tidak terjadi kerusakan, manipulasi, atau akses tidak sah. Menurut Maulana (2021), penyimpanan bukti digital membutuhkan infrastruktur yang memadai, seperti server yang memiliki keamanan tinggi dan sistem *backup* yang baik untuk mencegah hilangnya data. Di Kepolisian Samarinda, bukti digital disimpan dalam media penyimpanan yang terenkripsi dan disimpan di lokasi yang hanya dapat diakses oleh personel yang berwenang. Penyimpanan ini penting untuk memastikan bahwa bukti digital dapat dipresentasikan di pengadilan dalam kondisi yang sama seperti saat pertama kali dikumpulkan, sehingga kredibilitasnya sebagai alat bukti tidak diragukan.

Tahap terakhir dalam pengelolaan bukti digital adalah analisis bukti digital, yang melibatkan penyelidikan lebih lanjut terhadap data yang telah dikumpulkan untuk menemukan pola, informasi, atau hubungan yang dapat digunakan untuk membuktikan keterlibatan tersangka dalam tindakan kriminal. Prasetyo (2020) mengungkapkan bahwa analisis bukti digital harus dilakukan oleh ahli yang berkompeten dalam bidang forensik digital untuk memastikan bahwa informasi yang diperoleh akurat dan relevan dengan kasus. Di Kepolisian Samarinda, analisis bukti digital dilakukan oleh tim forensik yang terlatih menggunakan perangkat lunak analisis khusus yang dapat memproses data dalam jumlah besar dan mengidentifikasi bukti-bukti yang relevan, seperti file tersembunyi atau riwayat aktivitas digital yang telah dihapus.

Selain itu, integritas bukti digital menjadi perhatian utama dalam keseluruhan proses. Setiap tahap harus sesuai dengan prosedur yang ketat untuk memastikan bahwa bukti tersebut tidak rusak atau dimanipulasi selama proses investigasi. Hal ini sangat penting karena bukti yang tidak diolah sesuai prosedur yang tepat dapat dianggap tidak valid di pengadilan. Menurut Saragih (2021), setiap tindakan yang dilakukan terhadap bukti digital, mulai dari identifikasi hingga analisis, harus terdokumentasi dengan baik melalui catatan *log* yang menunjukkan siapa yang mengakses bukti tersebut, kapan, dan untuk tujuan apa. Ini memberikan *audit trail* yang lengkap dan memungkinkan bukti digital dipertanggungjawabkan di pengadilan.

Di Kepolisian Samarinda, tantangan utama dalam proses pengelolaan bukti digital adalah kurangnya sumber daya manusia yang terlatih secara khusus dalam bidang forensik digital serta keterbatasan perangkat teknologi yang dimiliki. Widodo dan Saputra (2022) menegaskan bahwa banyak penyidik yang masih belum terbiasa dengan teknik-teknik pengelolaan bukti digital yang kompleks, sehingga sering kali

diperlukan bantuan ahli eksternal untuk mengelola bukti tersebut. Selain itu, perangkat lunak dan perangkat keras yang digunakan untuk memproses bukti digital sering kali memerlukan biaya yang tidak sedikit, yang menjadi kendala dalam pengadaan teknologi forensik yang lebih mutakhir.

Oleh karena itu, ada kebutuhan mendesak untuk meningkatkan pelatihan dan kapasitas sumber daya manusia di Kepolisian Samarinda dalam bidang forensik digital. Hasan (2022) menekankan bahwa pelatihan intensif diperlukan untuk memastikan penyidik dapat menggunakan perangkat lunak forensik dengan benar dan efektif. Dengan demikian, investigasi kriminal yang melibatkan bukti digital dapat dilakukan dengan lebih cepat dan akurat, sehingga proses penegakan hukum dapat berjalan lebih lancar.

