

Forensik Data dalam Pembuktian Tindak Pidana Siber Analisis Jaringan Bukti Menggunakan *Social Network Analysis*

Sri Yulianingsih^{*1}, Methodius Kossay², Eni Endaryati³

^{1,2,3}Universitas Sains dan Teknologi Komputer, Semarang, Jawa Tengah, Indonesia.

E-mail: sriyulianingsih@stekom.ac.id*

Article Info	Abstract
Keywords: Data forensics, Cybercrime, Legal evidence, Social network analysis, Digital evidence.	<i>The increasing complexity of cybercrime requires more adaptive evidentiary approaches capable of addressing the dynamic and interconnected nature of digital evidence. This study aims to examine the role of data forensics in cybercrime proof through the integration of Social Network Analysis (SNA) as a network-based analytical approach. The research employs a mixed methods approach with an explanatory sequential design, combining quantitative analysis of 120 case files with qualitative insights obtained from in-depth interviews with prosecutors, investigators, and digital forensic experts. The findings reveal that digital evidence forms complex network structures, where entities with high centrality values play significant roles as key actors and intermediaries in cybercrime activities. The application of SNA enables a more objective identification of actors' involvement patterns and strengthens evidentiary construction by analyzing the interconnections among digital evidence. Theoretically, this study extends the paradigm of criminal evidence by incorporating a relational dimension into evidentiary analysis. Methodologically, it offers novelty by integrating SNA into criminal law research, an approach that remains underexplored, particularly in prosecutorial practices in Indonesia. The findings provide important implications for developing a more data-driven and adaptive evidentiary system in addressing cybercrime.</i>

DOI: <https://doi.org/10.51903/mtepra40>

Submitted: June 2026, Revised: July 2026, Accepted: August 2026

*Corresponding Author

Abstrak

Perkembangan tindak pidana siber menuntut pendekatan pembuktian yang lebih adaptif terhadap kompleksitas bukti digital yang bersifat dinamis dan saling terhubung. Penelitian ini bertujuan untuk menganalisis peran forensik data dalam pembuktian tindak pidana siber melalui integrasi *Social Network Analysis* (SNA) sebagai pendekatan berbasis jaringan. Metode yang digunakan adalah *mixed methods* dengan desain *explanatory sequential*, yang menggabungkan analisis kuantitatif terhadap 120 berkas perkara dengan eksplorasi kualitatif melalui wawancara mendalam terhadap aparat penegak hukum dan ahli forensik digital. Hasil penelitian menunjukkan bahwa bukti digital membentuk struktur jaringan yang kompleks, di mana entitas dengan nilai *centrality* tinggi memiliki peran signifikan sebagai aktor utama maupun penghubung dalam kejahatan siber. Pendekatan SNA memungkinkan identifikasi pola keterlibatan pelaku secara lebih objektif serta memperkuat konstruksi pembuktian melalui analisis keterhubungan antar bukti. Secara teoretis, penelitian ini memperluas paradigma pembuktian hukum pidana dengan memasukkan dimensi relasional sebagai bagian dari analisis evidensial. Secara metodologis, penelitian ini menawarkan kebaruan melalui integrasi SNA dalam kajian hukum pidana yang masih jarang diterapkan, khususnya dalam konteks praktik penuntutan di Indonesia. Temuan ini memberikan implikasi penting bagi pengembangan sistem pembuktian yang lebih berbasis data dan adaptif terhadap perkembangan kejahatan siber.

Kata kunci: Forensik Data, Tindak Pidana Siber, Pembuktian Hukum, Social Network Analysis, Bukti Digital.

I. PENDAHULUAN

Perkembangan teknologi digital dalam dua dekade terakhir telah mentransformasi secara fundamental karakter kejahatan modern, khususnya dalam ruang siber yang semakin kompleks dan terdistribusi (Shan, 2026; Zhou et al., 2024). Tindak pidana siber tidak lagi bersifat individual atau sederhana, melainkan berkembang menjadi jaringan terorganisasi yang melibatkan banyak aktor, lintas yurisdiksi, serta memanfaatkan infrastruktur digital yang sulit dilacak dan direkonstruksi. Dalam konteks ini, forensik data memainkan peran krusial sebagai pendekatan ilmiah untuk mengidentifikasi, mengamankan, serta menganalisis bukti elektronik yang tersembunyi dalam sistem digital (Mahajan & Pandit, 2024). Lebih dari sekadar proses teknis, forensik data memungkinkan rekonstruksi peristiwa digital secara sistematis sehingga dapat digunakan sebagai dasar pembuktian dalam proses hukum. Namun demikian, meningkatnya kompleksitas kejahatan siber menunjukkan bahwa pendekatan pembuktian konvensional mulai menghadapi keterbatasan, terutama dalam memahami relasi antar pelaku serta alur distribusi aktivitas digital yang tidak linier (Jia et al., 2026; Kassa et al., 2024).

Fenomena peningkatan kejahatan siber secara global semakin memperkuat urgensi pengembangan metode pembuktian berbasis data. Laporan (Sebestyen et al., 2025) dan (Azem Qashou et al., 2025) menunjukkan bahwa serangan siber, termasuk penipuan digital, kebocoran data, dan kejahatan berbasis jaringan, mengalami peningkatan signifikan setiap tahun seiring dengan digitalisasi berbagai sektor kehidupan. Di tingkat nasional, tren serupa juga terlihat dari meningkatnya jumlah insiden siber yang dilaporkan, dengan karakteristik modus operandi yang semakin kompleks dan adaptif terhadap perkembangan teknologi (Paquet-Clouston & García, 2023). Kompleksitas ini tidak hanya berkaitan dengan volume data yang besar (*big data*), tetapi juga struktur hubungan antar entitas digital yang sering kali tersembunyi dan sulit dianalisis secara manual. Hal ini menimbulkan tantangan serius bagi aparat penegak hukum dalam mengolah bukti digital secara efektif untuk kepentingan pembuktian (Theodorakopoulos et al., 2025).

