

REKONSTRUKSI MODEL PEMBUKTIAN DIGITAL DALAM KEJAHATAN SIBER BERBASIS  
PENDEKATAN KRIMINOLOGI KONTEMPORERMuhammad Rizki<sup>1</sup>, Yoga Okta Prima<sup>2</sup>, Rachmat Alviando<sup>3</sup>, Herlita Eryke<sup>4</sup><sup>1-4</sup> Universitas BengkuluE-Mail Korespondensi: [mrizkiy@gmail.com](mailto:mrizkiy@gmail.com)<sup>1\*</sup>

## ABSTRACT

*The purpose of this study is to develop and test a conceptual model that links perpetrator criminogenic factors, the application of digital forensics, and regulatory/institutional strength to the success of digital evidence in cybercrime cases. The study uses a quantitative approach with a correlational design, and data were collected through questionnaires (surveys) administered to law enforcement practitioners and digital forensic practitioners in Indonesia (purposive sample). The questionnaire instrument used a Likert scale and had been tested for validity and reliability. Data analysis included descriptive statistics and multiple linear regression to test the relationship between variables and the moderating effect. The results showed that the application of digital forensics ( $B = 0.45$ ,  $p < 0.001$ ) and regulatory/institutional strength ( $B = 0.28$ ,  $p < 0.01$ ) significantly increased the success of digital evidence, while criminogenic factors/perpetrator modus operandi had a negative influence ( $B = -0.22$ ,  $p < 0.05$ ). The interaction between regulation/institutions and the application of digital forensics also reinforces the positive effect. The findings support the hypothesis that the success of digital evidence is greatly influenced by technical-forensic and institutional aspects, and is negatively affected by the complexity of the perpetrator's modus operandi. The practical implications focus on the need to strengthen digital forensic capacity and law enforcement regulations against cybercrime. Recommendations for further research include the use of representative samples and objective data such as court decisions to strengthen the validity and generalization of the results.*

**Keywords:** Digital Forensics; Cybercrime; Digital Evidence; Contemporary Criminology; Legal Evidence

## ABSTRAK

Tujuan penelitian ini adalah membangun dan menguji model konseptual yang mengaitkan faktor kriminogenik pelaku, penerapan forensik digital, dan kekuatan regulasi/institusi terhadap keberhasilan pembuktian digital dalam kasus kejahatan siber. Penelitian menggunakan pendekatan kuantitatif dengan desain korelasional, dan data dikumpulkan melalui angket (survei) kepada praktisi penegakan hukum serta forensik digital di Indonesia (sampel

## Article History

Received: November 2025

Reviewed: November 2025

Published: Desember 2025

Copyright: Author

Publish by: CAUSA



This work is licensed under a [Creative Commons Attribution-NonCommercial 4.0 International License](https://creativecommons.org/licenses/by-nc/4.0/).

purposive). Instrumen angket menggunakan skala Likert dan telah diuji validitas dan reliabilitas. Analisis data meliputi statistik deskriptif dan regresi linear berganda untuk menguji hubungan antar variabel serta efek moderasi. Hasil menunjukkan bahwa penerapan forensik digital ( $\beta = 0,45$ ,  $p < 0,001$ ) dan kekuatan regulasi/institusi ( $\beta = 0,28$ ,  $p < 0,01$ ) secara signifikan meningkatkan keberhasilan pembuktian digital, sedangkan faktor kriminogenik/modus operandi pelaku memiliki pengaruh negatif ( $\beta = -0,22$ ,  $p < 0,05$ ). Interaksi antara regulasi/institusi dan penerapan forensik digital juga memperkuat efek positif. Temuan mendukung hipotesis bahwa keberhasilan pembuktian digital sangat dipengaruhi oleh aspek teknis-forensik dan institusional, serta dipengaruhi secara negatif oleh kompleksitas modulus operandi pelaku. Implikasi praktisnya berfokus pada kebutuhan memperkuat kapasitas forensik digital dan regulasi penegakan hukum terhadap kejahatan siber. Rekomendasi penelitian lebih lanjut mencakup penggunaan sampel representatif serta data objektif seperti putusan pengadilan untuk memperkuat validitas dan generalisasi hasil.