Di samping tantangan teknis dalam pengelolaan *bukti digital*, terdapat pula tantangan regulasi yang dihadapi oleh Kepolisian Samarinda. Meskipun Indonesia telah memiliki beberapa regulasi terkait dengan teknologi dan informasi, seperti Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (*UU ITE*), serta aturan turunannya, namun penerapan regulasi ini dalam konteks bukti digital masih belum sepenuhnya matang. Menurut Hartanto (2021), ada sejumlah celah dalam regulasi yang menyebabkan ketidakpastian hukum, terutama terkait dengan privasi data dan kewenangan penyidik dalam mengakses data pribadi dari perangkat digital tersangka. Regulasi yang ada belum secara komprehensif mengatur mengenai standar pengelolaan *bukti digital*, sehingga sering kali menimbulkan interpretasi yang berbeda-beda di tingkat penegak hukum.

Hal ini berdampak pada proses investigasi yang melibatkan *bukti digital*, di mana penyidik sering kali harus menghadapi tantangan hukum terkait penggunaan bukti yang berasal dari perangkat digital tersangka. Saragih (2021) menyoroti bahwa beberapa bukti digital ditolak di pengadilan karena tidak ada prosedur yang jelas tentang bagaimana bukti tersebut harus dikumpulkan dan disimpan. Di Kepolisian Samarinda, kasus-kasus yang melibatkan *cybercrime* atau kejahatan yang melibatkan teknologi modern memerlukan perhatian lebih terhadap bagaimana regulasi diterapkan secara konsisten. Penyidik harus memahami dengan baik aturan yang berlaku agar bukti yang dikumpulkan dapat digunakan secara sah di pengadilan.

Lebih jauh lagi, tantangan lintas yurisdiksi juga menjadi salah satu hambatan dalam pengelolaan *bukti digital*, terutama jika kejahatan yang diinvestigasi melibatkan pelaku atau data yang berada di luar wilayah hukum Indonesia. Rahmawati dan Hidayat (2022) menegaskan bahwa kejahatan siber sering kali melibatkan jaringan internasional yang mempersulit upaya pengumpulan bukti digital. Penyidik di Kepolisian Samarinda kerap kali membutuhkan kerja sama dengan pihak internasional, seperti penyedia layanan internet atau perusahaan teknologi yang beroperasi di luar negeri, untuk mendapatkan akses ke data yang relevan dengan kasus. Namun, proses ini sering kali memakan waktu lama dan terhambat oleh perbedaan hukum dan peraturan privasi antar negara.

Dalam konteks ini, kerjasama internasional dalam penegakan hukum menjadi semakin penting. Menurut Zhang (2020), beberapa negara maju telah membentuk kerangka kerja sama lintas batas untuk menangani kasus-kasus yang melibatkan *cybercrime* dan bukti digital. Indonesia, termasuk Kepolisian Samarinda, perlu lebih aktif dalam membangun kemitraan internasional untuk menangani kasus-kasus yang melibatkan bukti digital yang berada di luar yurisdiksi nasional. Dengan adanya kerja sama yang lebih erat, penyidik di lapangan dapat lebih cepat mendapatkan akses ke data yang diperlukan tanpa terhalang oleh batasan-batasan geografis atau regulasi yang berbeda.

Oleh karena itu, dalam menghadapi kompleksitas kejahatan yang semakin melibatkan teknologi digital, penting bagi Kepolisian Samarinda untuk memperkuat sistem pengelolaan bukti digital yang mereka miliki. Hasan (2023) mengusulkan bahwa selain peningkatan teknologi dan pelatihan, perlu juga ada pembaruan regulasi yang lebih adaptif terhadap perkembangan teknologi informasi. Hal ini akan membantu mengurangi ketidakpastian hukum yang sering kali menghambat proses investigasi dan memastikan bahwa bukti digital dapat diterima di pengadilan tanpa menimbulkan konflik hukum. Dengan demikian, efektivitas penegakan hukum yang melibatkan *bukti digital* dapat meningkat secara signifikan.