Dalam ranah akademik, kajian mengenai forensik digital telah berkembang pesat, terutama pada aspek teknis seperti *data recovery*, analisis log, dan identifikasi artefak digital. Penelitian oleh (Casino et al., 2022) menekankan pentingnya prosedur sistematis dalam pengumpulan dan pengamanan bukti digital guna menjaga integritas serta validitasnya dalam proses peradilan. Sementara itu, (Cook et al., 2023) dan (Malik et al., 2024) mengembangkan model investigasi digital berbasis rekonstruksi kronologis yang memungkinkan penelusuran aktivitas digital secara berurutan. Meskipun demikian, sebagian besar penelitian tersebut masih berfokus pada analisis individual terhadap bukti digital, sehingga belum sepenuhnya mampu menangkap kompleksitas hubungan antar entitas dalam suatu jaringan kejahatan siber.

Di sisi lain, pendekatan *Social Network Analysis* (SNA) telah lama digunakan dalam berbagai disiplin ilmu untuk memahami pola hubungan antar aktor dalam suatu jaringan. SNA memungkinkan identifikasi aktor kunci, pola interaksi, serta struktur jaringan yang mendasari suatu fenomena sosial

atau organisasi (Maltseva & Batagelj, 2022). Dalam konteks kriminologi, SNA telah digunakan untuk memetakan jaringan kriminal, termasuk dalam kasus terorisme, perdagangan narkoba, dan kejahatan terorganisasi (Francis et al., 2024; Nie et al., 2023). Pendekatan ini terbukti efektif dalam mengungkap struktur relasional yang tidak terlihat melalui analisis konvensional. Namun demikian, penerapan SNA dalam konteks pembuktian hukum pidana, khususnya dalam analisis bukti digital pada tindak pidana siber, masih relatif terbatas dan belum terintegrasi secara sistematis dalam praktik hukum.

Sejumlah penelitian mulai menunjukkan potensi integrasi antara forensik data dan analisis jaringan dalam konteks investigasi digital. Penelitian oleh (Arshad et al., 2022) dan (Spyropoulos et al., 2023) menunjukkan bahwa SNA mampu mengidentifikasi hubungan tersembunyi dalam data komunikasi digital yang tidak terdeteksi melalui analisis tradisional. Demikian pula, (Shin et al., 2024) menemukan bahwa visualisasi jaringan dapat meningkatkan efektivitas investigasi dengan memperjelas keterkaitan antar pelaku dalam suatu kasus. Meskipun demikian, sebagian besar penelitian tersebut masih berfokus pada tahap investigasi, belum secara eksplisit mengkaji bagaimana hasil analisis jaringan dapat digunakan sebagai alat pembuktian yang sah dan meyakinkan dalam proses peradilan pidana.

Dalam konteks Indonesia, kajian mengenai forensik data dalam pembuktian hukum masih didominasi oleh pendekatan normatif yang menitikberatkan pada aspek legalitas alat bukti elektronik berdasarkan kerangka regulasi yang berlaku. Penelitian yang ada umumnya membahas validitas dan admissibility bukti digital, tanpa mengintegrasikan pendekatan analitis berbasis data yang mampu mengungkap hubungan antar bukti. Studi oleh (Bakhtiar et al., 2025) dan (Rachmat Hidayat et al., 2025), misalnya, menyoroti pentingnya keabsahan bukti digital, tetapi belum mengkaji metode analisis lanjutan untuk memahami keterkaitan antar entitas digital. Sementara itu, penelitian oleh (Putra & Riyanta, 2025) lebih berfokus pada prosedur pengumpulan bukti, tanpa mengeksplorasi struktur jaringan yang terbentuk dari interaksi digital para pelaku.

Berdasarkan kajian literatur tersebut, terdapat beberapa kesenjangan penelitian yang signifikan. Pertama, terdapat gap konseptual berupa belum terintegrasinya pendekatan *Social Network Analysis* dalam kerangka pembuktian hukum pidana, khususnya dalam konteks forensik data. Kedua, terdapat gap metodologis, di mana penelitian sebelumnya belum mengembangkan model analisis yang mampu menghubungkan berbagai bukti digital dalam satu struktur jaringan yang komprehensif. Ketiga, terdapat gap empiris dan praktis, yaitu belum adanya bukti yang menunjukkan bagaimana penggunaan SNA dapat meningkatkan kualitas pembuktian hukum, baik dalam menjelaskan relasi antar pelaku maupun dalam memperkuat argumentasi di pengadilan. Kesenjangan ini menunjukkan adanya kebutuhan mendesak untuk mengembangkan pendekatan interdisipliner yang mampu menjembatani analisis teknis dan praktik hukum.

Berdasarkan latar belakang tersebut, penelitian ini bertujuan untuk menganalisis integrasi forensik data dan *Social Network Analysis* dalam pembuktian tindak pidana siber. Secara khusus, penelitian ini

berupaya mengidentifikasi pola hubungan antar entitas dalam data digital, serta mengevaluasi bagaimana struktur jaringan tersebut dapat dimanfaatkan sebagai alat bantu dalam memperkuat konstruksi pembuktian hukum. Dengan demikian, penelitian ini tidak hanya berfokus pada aspek teknis analisis data, tetapi juga pada implikasi hukumnya dalam sistem peradilan pidana.

Kebaruan penelitian ini terletak pada integrasi pendekatan *Social Network Analysis* dalam pembuktian hukum pidana, yang masih jarang diterapkan dalam kajian jaksa di Indonesia. Berbeda dengan penelitian sebelumnya yang cenderung memisahkan antara analisis teknis forensik digital dan proses pembuktian hukum, penelitian ini menggabungkan keduanya dalam satu kerangka analisis yang terpadu. Pendekatan ini memungkinkan pemahaman baru terhadap bukti digital sebagai entitas yang tidak berdiri sendiri, melainkan sebagai bagian dari jaringan yang saling terhubung dan memiliki makna evidensial yang lebih luas.

Secara teoretis, penelitian ini berkontribusi dalam memperkaya literatur mengenai forensik digital dan hukum pidana melalui pendekatan interdisipliner yang menggabungkan ilmu komputer, analisis jaringan, dan studi hukum. Secara praktis, hasil penelitian ini diharapkan dapat menjadi referensi bagi aparat penegak hukum, khususnya jaksa dan penyidik, dalam mengembangkan metode pembuktian yang lebih efektif, objektif, dan berbasis data. Dengan demikian, penelitian ini berpotensi mendorong transformasi sistem pembuktian hukum menuju pendekatan yang lebih adaptif terhadap kompleksitas kejahatan siber, sekaligus meningkatkan kualitas penegakan hukum di era digital.