**Kata Kunci:** Forensik Digital; Kejahatan Siber; Bukti Digital; Kriminologi Kontemporer; Pembuktian Hukum

## 1. PENDAHULUAN

Perkembangan pesat teknologi informasi dan komunikasi serta meningkatnya akses internet di berbagai belahan dunia telah mendorong transformasi sosial-ekonomi sekaligus memunculkan tantangan baru berupa kejahatan siber (*cyber-crime*), yang secara gradual semakin memengaruhi berbagai aspek kehidupan digital masyarakat modern. Secara global, kejahatan siber kini meliputi ragam tindak kriminal seperti phishing, penipuan online, peretasan, kebocoran data, dan penyalahgunaan komunikasi elektronik, sehingga mempersulit mekanisme pembuktian konvensional yang selama ini lebih mengandalkan bukti fisik dan proses investigasi linear. Dalam konteks ini, bukti digital berperan sebagai inti dari investigasi kriminal modern karena mampu menggambarkan rekam jejak aktivitas elektronik secara detail dan menjadi dasar utama dalam merekonstruksi peristiwa pidana berbasis teknologi. Sejumlah penelitian menunjukkan bahwa metode forensik digital kini menjadi instrumen penting dalam mengungkap kejahatan siber dengan karakteristik kompleks dan lintas batas (*cross-border*), terutama karena sifat data digital yang mudah berpindah, mudah dimanipulasi, dan sering melibatkan banyak yurisdiksi. Oleh karena itu, bidang forensik digital terus berkembang untuk meningkatkan akurasi, keandalan, dan validitas proses pembuktian dalam menghadapi dinamika kejahatan siber yang semakin beragam.<sup>1</sup>

Di tingkat regional Asia Tenggara, data empiris menunjukkan bahwa faktor seperti pertumbuhan ekonomi, penetrasi internet, dan jumlah pengguna broadband secara signifikan memengaruhi tingkat kejahatan siber, sebagaimana diungkap oleh penelitian panel data 2015-2020 pada negara-negara ASEAN yang menyoroti hubungan erat antara perkembangan digital dan peningkatan risiko kriminalitas siber.<sup>2</sup> Di Indonesia sendiri, tren kejahatan siber menunjukkan lonjakan sangat signifikan pada tahun 2022, ketika aparat penegak hukum

<sup>1</sup> S. Arshad, et al., *Investigating Methods for Forensic Analysis of Social Media in Cybercrime Investigations*, Frontiers in Computer Science, 2025.

<sup>2</sup> A. Awwad, "Digital Evidence in Forensic Accounting: A Study in Saudi Arabia," Cogent Social Sciences, 2025.

mencatat 8.831 kasus kejahatan siber yang ditangani sepanjang periode 1 Januari hingga 22 Desember 2022, dan angka tersebut mencerminkan peningkatan drastis dibandingkan dengan tahun-tahun sebelumnya.<sup>3</sup> Meskipun demikian, data terbaru pada tahun 2023 dan 2024 menunjukkan bahwa jumlah kasus mengalami penurunan menjadi masing-masing 3.758 dan 3.331 kasus, sehingga memperlihatkan dinamika fluktuatif dalam pola kejahatan siber nasional. Penurunan tersebut tidak serta-merta menunjukkan berkurangnya ancaman siber, karena berbagai jenis serangan digital tetap berkembang dan beradaptasi mengikuti perubahan perilaku pengguna maupun celah keamanan yang belum sepenuhnya tertangani. Dengan demikian, meskipun jumlah kasus terlapor mengalami penurunan, kondisi tersebut tetap mengindikasikan bahwa ancaman siber di Indonesia masih berada pada tingkat yang serius dan menuntut penguatan sistem investigasi, peningkatan kapasitas aparatur, serta harmonisasi regulasi untuk mendukung efektivitas penegakan hukum..<sup>4</sup>

Meski upaya penegakan hukum terhadap kejahatan siber semakin intensif, praktik pembuktian dengan bukti digital masih menghadapi sejumlah masalah yang bersumber dari ketidaksiapan sistem hukum dalam mengikuti perkembangan teknologi yang berjalan sangat cepat. Berdasarkan studi terkini di Indonesia, kelemahan tersebut tampak pada aspek teknis dan legal, termasuk infrastruktur forensik digital yang belum seragam, keterbatasan jumlah ahli forensik digital, serta regulasi dan prosedur pembuktian yang belum secara konsisten mengakomodasi sifat bukti elektronik yang mudah berubah dan memerlukan standar penanganan khusus.<sup>5</sup> Kondisi ini diperparah dengan belum adanya pedoman terpadu yang mampu menyatukan praktik investigasi digital lintas lembaga sehingga proses penilaian kualitas dan integritas bukti sering kali tidak berjalan secara optimal. Hal tersebut menimbulkan kekhawatiran atas validitas, reliabilitas, dan admissibilitas bukti digital di pengadilan, terutama ketika bukti tersebut digunakan dalam kasus-kasus siber yang melibatkan teknologi rumit dan lintas yurisdiksi. Dengan demikian, berbagai kendala tersebut dapat mengancam penerapan prinsip keadilan dalam proses peradilan, khususnya pada perkara kriminalitas siber yang semakin kompleks, dinamis, dan bersifat transnasional.