Secara keseluruhan, proses pengelolaan bukti digital di Kepolisian Samarinda melibatkan serangkaian tahapan yang harus dilakukan dengan prosedur ketat untuk memastikan bahwa bukti tetap utuh, dapat diandalkan, dan dapat diterima di pengadilan. Tantangan dalam pengelolaan bukti digital ini perlu segera diatasi melalui peningkatan pelatihan penyidik, investasi dalam teknologi yang lebih canggih, serta pembaruan regulasi yang sesuai dengan perkembangan teknologi saat ini.

2. Tantangan dalam Pengelolaan Bukti Digital di Kepolisian Samarinda dan Solusi yang Dapat Diterapkan

Pengelolaan *bukti digital* dalam investigasi kriminal di Kepolisian Samarinda tidak terlepas dari berbagai tantangan yang kompleks, baik dari segi teknis, hukum, maupun sumber daya manusia. Salah satu tantangan terbesar yang dihadapi adalah kurangnya sumber daya manusia yang terlatih dalam bidang *forensik digital*. Menurut Widodo dan Saputra (2022), meskipun beberapa penyidik di Kepolisian Samarinda telah mendapatkan pelatihan dasar mengenai pengelolaan bukti digital, masih ada kekurangan dalam hal pengetahuan mendalam mengenai metode *forensik digital* yang mutakhir. Hal ini menyebabkan kesulitan dalam mengidentifikasi, mengumpulkan, dan menganalisis bukti digital yang rumit, seperti data terenkripsi atau data yang telah dihapus.

Tantangan ini semakin diperburuk oleh kurangnya infrastruktur teknologi yang memadai. Untuk dapat memproses *bukti digital* secara efisien, penyidik membutuhkan perangkat lunak dan perangkat keras khusus yang dirancang untuk menangani data elektronik dengan standar keamanan yang tinggi. Menurut Pratama (2021), perangkat teknologi yang digunakan untuk pengelolaan bukti digital, seperti perangkat lunak *forensik* dan alat untuk mengekstrak data dari perangkat mobile, memerlukan investasi yang besar. Namun, keterbatasan anggaran sering kali menjadi penghambat bagi kepolisian daerah, termasuk di Samarinda, dalam mengakses teknologi terbaru yang dapat mendukung penyelidikan berbasis bukti digital.

Selain itu, aspek hukum terkait pengelolaan bukti digital juga menghadirkan tantangan tersendiri. Regulasi yang ada, seperti Undang-Undang Informasi dan Transaksi Elektronik (*UU ITE*), belum sepenuhnya mencakup prosedur teknis terkait pengelolaan dan penggunaan *bukti digital* dalam pengadilan. Menurut Hartanto (2021), celah dalam peraturan hukum ini sering kali menyebabkan penyidik menghadapi kesulitan dalam memastikan bukti digital diterima sebagai bukti yang sah di pengadilan. Hal ini terkait dengan prosedur pengumpulan bukti yang tidak selalu jelas diatur, terutama dalam hal pengambilan data pribadi tanpa melanggar hak privasi tersangka.

Lebih lanjut, tantangan keamanan dalam penyimpanan bukti digital juga menjadi perhatian. Bukti digital yang disimpan di perangkat penyimpanan elektronik rentan terhadap serangan *cyber* atau peretasan, yang dapat mengakibatkan hilangnya bukti atau manipulasi data. Maulana (2022) menekankan pentingnya sistem keamanan yang kuat untuk melindungi bukti digital dari akses tidak sah. Di Kepolisian Samarinda, masalah ini muncul karena keterbatasan infrastruktur teknologi dan keamanan siber yang masih perlu ditingkatkan. Sistem penyimpanan yang tidak dilengkapi dengan protokol keamanan yang ketat dapat menyebabkan bukti digital tidak bisa dipertahankan keasliannya, yang pada akhirnya dapat merugikan proses penyelidikan dan peradilan.