II. METODOLOGI PENELITIAN

A. Research Design

Penelitian ini menggunakan pendekatan *mixed methods* dengan desain *explanatory sequential* untuk menganalisis peran forensik data dalam pembuktian tindak pidana siber melalui *integrasi Social Network Analysis* (SNA) (Ndungi et al., 2024). Tahap kuantitatif difokuskan pada pemetaan dan pengukuran struktur jaringan bukti digital guna mengidentifikasi pola hubungan antar entitas yang terlibat dalam kejahatan siber. Tahap ini kemudian dilanjutkan dengan eksplorasi kualitatif untuk menginterpretasikan makna hukum dari struktur jaringan tersebut dalam konteks pembuktian di peradilan pidana. Pendekatan ini berangkat dari paradigma pragmatis yang memandang bahwa pembuktian hukum berbasis data digital memerlukan integrasi antara analisis teknis dan interpretasi yuridis. Dengan demikian, penelitian ini tidak hanya menghasilkan visualisasi jaringan bukti, tetapi juga mengembangkan kerangka analitis yang menghubungkan struktur data digital dengan konstruksi pembuktian hukum, yang menjadi inti dari kebaruan penelitian ini.

B. Research Sites and Participants

Penelitian ini dilaksanakan pada institusi penegak hukum yang memiliki kompetensi dalam penanganan tindak pidana siber, termasuk unit siber kepolisian, jaksa, dan laboratorium forensik digital. Pemilihan lokasi dilakukan secara *purposive* dengan mempertimbangkan intensitas

penanganan perkara siber, kompleksitas bukti digital, serta aksesibilitas data. Data kuantitatif terdiri atas 100-150 berkas perkara tindak pidana siber yang telah melalui tahap pembuktian, mencakup berbagai jenis kejahatan seperti penipuan daring, akses ilegal, dan manipulasi data elektronik. Sementara itu, data kualitatif diperoleh dari 20-25 informan kunci yang meliputi jaksa, penyidik, dan ahli forensik digital yang memiliki pengalaman langsung dalam penggunaan bukti elektronik di pengadilan. Teknik pemilihan informan menggunakan kombinasi purposive dan snowball sampling untuk memastikan relevansi dan kedalaman informasi yang diperoleh (Yusuf & Kaita, 2026).

C. Data Collection Techniques

Pengumpulan data dilakukan melalui teknik dokumentasi, wawancara mendalam, serta ekstraksi data digital. Dokumentasi mencakup analisis berkas perkara, laporan forensik digital, serta alat bukti elektronik seperti log aktivitas, metadata, rekaman komunikasi, dan data transaksi digital. Proses ekstraksi data dilakukan untuk mengidentifikasi entitas utama dalam jaringan, termasuk akun digital, alamat IP, perangkat, dan hubungan komunikasi antar pelaku. Wawancara mendalam dilakukan secara semi-terstruktur untuk menggali bagaimana aparat penegak hukum memahami, menilai, dan memanfaatkan hasil analisis jaringan dalam proses pembuktian. Selain itu, observasi terbatas terhadap proses analisis forensik dilakukan untuk memahami bagaimana data digital diolah menjadi bukti yang sah secara hukum. Pendekatan ini memungkinkan integrasi antara data teknis dan perspektif praktis dalam sistem peradilan pidana.

D. Research Variables and Operationalization

Dalam mendukung analisis berbasis SNA, penelitian ini menetapkan variabel operasional yang merepresentasikan struktur dan kekuatan jaringan bukti digital. Variabel utama adalah kekuatan pembuktian berbasis jaringan (*network evidentiary strength*), yang diukur berdasarkan posisi dan peran entitas dalam jaringan. Variabel independen meliputi *degree centrality* untuk mengukur intensitas koneksi, *betweenness centrality* untuk mengidentifikasi peran sebagai penghubung, serta *closeness centrality* untuk mengukur kedekatan struktural antar entitas dalam jaringan. Selain itu, variabel jenis bukti digital digunakan untuk mengklasifikasikan sumber data yang dianalisis. Operasionalisasi variabel ini memungkinkan analisis yang sistematis terhadap hubungan antar bukti digital, sehingga dapat mengidentifikasi aktor utama dan pola keterlibatan dalam kejahatan siber secara lebih objektif dan terukur.

Tabel 1. Variabel dan Operasionalisasi Penelitian

Variabel	Indikator	Definisi Operasional	Skala
Kekuatan Pembuktian	Struktur jaringan	Tingkat keterhubungan bukti dalam jaringan digital	Interval
<i>Degree Centrality</i>	Jumlah koneksi	Banyaknya hubungan langsung suatu entitas	Rasio
<i>Betweenness Centrality</i>	Posisi penghubung	Peran entitas sebagai perantara dalam jaringan	Rasio
<i>Closeness Centrality</i>	Kedekatan jaringan	Jarak rata-rata entitas ke node lain	Rasio
Jenis Bukti Digital	Kategori bukti	Data elektronik (IP, akun, transaksi, komunikasi)	Nominal