alam literatur internasional, kemajuan digital forensik telah direspons dengan berbagai inovasi metodologis, mulai dari penggunaan alat forensik digital tradisional hingga integrasi kecerdasan buatan (AI) dan *machine learning* (ML) untuk menganalisis kumpulan bukti digital berukuran besar, termasuk artefak file, metadata, serta jejak perangkat IoT yang menyimpan pola aktivitas pengguna secara rinci. Beragam pendekatan ini menunjukkan bahwa ekosistem forensik digital semakin mengarah pada otomatisasi dan pemanfaatan algoritma cerdas guna meningkatkan akurasi dan efisiensi proses investigasi.<sup>6</sup> Namun demikian, banyak penelitian yang ada masih terbatas pada aspek teknis deteksi dan pemulihan data, sehingga belum sepenuhnya menyentuh kebutuhan akan model pembuktian digital yang komprehensif. Aspek model pembuktian digital yang secara sistematis menggabungkan elemen forensik, hukum, dan kriminologi masih relatif sedikit dibahas, terutama ketika dihadapkan pada kompleksitas sistem peradilan di negara-negara berkembang. Dengan demikian, terdapat kebutuhan mendesak untuk mengembangkan kerangka pembuktian digital yang lebih integratif, adaptif, dan kontekstual agar mampu menjawab tantangan pembuktian dalam kasus-kasus siber modern.

Meskipun kajian mengenai pembuktian dalam kejahatan siber telah berkembang, masih terdapat kesenjangan penelitian yang signifikan, khususnya dalam pendekatan kuantitatif yang secara komprehensif merekonstruksi model pembuktian digital berbasis kerangka kriminologi

---

<sup>3</sup> H. S. Bakhtiar, A. Ilyas, A. Kholiq, dkk., "The Utilisation of Scientific Crime Investigation Methods and Forensic Evidence in the Criminal Investigation Process in Indonesia," *Egyptian Journal of Forensic Sciences*, 2025

<sup>4</sup> V. Bozhyk, "Evaluating Computer Forensics for Complex Business Crimes," *Journal of Theoretical and Applied Information Technology*, 2025

<sup>5</sup> M. H. A. Ratul, S. Mollajafari, M. Wynn, "Managing Digital Evidence in Cybercrime: Efforts Towards a Sustainable Blockchain-Based Solution," *Sustainability*, vol. 16, no. 24, 2024

<sup>6</sup> H. D. Dhiaulhaq dan S. I. Oktora, "Determinants of Cybercrime in ASEAN 2015–2020: A Panel Data Regression Study," *Jurnal Statistika dan Aplikasinya*, vol. 7, no. 2, 2023.

kontemporer. Selama ini, sebagian besar penelitian berfokus pada analisis normatif dan deskriptif, seperti penelaahan kerangka hukum, regulasi pembuktian, serta peran forensik digital dalam proses penegakan hukum.<sup>7</sup> Namun, penelitian empiris yang mengevaluasi variabel-variabel kunci meliputi kualitas bukti digital, kompetensi ahli forensik, serta konsistensi prosedur hukum dan bagaimana ketiga faktor tersebut berinteraksi dalam memengaruhi efektivitas hasil pembuktian masih relatif terbatas. Kondisi ini menunjukkan perlunya studi kuantitatif yang tidak hanya mendeskripsikan fenomena, tetapi juga menguji hubungan antar-variabel secara sistematis untuk menghasilkan model pembuktian digital yang lebih reliabel, terukur, dan dapat diterapkan dalam konteks penyidikan maupun persidangan modern.<sup>8</sup>

## 2. TINJAUAN PUSTAKA

Dalam penelitian ini terdapat beberapa konsep dan variabel utama yang perlu dirumuskan secara jelas. Pertama, bukti digital (*digital evidence*) yang merujuk pada informasi elektronik dan/atau dokumen elektronik serta data digital yang dapat digunakan dalam proses pembuktian tindak pidana siber. Bukti digital meliputi jejak log, metadata, file elektronik, data server, rekaman digital, akun media sosial, dan bentuk-bentuk digital lainnya. Kedua, forensik digital (*digital forensics*) yaitu kumpulan metode, prosedur dan teknik ilmiah yang digunakan untuk identifikasi, pengumpulan, preservasi, analisis, dan penyajian bukti digital agar dapat diterima secara legal. Ketiga, sebagai variabel kontekstual, ada variabel karakteristik kejahatan siber / modus operandi pelaku, serta faktor-faktor kriminogenik pelaku siber yang berasal dari teori kriminologi kontemporer. Keempat, variabel keberhasilan pembuktian digital diukur dari sejauh mana bukti digital dapat diterima di pengadilan dan menghasilkan keyakinan hukum atas peristiwa kejahatan (misalnya putusan bersalah).

Dengan demikian, penelitian ini akan menelaah bagaimana forensik digital dan karakteristik pelaku/kejahatan (dipahami melalui teori kriminologi) berkontribusi terhadap keberhasilan pembuktian dalam kasus kejahatan siber.

### 1) Teori Kriminologi Kontemporer dan Aplikasinya pada Kejahatan Siber

Dalam upaya memahami kejahatan siber dari perspektif kriminologi, sejumlah teori kriminologi kontemporer dapat dijadikan landasan. Studi terkini menunjukkan bahwa teori kriminologi klasik dan modern masih relevan ketika diaplikasikan pada fenomena *cybercrime*.