Untuk menghadapi tantangan-tantangan tersebut, ada beberapa solusi yang dapat diterapkan guna meningkatkan pengelolaan *bukti digital* di Kepolisian Samarinda. Solusi pertama adalah peningkatan pelatihan dan kapasitas sumber daya manusia. Menurut Hasan (2022), pelatihan yang lebih intensif dan mendalam perlu diberikan kepada para penyidik, terutama yang bertugas menangani kasus-kasus yang melibatkan *bukti digital*. Program pelatihan ini harus mencakup teknik *forensik digital* yang lebih mutakhir, seperti cara menangani data terenkripsi, pemulihan data yang telah dihapus, dan penggunaan perangkat lunak analisis *forensik* yang canggih. Dengan peningkatan keterampilan ini, penyidik akan lebih siap dalam menangani bukti digital secara efektif dan efisien.

Solusi kedua adalah investasi dalam teknologi yang lebih canggih. Menurut Rahmawati dan Hidayat (2022), kepolisian perlu mengalokasikan anggaran untuk pengadaan perangkat teknologi yang dapat mendukung pengelolaan bukti digital dengan standar yang tinggi. Perangkat lunak forensik yang canggih, server dengan tingkat keamanan tinggi, serta sistem penyimpanan yang terenkripsi adalah beberapa contoh teknologi yang dapat meningkatkan kualitas investigasi kriminal berbasis bukti digital. Penggunaan teknologi ini tidak hanya mempercepat proses investigasi, tetapi juga menjamin bahwa bukti digital yang diperoleh dan disimpan tetap aman dan dapat diandalkan di pengadilan.

Selanjutnya, penguatan regulasi hukum juga menjadi solusi penting untuk mengatasi tantangan hukum terkait bukti digital. Menurut Saragih (2021), perlu ada revisi atau pembaruan dalam Undang-Undang ITE dan peraturan turunannya, terutama yang terkait dengan prosedur teknis dalam pengumpulan, penyimpanan, dan analisis bukti digital. Regulasi yang lebih jelas akan membantu penyidik untuk

beroperasi dalam batas-batas hukum yang tepat, sehingga tidak ada kebingungan mengenai apa yang diperbolehkan dan apa yang tidak dalam hal pengelolaan bukti digital. Pembaruan regulasi ini juga akan memberikan kepastian hukum yang lebih baik, baik bagi penyidik maupun bagi pengadilan dalam memutuskan kasus-kasus yang melibatkan bukti digital.

Terakhir, solusi yang dapat diterapkan adalah peningkatan keamanan siber di Kepolisian Samarinda. Mengingat risiko yang tinggi terhadap manipulasi atau pencurian bukti digital, Widodo (2022) menyarankan bahwa investasi dalam sistem keamanan siber yang lebih kuat sangat diperlukan. Penggunaan enkripsi pada semua tahap pengelolaan bukti, mulai dari pengumpulan hingga penyimpanan, dapat memastikan bahwa bukti digital tetap utuh dan terlindungi dari ancaman eksternal. Selain itu, sistem *backup* yang otomatis dan aman perlu diterapkan untuk menghindari hilangnya data dalam situasi darurat, seperti kerusakan perangkat keras atau serangan siber.

Selain tantangan-tantangan teknis, hukum, dan sumber daya yang telah dibahas sebelumnya, Kepolisian Samarinda juga menghadapi tantangan keterbatasan kerja sama lintas sektor dan lintas negara dalam menangani kasus-kasus yang melibatkan *bukti digital*. Kejahatan siber sering kali melibatkan aktor atau data yang berada di luar yurisdiksi nasional, sehingga pengelolaan bukti digital menjadi lebih kompleks. Menurut Zhang (2021), kolaborasi internasional antara lembaga penegak hukum sangat penting untuk mempercepat proses pengumpulan dan validasi bukti digital, terutama jika data yang dibutuhkan tersimpan di luar negeri. Namun, proses birokrasi dan perbedaan hukum antarnegara sering menjadi hambatan yang memperlambat investigasi.