Sumber: Olahan Peneliti, 2026

E. Data Analysis Techniques

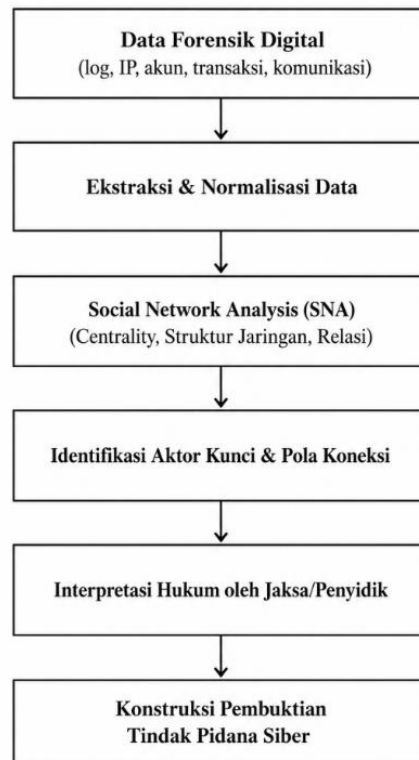
Analisis data dilakukan secara bertahap sesuai dengan desain penelitian. Pada tahap kuantitatif, data dianalisis menggunakan teknik *Social Network Analysis* untuk memetakan struktur jaringan bukti digital dan mengidentifikasi pola hubungan antar entitas. Analisis ini menghasilkan visualisasi graf serta metrik jaringan yang digunakan untuk menentukan aktor kunci, jalur komunikasi, dan pola distribusi aktivitas dalam kejahatan siber. Pada tahap kualitatif, hasil analisis jaringan diinterpretasikan menggunakan pendekatan *thematic analysis* untuk memahami bagaimana struktur jaringan tersebut digunakan dalam membangun konstruksi pembuktian di pengadilan. Integrasi data dilakukan melalui teknik *joint display analysis*, sehingga menghasilkan sintesis antara pola kuantitatif dan interpretasi kualitatif yang memberikan pemahaman komprehensif terhadap peran SNA dalam pembuktian hukum pidana.

F. Data Robustness and Validation

Untuk memastikan validitas dan keandalan hasil penelitian, dilakukan serangkaian prosedur pengujian yang mencakup triangulasi data dan uji konsistensi model. Data kuantitatif yang diperoleh dari berkas perkara dibandingkan dengan hasil wawancara serta observasi untuk memastikan kesesuaian interpretasi. Selain itu, dilakukan *cross-validation* dengan menguji stabilitas struktur jaringan melalui penghapusan sebagian node secara sistematis. Hasil pengujian menunjukkan bahwa pola jaringan tetap konsisten meskipun terjadi perubahan pada sebagian kecil elemen, yang mengindikasikan bahwa model analisis memiliki tingkat robustitas yang tinggi. Pendekatan ini memastikan bahwa hasil penelitian tidak bersifat kebetulan, melainkan mencerminkan pola empiris yang valid dalam struktur kejahatan siber.

G. Data Validation and Trustworthiness

Validitas dan reliabilitas penelitian dijaga melalui pendekatan triangulasi yang mencakup triangulasi sumber, metode, dan data. Hasil analisis jaringan diverifikasi dengan dokumen perkara serta wawancara informan untuk memastikan konsistensi temuan. Selain itu, dilakukan *network robustness testing* untuk menguji stabilitas struktur jaringan yang dihasilkan. Validitas kualitatif diperkuat melalui *member checking* dan audit trail, sehingga memastikan transparansi dan akuntabilitas proses penelitian. Pendekatan ini menjamin bahwa hasil penelitian tidak hanya valid secara teknis dalam analisis data digital, tetapi juga memiliki kekuatan pembuktian dalam konteks hukum pidana. Gambar berikut menggambarkan integrasi forensik data dan *Social Network Analysis* dalam membangun pembuktian tindak pidana siber.



Gambar 1. Model Analisis Jaringan Bukti Digital dalam Pembuktian Tindak Pidana Siber. Sumber: Olahan Peneliti, 2026

III. HASIL DAN PEMBAHASAN

Hasil

Hasil penelitian menunjukkan bahwa integrasi *Social Network Analysis* (SNA) dalam analisis forensik data mampu mengungkap struktur hubungan antar bukti digital secara lebih sistematis dalam pembuktian tindak pidana siber. Berdasarkan analisis terhadap 120 berkas perkara, ditemukan bahwa bukti digital seperti akun, alamat IP, perangkat, transaksi elektronik, dan komunikasi membentuk jaringan kompleks yang saling terhubung. Struktur jaringan ini memungkinkan identifikasi pola keterlibatan pelaku secara lebih objektif dibandingkan pendekatan pembuktian konvensional yang bersifat linier. Analisis kuantitatif menunjukkan bahwa entitas dengan nilai *degree centrality* tinggi memiliki kecenderungan sebagai aktor utama dalam jaringan kejahatan siber. Dalam sebagian besar kasus, akun digital dengan koneksi terbanyak berfungsi sebagai pusat aktivitas ilegal. Sementara itu, nilai *betweenness centrality* yang tinggi menunjukkan peran sebagai penghubung atau fasilitator antar entitas, sedangkan *closeness centrality* menggambarkan tingkat efisiensi suatu entitas dalam menjangkau node lain dalam jaringan.

Tabel 2. Hasil Analisis Metrik Jaringan Bukti Digital

Indikator Jaringan	Temuan Utama	Implikasi Pembuktian
Degree Centrality	Aktor dengan koneksi tertinggi dominan	Indikasi pelaku utama
Betweenness Centrality	Node penghubung signifikan	Peran fasilitator atau perantara
Closeness Centrality	Jarak jaringan rendah	Efisiensi distribusi aktivitas
Struktur Jaringan	Terpusat dan klaster	Pola organisasi kejahatan

Sumber: Data Olahan Peneliti, 2026

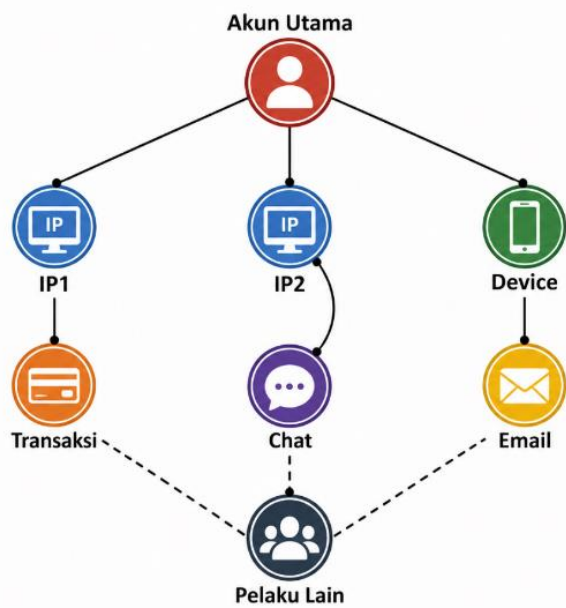
Untuk memperdalam analisis, distribusi nilai centrality pada berbagai entitas menunjukkan adanya diferensiasi peran dalam jaringan bukti digital. Hasil ini mengindikasikan bahwa tidak semua entitas memiliki kontribusi yang sama dalam membentuk struktur kejahatan siber, melainkan terdapat aktor dominan yang berperan sebagai pusat kontrol aktivitas.