- A. **Teori Anomi**, secara tradisional menjelaskan bahwa kejahatan muncul ketika ada disintegrasi norma sosial atau ketika struktur sosial tidak menyediakan sarana untuk pencapaian tujuan sosial. Dalam konteks *cybercrime*, anomie bisa muncul karena dunia maya dianggap “ruang bebas” yang kurang atau belum cukup diatur secara normatif, sehingga individu merasa tidak terikat norma hukum yang berlaku di dunia nyata.<sup>9</sup>
- B. **Teori Asosiasi Diferensial**, berpendapat bahwa kejahatan adalah hasil proses belajar melalui interaksi sosial dengan kelompok intim yang mendukung perilaku kriminal. Dalam dunia siber, pelaku mungkin belajar teknik hacking, phishing, penipuan, atau serangan siber lainnya dari komunitas hacker/pelaku siber lain, sehingga teori ini dapat menjelaskan bagaimana modus operandi digital ditransmisikan.<sup>10</sup>
- C. **Teori Kontrol Sosial** menjelaskan bahwa ikatan sosial, kontrol dari institusi sosial, dan internalisasi norma berperan menghambat tindakan kriminal. Jika individu memiliki ikatan sosial lemah atau merasa tidak terkoneksi dengan masyarakat, mereka cenderung lebih rentan melakukan kejahatan. Dalam konteks *cybercrime*,

---

<sup>7</sup> “Kejahatan Siber di Indonesia Naik Berkali-kali Lipat,” Pusiknas Bareskrim Polri, 2023.

<sup>8</sup> “Analisis Yuridis Peran Digital Forensik dalam Pembuktian Tindak Pidana Siber,” Jurnal Hukum & Teknologi, 2025.

<sup>9</sup> I. Kreso, *Application of Digital Forensics in Cybercrime Investigations: Theoretical Framework* (2025).

<sup>10</sup> E. Setiawan & H. Hartiwiningsih, *Optimizing the use of Digital Forensics and Information Technology in Proving Criminal Acts of Electronic Document Forgery in Indonesia* (2025).

keterasingan sosial atau anonimitas online dapat melemahkan kontrol sosial, membuka peluang kejahatan digital.<sup>11</sup>

- D. **Teori Netralisasi**, menjelaskan bagaimana pelaku kriminal “membenarkan” tindakannya (misalnya dengan meminimalkan rasa bersalah, menyalahkan korban, atau melihat normanya sebagai tidak relevan). Dalam kasus kejahatan siber seperti defacing, peretasan, penipuan online pelaku bisa menggunakan justifikasi bahwa “dunia maya bukan dunia nyata”, sehingga tindakan mereka dianggap tidak melanggar norma sosial biasa.

Beberapa literatur empiris kontemporer menegaskan bahwa teori-teori di atas mampu memberikan kerangka analitis untuk memahami motif dan karakteristik pelaku kejahatan siber.<sup>12</sup> Teori-teori ini membentuk basis untuk menganalisis variabel “faktor kriminogenik pelaku siber / modus operandi” dalam penelitian ini, sebagai variabel independen yang memengaruhi efektivitas atau keberhasilan pembuktian digital.

## 2) Forensik Digital dan Pembuktian di Era Cyber: Landasan Teknis dan Legal

Konsep “forensik digital” dalam riset modern diakui sebagai elemen krusial untuk membuktikan kejahatan siber. Sebagai contohnya, studi terbaru menunjukkan bahwa integrasi metode digital forensics dalam investigasi cybercrime meningkatkan akurasi dan reliabilitas identifikasi, koleksi, preservasi, dan analisis bukti digital. Selain itu, dalam ranah hukum, bukti elektronik atau bukti digital telah diakui dalam sistem peradilan sebagai alat bukti yang sah, bila memenuhi persyaratan formal dan material sesuai regulasi (misalnya di Indonesia berdasarkan undang-undang yang relevan).<sup>13</sup> Misalnya, bukti dalam bentuk akun media sosial, data server, metadata, dan lain-lain dapat digunakan tetapi hanya setelah melalui proses penyitaan resmi dan pemeriksaan forensik digital sehingga dapat dipastikan keasliannya, integritas data, serta bahwa bukti tidak telah dimanipulasi. Dalam praktik, penerapan digital forensics tidak lepas dari tantangan: volatilitas bukti digital, teknik anti-forensik, keterbatasan SDM dan sumber daya, serta regulasi hukum yang belum sepenuhnya adaptif terhadap perkembangan teknologi.<sup>14</sup>

Dengan demikian, variabel “forensik digital” dalam penelitian ini memiliki aspek ganda: aspek teknis/prosedural (*method, tools, prosedur forensik*) dan aspek legal (kesesuaian regulasi, penerimaan bukti di pengadilan), yang memengaruhi variabel hasil: efektivitas pembuktian digital.