Untuk mengatasi tantangan ini, salah satu solusi yang dapat diterapkan adalah membangun kemitraan strategis dengan penyedia layanan teknologi dan lembaga penegak hukum internasional. Maulana (2023) menekankan bahwa kerjasama dengan perusahaan teknologi global, seperti penyedia layanan internet, media sosial, dan platform e-commerce, akan memudahkan akses terhadap data yang relevan dengan investigasi. Di sisi lain, kerjasama lintas negara dengan lembaga seperti Interpol atau Europol juga dapat mempercepat pertukaran informasi dan bukti antarnegara. Dengan adanya kerangka kerjasama yang baik, Kepolisian Samarinda dapat mengatasi keterbatasan wilayah dan mendapatkan bukti digital yang berada di luar yurisdiksi mereka.

Di samping itu, Hasan (2023) juga menyarankan bahwa Indonesia, termasuk Kepolisian Samarinda, harus terlibat lebih aktif dalam forum-forum internasional terkait kejahatan siber dan *cyber forensics*. Partisipasi dalam forum tersebut memungkinkan pertukaran pengetahuan, teknologi, dan strategi investigasi terkini yang dapat diterapkan dalam konteks lokal. Selain itu, hal ini juga dapat membantu memperkuat sistem hukum nasional terkait *cybercrime* dan *forensik digital* agar lebih responsif terhadap perkembangan teknologi global.

Lebih jauh lagi, pengembangan pusat keunggulan forensik digital di tingkat regional atau nasional juga merupakan solusi yang dapat meningkatkan kapasitas Kepolisian Samarinda dalam mengelola bukti digital. Pusat ini dapat berfungsi sebagai tempat pelatihan dan pengembangan teknologi terbaru dalam *digital forensics*, serta menjadi sumber daya yang dapat diakses oleh berbagai institusi penegak hukum di Indonesia. Menurut Pratama (2021), pusat keunggulan ini juga dapat berperan sebagai tempat penelitian dan inovasi yang berfokus pada tantangan-tantangan lokal dalam pengelolaan bukti digital, sehingga solusi yang dikembangkan lebih sesuai dengan kebutuhan di lapangan.

Dengan menerapkan solusi-solusi ini, Kepolisian Samarinda tidak hanya dapat meningkatkan pengelolaan bukti digital di tingkat lokal, tetapi juga mampu beradaptasi dengan dinamika global dalam penegakan hukum yang melibatkan teknologi digital. Penguatan kerjasama internasional, peningkatan kapasitas teknologi, dan inovasi lokal dalam *forensik digital* akan menjadi kunci keberhasilan dalam menghadapi tantangan yang terus berkembang di era digital.

SIMPULAN DAN SARAN

Kesimpulan

Berdasarkan Hasil penelitian bahwa Pengelolaan bukti digital dalam investigasi kriminal di Kepolisian Samarinda melibatkan serangkaian tahapan yang sangat penting, yaitu identifikasi, pengumpulan, penyimpanan, dan analisis. Setiap tahapan memerlukan prosedur yang ketat untuk menjaga integritas bukti digital agar tetap sah dan dapat dipertanggungjawabkan di pengadilan. Proses pengelolaan ini berbeda dengan bukti konvensional karena sifat bukti digital yang rentan terhadap kerusakan,

modifikasi, atau penghapusan. Oleh karena itu, Kepolisian Samarinda menghadapi tantangan besar dalam memastikan bahwa bukti yang dikelola tetap dapat digunakan sebagai alat pembuktian yang valid.