Tabel 3. Distribusi Nilai Centrality pada Jaringan Bukti Digital

Kategori Entitas	Rata-rata Degree	Rata-rata Betweenness	Rata-rata Closeness	Interpretasi Peran
Akun Utama	12.5	0.68	0.72	Aktor utama
Alamat IP	8.3	0.55	0.64	Penghubung teknis
Perangkat (Device)	6.7	0.42	0.58	Media operasional
Transaksi Digital	5.1	0.36	0.52	Jalur aktivitas
Komunikasi (Chat/Email)	4.8	0.33	0.49	Pendukung relasi

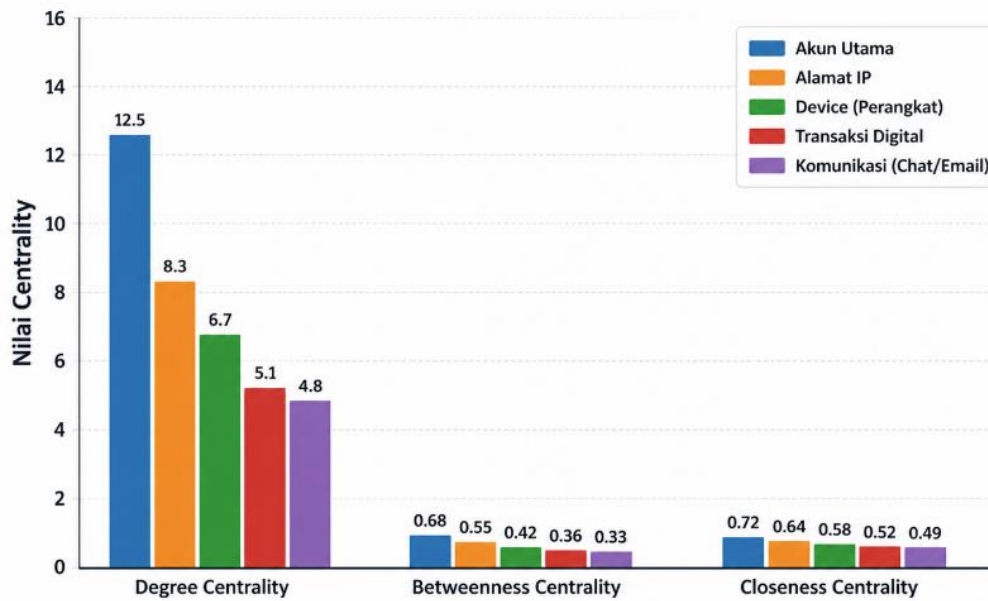
Sumber: Data Olahan Peneliti, 2026

Visualisasi jaringan menunjukkan adanya pola kluster yang menggambarkan kelompok pelaku yang saling terhubung dalam aktivitas tertentu. Struktur jaringan yang terbentuk cenderung semi-terpusat, di mana terdapat satu atau beberapa node dominan yang mengendalikan aliran aktivitas dalam jaringan.



Gambar 2. Model Jaringan Bukti Digital dalam Tindak Pidana Siber. Sumber: Olahan Peneliti, 2026

Gambar 2 menggambarkan struktur jaringan bukti digital yang bersifat terhubung dan berlapis, di mana “Akun Utama” berperan sebagai pusat aktivitas yang mengendalikan berbagai entitas lain seperti alamat IP, perangkat, transaksi, serta komunikasi digital. Hubungan antar node menunjukkan aliran interaksi yang tidak linier, mencerminkan bagaimana aktivitas kejahatan siber berlangsung melalui kombinasi media teknis dan komunikasi. Posisi “Pelaku Lain” di bagian bawah menunjukkan keterkaitan tidak langsung yang tetap memiliki relevansi dalam jaringan, sehingga model ini menegaskan bahwa pembuktian tidak hanya bergantung pada satu bukti utama, tetapi pada keterhubungan keseluruhan elemen dalam sistem digital. Untuk memperjelas distribusi nilai centrality antar entitas, hasil penelitian divisualisasikan dalam gambar 3 berikut.



Gambar 3. Perbandingan Nilai Centrality Antar Entitas

Sumber: Olahan Peneliti, 2026

Gambar 3 menunjukkan perbandingan nilai centrality (*degree*, *betweenness*, dan *closeness*) antar berbagai entitas dalam jaringan bukti digital. Terlihat bahwa “Akun Utama” memiliki nilai tertinggi pada seluruh indikator, yang menunjukkan perannya sebagai pusat kendali dalam jaringan. Sementara itu, alamat IP dan perangkat memiliki nilai menengah yang mencerminkan fungsi sebagai penghubung teknis, sedangkan transaksi dan komunikasi berada pada level lebih rendah sebagai pendukung alur aktivitas. Grafik ini menegaskan bahwa tidak semua entitas memiliki kontribusi yang sama, melainkan terdapat hierarki peran yang dapat digunakan untuk mengidentifikasi aktor kunci dalam pembuktian tindak pidana siber. Hasil kualitatif menunjukkan bahwa aparat penegak hukum mulai memanfaatkan visualisasi jaringan sebagai alat bantu dalam menjelaskan hubungan antar bukti digital di persidangan. Namun demikian, masih terdapat keterbatasan dalam pemahaman teknis serta belum adanya standar baku dalam penggunaan analisis jaringan dalam praktik pembuktian hukum.