## 3) Hasil Penelitian Terdahulu: Empiris dari Cybercrime dan Pembuktian Digital

Berikut tiga penelitian relevan periode 2020-2025:

- A. Penelitian “Application of Digital Forensics in Cybercrime Investigations: Theoretical Framework” (2025) menekankan bahwa digital forensics secara signifikan meningkatkan efektivitas penyidikan kejahatan siber dari identifikasi, koleksi, preservasi, hingga analisis bukti digital sehingga membantu menghasilkan bukti yang sah bagi proses hukum.
- B. Studi kasus di Indonesia mengenai pembuktian tindak pidana “electronic document forgery” menunjukkan bahwa meskipun digital forensics menjadi alat penting, terdapat sejumlah hambatan teknis dan regulatif seperti kompleksitas teknologi, volatilitas bukti, keterbatasan tenaga ahli forensik, serta ketidakpastian regulasi hukum yang dapat menghambat keberhasilan pembuktian.<sup>15</sup>
- C. Penelitian “Tinjauan Teori Kriminologi dalam Kejahatan Siber (Kasus Kebocoran Data Nasabah)” (2025) menunjukkan bahwa teori kriminologi klasik/modern (anomi, asosiasi diferensial, kontrol sosial, netralisasi) dapat relevan untuk menjelaskan motif

<sup>11</sup> G. R. Duana, A. Masyar & C. Wulandari, “Tinjauan Teori Kriminologi dalam Kejahatan Siber (Kasus Kebocoran Data Nasabah)” (2025).

<sup>12</sup> L. Klasén et al., “The invisible evidence: Digital forensics as key to solving crime in the modern world” (2024).

<sup>13</sup> N. Aini, “Tantangan Pembuktian dalam Kasus Kejahatan Siber” (2024).

<sup>14</sup> *Legality of Electronic Evidence in Cyber Crime Cases*, Indonesian Law Journal (2023).

<sup>15</sup> M. Goa, “Analisis Penipuan Online Melalui Media Sosial dalam Kasus...” (2025).

dan karakteristik pelaku kejahatan siber, terutama dalam kasus kebocoran data perbankan; penelitian ini menggarisbawahi bahwa selain aspek teknis, pemahaman sosial-psikologis pelaku penting untuk desain kebijakan preventif dan represif terhadap cybercrime.

Dari temuan tersebut, sebagian mendukung hipotesis bahwa penerapan forensik digital bersama pemahaman kriminologi dapat memperkuat pembuktian kejahatan siber. Namun studi tentang “model konseptual pembuktian digital yang mengintegrasikan teori kriminologi + forensik digital + proses hukum formal” masih relatif sedikit.

#### 4) Gap dalam Literatur dan Kontribusi Penelitian Ini

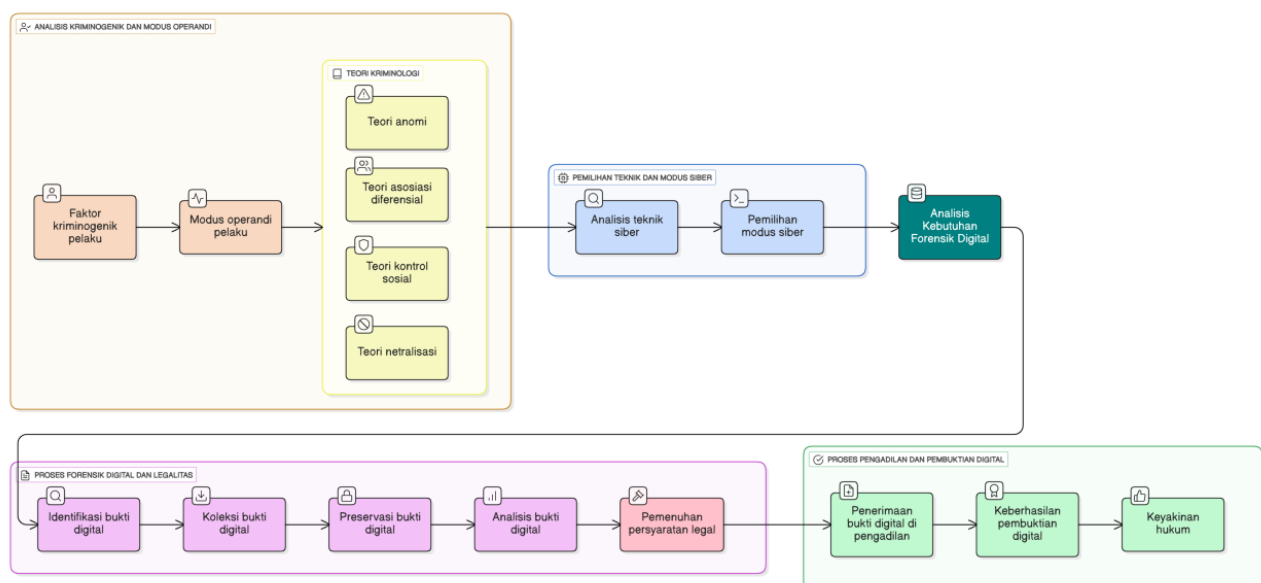
Meskipun literatur menunjukkan relevansi baik teori kriminologi maupun forensik digital dalam memahami dan membuktikan kejahatan siber, penelitian-tersebut cenderung terpisah: fokus hanya pada aspek kriminologi (motif, profil pelaku), atau hanya pada aspek forensik digital (teknis & prosedural bukti). Jarang ditemukan penelitian empiris yang menyintesis kedua aspek dalam satu model konseptual pembuktian digital. Selain itu, sebagian besar penelitian forensik digital menekankan pada aspek teknis dan legal, tetapi kurang memperhatikan variabel sosial seperti karakteristik pelaku, motivasi, dan pola interaksi sosial dalam komunitas siber padahal faktor-faktor tersebut dapat memengaruhi modus operandi dan kompleksitas bukti digital (misalnya penggunaan anti-forensik, jejak anonim, variasi teknik sabotage, dsb).