Kemudian Tantangan utama yang dihadapi dalam pengelolaan bukti digital di Kepolisian Samarinda meliputi kurangnya sumber daya manusia yang terlatih dalam forensik digital, terbatasnya anggaran untuk perangkat teknologi yang diperlukan, serta ketidakjelasan regulasi hukum terkait bukti digital. Tanpa sumber daya yang memadai dan regulasi yang kuat, bukti digital yang dikumpulkan berisiko tidak dapat diterima di pengadilan. Oleh karena itu, peningkatan keterampilan penyidik dan revisi regulasi sangat dibutuhkan untuk memastikan proses penegakan hukum yang melibatkan bukti digital dapat berjalan lebih efektif dan sesuai dengan hukum yang berlaku.

Saran

Untuk meningkatkan efektivitas pengelolaan bukti digital, diperlukan peningkatan pelatihan dan pengembangan kemampuan teknis penyidik dalam bidang forensik digital. Kolaborasi dengan pihak swasta dan penyedia teknologi dapat mempercepat pengadaan perangkat yang diperlukan untuk investigasi berbasis teknologi. Selain itu, regulasi terkait bukti digital perlu diperbarui dan disesuaikan dengan perkembangan teknologi untuk memastikan bukti digital dapat digunakan secara sah di pengadilan. Implementasi sistem keamanan siber yang lebih baik juga harus diprioritaskan untuk melindungi bukti digital dari risiko kerusakan atau manipulasi.

DAFTAR PUSTAKA

Buku:

Hartanto, D. (2021). *Bukti digital dan regulasi hukum di Indonesia*. Jakarta: Pustaka Ilmu.

Maulana, A. (2023). *Penguatan sistem keamanan dalam investigasi kriminal berbasis teknologi*. Bandung: Media Nusa.

Mohamed, R., et al. (2020). *Forensik digital dalam investigasi kriminal*. Yogyakarta: Laksana.

Pratama, F. (2021). *Perkembangan teknologi forensik digital dalam penegakan hukum*. Surabaya: Surya Jaya.

Saragih, R. (2021). *Cybercrime dan penegakan hukum: Bukti digital dalam konteks hukum Indonesia*. Jakarta: Pustaka Persada.

Setiawan, T., & Nurul, H. (2022). *Tantangan forensik digital di Indonesia*. Malang: UB Press.

Widodo, S., & Saputra, A. (2022). *Teknologi forensik digital dan implementasinya dalam investigasi kriminal*. Jakarta: Gramedia Pustaka Utama.

Zhang, L. (2020). *Manajemen bukti digital dalam era digital forensik*. Beijing: TechPress.

Jurnal:

Hasan, M. (2023). Penguatan regulasi dalam pengelolaan bukti digital. *Jurnal Hukum dan Teknologi*, 12(2), 110-120.

Hartanto, D. (2021). Tantangan regulasi bukti digital di Indonesia. *Jurnal Hukum Digital*, 8(1), 102-105.

Prasetyo, R. (2020). Penggunaan forensik digital dalam penegakan hukum. *Jurnal Teknologi Informasi dan Hukum*, 5(3), 45-48.

Rahman, S., & Kurniawan, A. (2021). Investigasi bukti digital dalam kejahatan siber. *Jurnal Kriminalitas Siber*, 6(2), 78-85.

Rahmawati, E., & Hidayat, A. (2022). Investigasi kriminal berbasis bukti digital: Solusi dan tantangan. *Jurnal Kriminalitas Digital*, 10(4), 120-123.

Wahyuni, R. (2022). Pengelolaan bukti digital dalam investigasi forensik. *Jurnal Forensik dan Teknologi*, 7(3), 88-90.

Widodo, S. (2022). Regulasi bukti digital di pengadilan: Studi kasus di Kepolisian Samarinda. *Jurnal Hukum dan Forensik*, 9(2), 95-97.

Yulianto, D., & Prasetyo, A. (2021). Standar internasional dalam pengelolaan bukti digital. *Jurnal Kriminal Internasional*, 7(1), 73-75.

Zhang, L. (2021). Kolaborasi internasional dalam investigasi berbasis bukti digital. *Jurnal Kriminalitas Global*, 10(3), 54-85.