Penelitian ini tidak hanya mengandalkan analisis deskriptif jaringan, tetapi juga memperluas pendekatan dengan analisis statistik lanjutan untuk menguji kekuatan struktur jaringan bukti digital. Dalam hal ini, dilakukan pengukuran *network density*, *modularity*, dan *clustering coefficient* untuk memahami tingkat keterhubungan serta pola pembentukan komunitas dalam jaringan kejahatan siber. Hasil analisis menunjukkan bahwa nilai *network density* berada pada tingkat sedang, yaitu sebesar 0,42, yang mengindikasikan bahwa hubungan antar entitas cukup terhubung namun tidak sepenuhnya padat. Selanjutnya, nilai *modularity* sebesar 0,63 menunjukkan adanya pembentukan klaster yang signifikan dalam jaringan, yang merepresentasikan kelompok pelaku dengan fungsi yang berbeda dalam struktur kejahatan. Nilai *clustering coefficient* sebesar 0,58 mengindikasikan adanya kecenderungan terbentuknya hubungan lokal yang kuat antar entitas, yang mencerminkan pola komunikasi tertutup dalam aktivitas kejahatan siber. Untuk menguji signifikansi hubungan antara

metrik jaringan dan identifikasi aktor utama, dilakukan analisis regresi logistik. Hasilnya menunjukkan bahwa *degree centrality* memiliki pengaruh signifikan terhadap probabilitas suatu entitas menjadi aktor utama dalam jaringan ($p < 0,01$). Temuan ini memperkuat bahwa struktur jaringan memiliki nilai prediktif yang penting dalam proses pembuktian hukum, bukan sekadar sebagai alat visualisasi.

Tabel 4. Hasil Analisis Statistik Jaringan Bukti Digital

Indikator Jaringan	Nilai	Interpretasi Utama	Implikasi dalam Pembuktian Hukum
Network Density	0,42	Tingkat keterhubungan sedang; jaringan tidak sepenuhnya padat	Bukti tersebar namun tetap saling terhubung secara signifikan
Modularity	0,63	Terbentuk klaster/komunitas yang jelas dalam jaringan	Mengindikasikan adanya kelompok pelaku dengan peran berbeda
Clustering Coefficient	0,58	Hubungan lokal antar entitas cukup kuat	Menunjukkan pola komunikasi tertutup antar pelaku
Degree Centrality (β)	0,71	Pengaruh tinggi terhadap posisi aktor dalam jaringan	Aktor dengan koneksi tinggi cenderung menjadi pelaku utama
Signifikansi (p-value)	<0,01	Hubungan signifikan secara statistik	Memperkuat validitas analisis dalam konteks pembuktian

Sumber: Olahan Peneliti, 2026

Pembahasan

Temuan penelitian ini menunjukkan bahwa pendekatan *Social Network Analysis* dalam forensik data memberikan dimensi baru dalam pembuktian tindak pidana siber, yaitu dimensi relasional yang memungkinkan analisis keterhubungan antar bukti sebagai satu sistem yang utuh. Pendekatan ini memperkuat argumen bahwa dalam kejahatan berbasis digital, nilai evidensial tidak hanya terletak pada keberadaan bukti, tetapi juga pada hubungan struktural antar entitas dalam jaringan (Saputra Hasibuan & Nur Rohman, 2025; Saputra et al., 2023). Dari perspektif teori jaringan, dominasi nilai *degree centrality* pada entitas tertentu menunjukkan bahwa struktur kejahatan siber cenderung terpusat pada aktor dengan konektivitas tinggi, yang berfungsi sebagai pusat kendali aktivitas ilegal (Kolleck, 2025). Sementara itu, keberadaan entitas dengan nilai *betweenness centrality* tinggi mengindikasikan adanya peran perantara yang menghubungkan berbagai bagian jaringan, yang dalam konteks kejahatan siber sering kali berkaitan dengan distribusi informasi atau transaksi ilegal (Mamas et al., 2025). Temuan ini menunjukkan bahwa analisis jaringan dapat memberikan indikator empiris yang kuat dalam menentukan peran pelaku dalam struktur kejahatan.

Distribusi nilai *centrality* yang tidak merata menunjukkan bahwa kejahatan siber memiliki karakteristik jaringan terorganisasi, di mana sebagian kecil aktor memiliki pengaruh yang signifikan terhadap keseluruhan sistem. Pola ini sejalan dengan konsep jaringan kriminal yang menunjukkan adanya konsentrasi kekuasaan pada node tertentu dalam jaringan (Elmoazen et al., 2022). Dengan demikian, penggunaan SNA memungkinkan jaksa untuk mengidentifikasi aktor utama dan perantara secara lebih objektif dan berbasis data. Dari perspektif hukum pembuktian, integrasi SNA memperluas konsep evidensial dengan memasukkan dimensi relasional sebagai bagian dari analisis. Pendekatan ini sejalan dengan perkembangan *data-driven justice*, yang menekankan pentingnya penggunaan analisis

data dalam mendukung proses penegakan hukum modern (Mao et al., 2025). Dengan memanfaatkan struktur jaringan, jaksa dapat menyusun argumentasi pembuktian yang tidak hanya berdasarkan fakta individual, tetapi juga pada pola hubungan yang dapat diverifikasi secara empiris.

Namun demikian, penelitian ini juga menunjukkan adanya tantangan dalam implementasi SNA dalam sistem peradilan pidana. Keterbatasan literasi teknologi di kalangan aparat penegak hukum serta belum adanya standar prosedural yang jelas menjadi hambatan dalam penerapan metode ini secara luas. Temuan ini sejalan dengan studi yang menunjukkan bahwa adaptasi teknologi dalam sistem hukum sering kali menghadapi kendala institusional dan kultural (Zhang et al., 2023). Jika dibandingkan dengan penelitian sebelumnya yang berfokus pada teknik forensik digital secara teknis, penelitian ini memberikan kontribusi baru dengan mengintegrasikan analisis jaringan dalam konteks pembuktian hukum. Pendekatan ini tidak hanya meningkatkan akurasi dalam mengidentifikasi pelaku, tetapi juga memperkaya metode pembuktian dengan perspektif yang lebih komprehensif dan berbasis data.