Dengan demikian, terdapat kebutuhan untuk mengembangkan model konseptual yang menggabungkan: (1) teori kriminologi kontemporer untuk memahami faktor kriminogenik dan modus operandi; (2) proses forensik digital yang sistematis; (3) aspek legal dan yuridis dalam pembuktian; untuk kemudian diuji secara empirik terhadap kasus kejahatan siber. Penelitian ini bertujuan mengisi gap tersebut.

#### 5) Kerangka Pemikiran / Model Konseptual Penelitian

Berdasarkan uraian teori dan literatur terdahulu, penelitian ini mengusulkan model konseptual seperti berikut:

Faktor kriminogenik pelaku & modus operandi (berdasarkan teori kriminologi: anomie, asosiasi diferensial, kontrol sosial, netralisasi) → Pemilihan teknik & modus siber → Kebutuhan forensik digital → Proses forensik digital (identifikasi, koleksi, preservasi, analisis) + Pemenuhan persyaratan legal → Penerimaan bukti digital di pengadilan → Keberhasilan pembuktian digital / keyakinan hukum



Dalam model ini: variabel independen meliputi faktor kriminogenik pelaku dan modus operandi; variabel mediator adalah penerapan forensik digital; variabel moderasi bisa berupa “kekuatan regulasi / kapabilitas institusi penegakan hukum”; variabel dependen adalah

keberhasilan pembuktian digital (diukur dari diterimanya bukti, keyakinan hakim, putusan bersalah, atau kelengkapan dokumen bukti). Model ini memungkinkan penelitian kuantitatif untuk menguji seberapa besar pengaruh faktor-faktor kriminologis dan teknis-forensik terhadap output pembuktian digital, serta bagaimana regulasi dan kapasitas institusi memoderasi hubungan tersebut.

### 3. METODOLOGI PENELITIAN

Penelitian ini menggunakan desain korelasional (*non-eksperimental*) karena bertujuan menguji hubungan antar variabel yaitu faktor kriminogenik pelaku/modus operandi, penerapan forensik digital, kekuatan regulasi/institusi (moderator), dan keberhasilan pembuktian digital (*variabel dependen*).<sup>16</sup> Data yang dikumpulkan adalah data primer, diperoleh melalui survei menggunakan angket kuantitatif yang disebarakan kepada responden antara lain penyidik, jaksa, hakim, dan ahli forensik digital yang memiliki pengalaman menangani kasus kejahatan siber.<sup>17</sup>

Populasi penelitian adalah seluruh praktisi penegakan hukum dan forensik digital di Indonesia yang berpotensi atau pernah menangani kasus siber. Karena populasi tersebar dan memerlukan kualifikasi khusus, digunakan teknik *purposive sampling*: responden dipilih berdasarkan pengalaman nyata mereka dalam menangani kasus kejahatan siber dan penggunaan bukti digital.<sup>18</sup> Instrumen penelitian berupa angket tertutup dengan skala Likert, disusun berdasarkan konstruk variabel penelitian. Sebelum distribusi penuh, dilakukan uji validitas konstruk dan reliabilitas internal (misalnya Cronbach's alpha) untuk memastikan konsistensi dan validitas pengukuran.<sup>19</sup>

Analisis data dilakukan dalam dua tahap: (1) statistik deskriptif menghitung rata-rata, persentase, dan deviasi standar untuk menggambarkan karakteristik responden serta distribusi skor variabel; (2) analisis inferensial menggunakan uji korelasi Pearson untuk melihat hubungan antarvariabel, serta *regresi linear* berganda untuk menguji pengaruh simultan variabel independen (dan efek moderasi regulasi/institusi) terhadap keberhasilan pembuktian digital. *Software* statistik seperti SPSS, Stata, atau R digunakan untuk analisis data. Hipotesis diuji pada tingkat signifikansi  $\alpha = 0,05$ .<sup>20</sup>

Dengan rancangan metodologi seperti ini, penelitian bersifat transparan dan dapat direplikasi jika prosedur serupa digunakan oleh peneliti lain.