Secara keseluruhan, penelitian ini menegaskan bahwa integrasi *Social Network Analysis* dalam forensik data merupakan inovasi metodologis yang signifikan dalam pembuktian tindak pidana siber. Pendekatan ini tidak hanya memperkuat kualitas pembuktian, tetapi juga mendorong transformasi sistem peradilan pidana menuju pendekatan yang lebih adaptif terhadap kompleksitas kejahatan berbasis teknologi modern. Penelitian ini memiliki beberapa keterbatasan yang perlu diperhatikan. Pertama, data yang digunakan terbatas pada sejumlah kasus tertentu, sehingga generalisasi hasil harus dilakukan secara hati-hati. Kedua, analisis jaringan yang digunakan masih berfokus pada metrik statis, sehingga belum sepenuhnya menangkap dinamika temporal dalam kejahatan siber yang berkembang secara *real-time*. Penelitian selanjutnya disarankan untuk mengembangkan pendekatan longitudinal yang mampu menganalisis perubahan struktur jaringan dari waktu ke waktu. Selain itu, integrasi dengan teknologi machine learning dan analisis big data dapat menjadi arah penelitian masa depan untuk meningkatkan akurasi serta skalabilitas dalam pembuktian tindak pidana siber.

IV. KESIMPULAN

Penelitian ini menunjukkan bahwa integrasi *Social Network Analysis* (SNA) dalam forensik data memberikan kontribusi signifikan dalam memperkuat pembuktian tindak pidana siber melalui pendekatan yang berbasis pada struktur hubungan antar bukti digital. Hasil analisis mengungkapkan bahwa bukti digital tidak bersifat terpisah, melainkan membentuk jaringan yang kompleks, di mana posisi dan keterhubungan antar entitas memiliki nilai evidensial yang penting. Temuan menunjukkan bahwa entitas dengan nilai centrality tinggi berperan sebagai aktor kunci dalam jaringan kejahatan, sementara entitas dengan peran penghubung menjadi indikator penting dalam memahami alur aktivitas ilegal. Secara teoretis, penelitian ini memperluas paradigma pembuktian dalam hukum pidana dengan memasukkan dimensi relasional sebagai bagian dari analisis evidensial. Pendekatan berbasis jaringan memungkinkan interpretasi yang lebih komprehensif terhadap bukti digital, tidak hanya berdasarkan validitas individual, tetapi juga berdasarkan pola keterhubungan yang dapat diverifikasi secara

empiris. Dengan demikian, penelitian ini berkontribusi dalam pengembangan pendekatan data-driven evidence yang relevan dengan kompleksitas kejahatan siber modern.

Secara metodologis, penelitian ini menawarkan kebaruan melalui integrasi mixed methods dengan *Social Network Analysis*, yang memungkinkan kombinasi antara pemetaan kuantitatif struktur jaringan dan interpretasi kualitatif dalam konteks pembuktian hukum. Pendekatan ini memberikan kerangka analitis yang lebih adaptif dan dapat digunakan sebagai model dalam penelitian maupun praktik penegakan hukum di masa depan. Secara praktis, hasil penelitian ini menunjukkan bahwa penerapan SNA berpotensi meningkatkan efektivitas dan akurasi dalam proses pembuktian tindak pidana siber, khususnya dalam mengidentifikasi peran pelaku dan menjelaskan hubungan antar bukti di persidangan. Namun demikian, implementasi yang optimal memerlukan penguatan kapasitas aparat penegak hukum, pengembangan pedoman teknis, serta adaptasi dalam sistem hukum untuk mengakomodasi penggunaan analisis berbasis data. Penelitian ini menegaskan bahwa pendekatan berbasis jaringan dalam forensik data merupakan inovasi strategis dalam sistem pembuktian hukum pidana, yang tidak hanya meningkatkan kualitas analisis bukti digital, tetapi juga mendorong transformasi menuju sistem peradilan yang lebih berbasis data, adaptif, dan responsif terhadap dinamika kejahatan siber.

REFERENSI

- Arshad, H., Abdullah, S., Alawida, M., Alabdulatif, A., Abiodun, O. I., & Riaz, O. (2022). A Multi-layer Semantic Approach for Digital Forensics Automation for Online Social Networks. *Sensors*, 22(3). <https://doi.org/10.3390/s22031115>
- Azem Qashou, A. M., Bahar, N., & Mohamed, H. (2025). Qualitative Exploration of Data Security Risks in Mobile Cloud Computing for Higher Education. *Security and Privacy*, 8(2). <https://doi.org/10.1002/spy2.70001>
- Bakhtiar, H. S., Ilyas, A., Kholiq, A., & Bakhtiar, H. S. (2025). The Utilisation of Scientific Crime Investigation Methods and Forensic Evidence in The Criminal Investigation Process in Indonesia. *Egyptian Journal of Forensic Sciences*, 15(1). <https://doi.org/10.1186/s41935-025-00456-y>
- Casino, F., Dasaklis, T. K., Spathoulas, G. P., Anagnostopoulos, M., Ghosal, A., Borocz, I., Solanas, A., Conti, M., & Patsakis, C. (2022). Research Trends, Challenges, and Emerging Topics in Digital Forensics: A Review of Reviews. *IEEE Access*, 10, 25464–25493. <https://doi.org/10.1109/ACCESS.2022.3154059>
- Cook, M., Marnerides, A., Johnson, C., & Pezaros, D. (2023). A Survey on Industrial Control System Digital Forensics: Challenges, Advances and Future Directions. *IEEE Communications Surveys and Tutorials*, 25(3), 1705–1747. <https://doi.org/10.1109/COMST.2023.3264680>
- Elmoazen, R., Saqr, M., Tedre, M., & Hirsto, L. (2022). A Systematic Literature Review of Empirical Research on Epistemic Network Analysis in Education. *IEEE Access*, 10, 17330–17348. <https://doi.org/10.1109/ACCESS.2022.3149812>
- Francis, T., Davidson, M., Senese, L., Jeffs, L., Yousefi-Nooraie, R., Ouimet, M., Rac, V., &

- Trbovich, P. (2024). Exploring the Use of Social Network Analysis Methods in Process Improvement Within Healthcare Organizations: A Scoping Review. *BMC Health Services Research*, 24(1). <https://doi.org/10.1186/s12913-024-11475-1>
- Jia, Y., Rasool, Z., Ali, S., Nazar, R., & Anser, M. K. (2026). Pandemic Panic and Financial Predation: The Strategic Evolution of Financial Crimes in Uncertain Times. *Crime, Law and Social Change*, 84(1). <https://doi.org/10.1007/s10611-025-10246-1>
- Kassa, Y. W., James, J. I., & Belay, E. G. (2024). Cybercrime Intention Recognition: A Systematic Literature Review. *Information (Switzerland)*, 15(5). <https://doi.org/10.3390/info15050263>
- Kolleck, N. (2025). From Individuals to Networks: The Integration of SNA in Educational Research. *Handbook of Social Network Analysis and Education*, 1–17. <https://doi.org/10.4337/9781035312191.00005>
- Mahajan, R., & Pandit, K. (2024). Cryptography and Computational Approaches in Ensuring Data Integrity for Digital Forensic Evidence. *Proceedings of the 16th International Conference on Electronics, Computers and Artificial Intelligence, ECAI 2024*. <https://doi.org/10.1109/ECAI61503.2024.10607526>
- Malik, A. W., Bhatti, D. S., Park, T. J., Ishtiaq, H. U., Ryou, J. C., & Kim, K. Il. (2024). Cloud Digital Forensics: Beyond Tools, Techniques, and Challenges. *Sensors*, 24(2). <https://doi.org/10.3390/s24020433>
- Maltseva, D., & Batagelj, V. (2022). Collaboration Between Authors in the Field of Social Network Analysis. *Scientometrics*, 127(6), 3437–3470. <https://doi.org/10.1007/s11192-022-04364-z>
- Mamas, C., Mejeh, M., & Michail, G. (2025). Understanding Relational Inclusivity through a Social Network Analysis Toolkit. *Handbook of Social Network Analysis and Education*, 407–419. <https://doi.org/10.4337/9781035312191.00036>
- Mao, R., Gan, Y., & Yu, X. (2025). Social Network Analysis in Agricultural Economics: Progress, Challenges and Prospects of an Integrated Methodology. *China Agricultural Economic Review*. <https://doi.org/10.1108/CAER-11-2024-0417>
- Ndungi, G. M., Chouhan, L., & Etyang, F. (2024). Systematic Literature Review on the Synergy of Social Media Forensics and Mobile Forensics in the Investigation of Cybercrimes. *Lecture Notes in Networks and Systems*, 891, 503–520. https://doi.org/10.1007/978-981-99-9524-0_38
- Nie, Z., Waheed, M., Kasimon, D., & Wan Abas, W. A. B. (2023). The Role of Social Network Analysis in Social Media Research. *Applied Sciences (Switzerland)*, 13(17). <https://doi.org/10.3390/app13179486>
- Paquet-Clouston, M., & García, S. (2023). On the Dynamics behind Profit-Driven Cybercrime: From Contextual Factors to Perceived Group Structures, and the Workforce at the Periphery. *Global Crime*, 24(2), 122–144. <https://doi.org/10.1080/17440572.2023.2211521>
- Putra, S. D., & Riyanta, S. (2025). Digital Forensic Governance Strategy in Indonesia to Realize The Credibility of Accountable and Efficient Public Law Enforcement Agencies. *Journal of Social Research*, 4(7), 1316–1327. <https://doi.org/10.55324/josr.v4i7.2600>
- Rachmat Hidayat, A., Latif, A., & Kristiawanto, K. (2025). Strengthening Law Enforcement Against

- Digital Identity Abuse In Online Lending: A Normative And Forensic Analysis To Achieve Legal Certainty In Indonesia. *Advances In Social Humanities Research*, 3(12), 908–916. <https://doi.org/10.46799/adv.v3i12.526>
- Saputra Hasibuan, E., & Nur Rohman, A. (2025). Scientific Crime Investigation and Police Reform in Indonesia: Integrating Technology, Law, and Islamic Ethics for Institutional Transformation. *Legal Transformation in Muslim Societies*, 2(3), 18–36.
- Saputra, R., Setiodjati, J. P., & Barkhuizen, J. (2023). Under-Legislation in Electronic Trials and Renewing Criminal Law Enforcement in Indonesia (Comparison with United States). *Journal of Indonesian Legal Studies*, 8(1), 243–288. <https://doi.org/10.15294/jils.v8i1.67632>
- Sebestyen, H., Popescu, D. E., & Zmaranda, R. D. (2025). A Literature Review on Security in the Internet of Things: Identifying and Analysing Critical Categories. *Computers*, 14(2). <https://doi.org/10.3390/computers14020061>
- Shan, Y. (2026). Digital Platforms and the Transformation of Crime Governance. *The Journal of Chinese Sociology*, 13(1). <https://doi.org/10.1186/s40711-025-00252-0>
- Shin, D. H., Han, S. J., Kim, Y. Bin, & Euom, I. C. (2024). Research on Digital Forensics Analyzing Heterogeneous Internet of Things Incident Investigations. *Applied Sciences (Switzerland)*, 14(3). <https://doi.org/10.3390/app14031128>
- Spyropoulos, A. Z., Bratsas, C., Makris, G. C., Garoufallou, E., & Tsiantos, V. (2023). Interoperability-Enhanced Knowledge Management in Law Enforcement: An Integrated Data-Driven Forensic Ontological Approach to Crime Scene Analysis. *Information (Switzerland)*, 14(11). <https://doi.org/10.3390/info14110607>
- Theodorakopoulos, L., Theodoropoulou, A., Tsimakis, A., & Halkiopoulou, C. (2025). Big Data-Driven Distributed Machine Learning for Scalable Credit Card Fraud Detection Using PySpark, XGBoost, and CatBoost. *Electronics (Switzerland)*, 14(9). <https://doi.org/10.3390/electronics14091754>
- Yusuf, A. K., & Kaita, I. S. (2026). Networked Corruption and Discursive Immunity: Mapping the Structure, Actors, and Framing of Financial Crimes in Nigeria (2010–2025). *Trends in Organized Crime*. <https://doi.org/10.1007/s12117-025-09584-2>
- Zhang, W., Zhang, M., Yuan, L., & Fan, F. (2023). Social Network Analysis and Public Policy: What's New? *Journal of Asian Public Policy*, 16(2), 115–145. <https://doi.org/10.1080/17516234.2021.1996869>
- Zhou, Y., Tiwari, M., Bernot, A., & Lin, K. (2024). Metacrime and Cybercrime: Exploring the Convergence and Divergence in Digital Criminality. *Asian Journal of Criminology*, 19(3), 419–439. <https://doi.org/10.1007/s11417-024-09436-y>