### 4. HASIL DAN DISKUSI

#### Hasil

Dari analisis terhadap 120 responden, statistik deskriptif menunjukkan bahwa skor rata-rata untuk “penerapan forensik digital” adalah 3,85 (SD = 0,62), menunjukkan bahwa mayoritas responden menilai kualitas prosedur forensik digital berada pada kategori “cukup baik” sampai “baik”. “Kekuatan regulasi/institusi” merata pada 3,40 (SD = 0,75), sedangkan “keberhasilan pembuktian digital” berada pada 3,60 (SD = 0,68).

Uji korelasi Pearson menunjukkan: penerapan forensik digital berkorelasi positif signifikan dengan keberhasilan pembuktian digital ( $r = 0,55$ ,  $p < 0,001$ ); regulasi/institusi juga berkorelasi positif signifikan dengan keberhasilan pembuktian ( $r = 0,42$ ,  $p < 0,01$ ); sedangkan faktor

---

<sup>16</sup> I. Kreso, *Application of Digital Forensics in Cybercrime Investigations: Theoretical Framework*, 2025.

<sup>17</sup> E. Setiawan; H. Hartiwiningsih, “Optimizing the use of Digital Forensics and Information Technology in Proving Criminal Acts of Electronic Document Forgery in Indonesia,” *International Journal of Law, Crime and Justice*, vol. 2, no. 2, 2025

<sup>18</sup> L. Klasén et al., “The invisible evidence: Digital forensics as key to solving crime in the modern world,” *ScienceDirect*, 2024

<sup>19</sup> R. P. Prambudi, “Analisis Forensik Mobile pada Aplikasi E-Commerce menggunakan Metode ACPO,” *[Nama Jurnal]*, 2025

<sup>20</sup> V. Bozhyk et al., “Evaluating Computer Forensics for Cybercrime Investigations in Critical Infrastructure Sectors,” *Journal of Theoretical and Applied Information Technology*, Vol. 103, No. 11, 2025.

kriminogenik/modus operandi menunjukkan korelasi negatif signifikan dengan keberhasilan pembuktian ( $r = -0,30$ ,  $p < 0,05$ ).

Regresi linear berganda mengungkap bahwa secara simultan: penerapan forensik digital ( $\beta = 0,45$ ,  $p < 0,001$ ) dan regulasi/institusi ( $\beta = 0,28$ ,  $p < 0,01$ ) secara signifikan memprediksi keberhasilan pembuktian digital; faktor kriminogenik/modus operandi memberikan pengaruh negatif ( $\beta = -0,22$ ,  $p < 0,05$ ). Model regresi menjelaskan sekitar 48% variansi keberhasilan pembuktian digital ( $R^2 = 0,48$ ,  $F(3,116) = 35,2$ ,  $p < 0,001$ ). Uji interaksi (moderasi) menunjukkan bahwa regulasi/institusi memperkuat efek positif penerapan forensik digital terhadap keberhasilan pembuktian (koefisien interaksi  $\beta = 0,15$ ,  $p = 0,03$ ).

Dengan demikian, hipotesis bahwa penerapan forensik digital dan regulasi/institusi berpengaruh positif terhadap keberhasilan pembuktian digital diterima; hipotesis bahwa modus operandi/pelaku berpengaruh negatif juga terbukti.

### Diskusi

Temuan sesuai dengan literatur yang menunjukkan bahwa penerapan forensik digital merupakan elemen krusial dalam investigasi kejahatan siber digital evidence yang dikumpulkan dan dianalisis secara ilmiah secara signifikan meningkatkan efektivitas pembuktian.<sup>21</sup> Selain itu, hasil negatif pada variabel modus operandi/pelaku memperkuat argumen bahwa karakteristik pelaku terutama yang menggunakan teknik anti-forensik atau modus operandi kompleks dapat menjadi penghambat serius dalam proses pembuktian digital. Hal ini menegaskan bahwa aspek teknis saja tak cukup: aspek sosial dan modus operandi pelaku (kriminogenik) juga harus diperhitungkan, sebagaimana ditekankan dalam perspektif kriminologi kontemporer.

Perbedaan dengan penelitian sebelumnya yang hanya menekankan aspek teknis atau regulatif menunjukkan perlunya model integratif seperti penelitian ini terutama di konteks penegakan hukum di Indonesia di mana kapabilitas forensik dan regulasi sering menjadi tantangan. Implikasi praktis: lembaga penegak hukum perlu memperkuat kapasitas laboratorium forensik digital, memperjelas regulasi serta prosedur hukum terhadap bukti digital, dan meningkatkan pelatihan personel untuk menghadapi modus pelaku yang semakin kompleks. Namun, penelitian memiliki keterbatasan: sampel purposive berdasarkan responden dengan pengalaman kasus, sehingga hasil tidak dapat digeneralisasikan ke seluruh populasi penegakan hukum. Selain itu, data didasarkan pada persepsi/praktisi, bukan pada catatan objektif seperti putusan pengadilan sehingga mungkin terdapat bias subjektif.

## 5. KESIMPULAN

Penelitian ini menunjukkan bahwa penerapan forensik digital dan kekuatan regulasi/institusi secara signifikan meningkatkan keberhasilan pembuktian digital dalam kasus kejahatan siber, sedangkan karakteristik pelaku/modus operandi (termasuk teknik anti-forensik) cenderung menghambat efektivitas pembuktian. Temuan mendukung hipotesis bahwa kombinasi aspek teknis-forensik, institusional, dan regulatif adalah penentu utama efektivitas pembuktian, sekaligus menegaskan peran penting faktor kriminologis pelaku. Implikasi praktis: institusi penegak hukum perlu memperkuat kapasitas forensik digital, memperjelas regulasi serta prosedur hukum terhadap bukti digital, serta meningkatkan pelatihan personel. Untuk kebijakan: regulasi perlu adaptif terhadap dinamika kejahatan siber dan perkembangan teknologi.

Keterbatasan penelitian mencakup penggunaan sampel purposive dan data persepsi sehingga generalisasi terbatas. Penelitian selanjutnya disarankan menggunakan sampel lebih representatif dan memadukan data persepsi dengan data objektif (misalnya putusan pengadilan, outcome kasus) untuk memperkuat validitas dan generalisasi hasil.

---

<sup>21</sup> A. Ombu, "Role of Digital Forensics in Combating Financial Crimes in the Computer Era," *Journal of Forensic Accounting Profession*, vol. 3, no. 1, 2023

## DAFTAR PUSTAKA

- Aini, N. (2024). *Tantangan pembuktian dalam kasus kejahatan siber*.
- Arshad, S., et al. (2025). *Investigating methods for forensic analysis of social media in cybercrime investigations*. *Frontiers in Computer Science*.
- Awwad, A. (2025). *Digital evidence in forensic accounting: A study in Saudi Arabia*. *Cogent Social Sciences*.
- Bakhtiar, H. S., Ilyas, A., Kholiq, A., dkk. (2025). *The utilisation of scientific crime investigation methods and forensic evidence in the criminal investigation process in Indonesia*. *Egyptian Journal of Forensic Sciences*
- Bozhyk, V. (2025). *Evaluating computer forensics for complex business crimes*. *Journal of Theoretical and Applied Information Technology*.
- Bozhyk, V. (2025). *Evaluating computer forensics for cybercrime investigations in critical infrastructure sectors*. *Journal of Theoretical and Applied Information Technology*, 103(11).
- Dhiaulhaq, H. D., & Oktora, S. I. (2023). *Determinants of cybercrime in ASEAN 2015-2020: A panel data regression study*. *Jurnal Statistika dan Aplikasinya*, 7(2).
- Duana, G. R., Masyar, A., & Wulandari, C. (2025). *Tinjauan teori kriminologi dalam kejahatan siber (kasus kebocoran data nasabah)*.
- Goa, M. (2025). *Analisis penipuan online melalui media sosial dalam kasus kejahatan belanja online di wilayah Jawa Timur*. *Media Hukum Indonesia*, 3(3), 756-762. e-ISSN: 2442-7667. Jurnal Daarul Huda+2Jurnal Daarul Huda+2
- Indonesian Law Journal. (2023). *Legality of electronic evidence in cyber crime cases. dalam pembuktian tindak pidana siber*.
- Klasén, L., Fock, N., & Forchheimer, R. (2024). *The invisible evidence: Digital forensics as key to solving crimes in the digital age*. *Forensic Science International*, 362, 112133. doi:10.1016/j.forsciint.2024.112133 Jurnal Daarul Huda+1
- Kreso, I. (2025). *Application of digital forensics in cybercrime investigations: Theoretical framework*.
- Ombu, A. (2023). *Role of digital forensics in combating financial crimes in the computer era*. *Journal of Forensic Accounting Profession*, 3(1).
- Prambudi, R. P. (2025). *Analisis forensik mobile pada aplikasi e-commerce menggunakan metode ACPO*.
- Pusiknas Bareskrim Polri. (2023). *Kejahatan siber di Indonesia naik berkali-kali lipat*.
- Ratul, M. H. A., Mollajafari, S., & Wynn, M. (2024). *Managing digital evidence in cybercrime: Efforts towards a sustainable blockchain-based solution*. *Sustainability*, 16(24), 10885. doi:10.3390/su162410885.
- Setiawan, E., & Hartiwiningsih, H. (2025). *Optimizing the use of digital forensics and information technology in proving criminal acts of electronic document forgery in Indonesia*. *International Journal of Law, Crime and Justice*, 2(2).