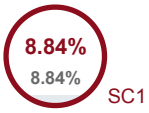
Similarity Report

Metadata

Name of the organization
Universitas Muhammadiyah Sidoarjo
Title
TA_Isabella Efendi
Author(s) Coordinator
perpustakaan umsidairta
Organizational unit
Perpustakaan

Record of similarities

SCs indicate the percentage of the number of words found in other texts compared to the total number of words in the analysed document. Please note that high coefficient values do not automatically mean plagiarism. The report must be analyzed by an authorized person.



7990
Length in words

58800
Length in characters

Alerts

In this section, you can find information regarding text modifications that may aim at temper with the analysis results. Invisible to the person evaluating the content of the document on a printout or in a file, they influence the phrases compared during text analysis (by causing intended misspellings) to conceal borrowings as well as to falsify values in the Similarity Report. It should be assessed whether the modifications are intentional or not.

Characters from another alphabet		0
Spreads	A→	0
Micro spaces		3
Hidden characters		36
Paraphrases (SmartMarks)	a	39

Active lists of similarities

This list of sources below contains sources from various databases. The color of the text indicates in which source it was found. These sources and Similarity Coefficient values do not reflect direct plagiarism. It is necessary to open each source, analyze the content and correctness of the source crediting.

The 10 longest fragments — Color of the text

NO	TITLE OR SOURCE URL (DATABASE)	NUMBER OF IDENTICAL WORDS (FRAGMENTS)
1	Penerapan Model Investigasi Forensik Komputer Umum dalam Analisis Forensik Video CCTV Nugraha Adhitya, Gaffar Andi Widya Mufila, Alwi Erick Irawadi;	34 0.43 %
2	Forensic storage framework development using composite logic method Yudi Prayudi,Helmi Rachman, Bambang Sugiantoro;	34 0.43 %
3	https://www.academia.edu/127287973/CYBERCRIMES_IN_THE_CRYPTOCURRENCY_DOMAIN_IDENTIFYING_TYPES_UNDERSTANDING_MOTIVES_AND_TECHNIQUES_AND_EXPLORING_FUTURE_DIRECTIONS_FOR_TECHNOLOGY_AND_REGULATION	33 0.41 %

4	Kajian Literatur: Metode Analisis dan Tools Live Forensics Pada Random Access Memory (RAM) Yustian Servanda,Ivan Adinata;	29 0.36 %
5	https://archive.umsida.ac.id/index.php/archive/preprint/download/6908/49552/55331	27 0.34 %
6	https://widyasari-press.com/wp-content/uploads/2024/08/8.-Marcella-Putri-Josca-PELINDUNGAN-KONSUMEN-MELALUI-KEWAJIBAN-PENCANTUMAN-SERTIFIKAT-KEANDALAN-.pdf	25 0.31 %
7	https://repository.uksw.edu/bitstream/123456789/29310/10/T1_312019162_Bab%20II.pdf	21 0.26 %
8	http://wajahhukum.unbari.ac.id/index.php/wjhkm/article/download/472/172	21 0.26 %
9	http://wajahhukum.unbari.ac.id/index.php/wjhkm/article/download/472/172	20 0.25 %
10	https://journal.uii.ac.id/JON/article/download/22266/14227/76207	19 0.24 %

from RefBooks database (3.03 %)

NO	TITLE	NUMBER OF IDENTICAL WORDS (FRAGMENTS)
Source: Paperity		
1	Penerapan Model Investigasi Forensik Komputer Umum dalam Analisis Forensik Video CCTV Nugraha Adhitya, Gaffar Andi Widya Mufila, Alwi Erick Irawadi;	**34 (1) 0.43 %**
2	Forensic storage framework development using composite logic method Yudi Prayudi,Helmi Rachman, Bambang Sugiantoro;	**34 (1) 0.43 %**
3	Kajian Literatur: Metode Analisis dan Tools Live Forensics Pada Random Access Memory (RAM) Yustian Servanda,Ivan Adinata;	**29 (1) 0.36 %**
4	ANALISIS KASUS PELECEHAN SEKSUAL CHILD CYBER GROOMING DI MEDIA SOSIAL BERDASARKAN PERSPEKTIF HUKUM PIDANA Haikal Muhammad;	25 (2) 0.31 %
5	PENERAPAN DIGITAL FORENSIK DALAM PEMBUKTIAN PENCEMARAN NAMA BAIK DI DUNIA MAYA Jesica Daun Ponno;	23 (2) 0.29 %
6	Child Cyber Grooming sebagai Bentuk Modus Baru Cyber Space Crimes Anjeli Holivia, Teguh Suratman;	21 (2) 0.26 %
7	Design of Digital Evidence Collection Framework in Social Media Using SNI 27037: 2014 Abba Suganda,Adi Setya;	19 (2) 0.24 %
8	THE ROLE OF SURVEILLANCE TECHNOLOGY IN THE INVESTIGATION PROCESS OF CYBER CRIMES: A LEGAL PERSPECTIVE IN INDONESIA Dwi Saputra Ardianto, Dian Mustika,Maryanti Dwiningsih;	16 (1) 0.20 %
9	KEKUATAN ALAT BUKTI MESIN POLYGRAPH DALAM PERSIDANGAN PERKARA PIDANA DI INDONESIA Erdiansyah Erdiansyah,Ruspian Ruspian, Evi Deliana;	12 (2) 0.15 %
10	Kebijakan Kriminal Penanggulangan Tindak Pidana Seksual Pada Anak Dhina Megayati;	11 (2) 0.14 %
11	Strategy for responding to computer incidents of insecurity set in Ecuadorian law Rodrigo Arturo Proaño-Escalante, Andrés Fernando Gavilanes-Molina;	11 (1) 0.14 %
12	Aspek Hukum dalam Pengaturan Ekonomi Digital: Tantangan dan Peluang di Indonesia Sriyanto Darmawan,Dewi Dian Kemala;	7 (1) 0.09 %

from the home database (0.00 %)

NO	TITLE	NUMBER OF IDENTICAL WORDS (FRAGMENTS)

from the Database Exchange Program (0.31 %)

NO	TITLE	NUMBER OF IDENTICAL WORDS (FRAGMENTS)
1	Макаренков, Коса [redacted] 11/5/2024 Publishing House "Helvetica" (Видавничий дім "Гельветика")	25 (2) 0.31 %

from the Internet (5.49 %)

NO	SOURCE URL	NUMBER OF IDENTICAL WORDS (FRAGMENTS)
1	http://wajahhukum.unbari.ac.id/index.php/wjhkm/article/download/472/172	64 (4) 0.80 %
2	https://journal.uii.ac.id/JON/article/download/22266/14227/76207	46 (3) 0.58 %
3	https://eskripsi.usm.ac.id/files/skripsi/A11A/2017/A.131.17.0002/A.131.17.0002-07-BAB-IV-20210820061221.pdf	38 (6) 0.48 %
4	**https://www.academia.edu/127287973/CYBERCRIMES_IN_THE_CRYPTOCURRENCY_DOMAIN_IDENTIFYING_TYPES_UNDERSTANDING_MOTIVES_AND_TECHNIQUES_AND_EXPLORING_FUTURE_DIRECTIONS_FOR_TECHNOLOGY_AND_REGULATION**	**33 (1) 0.41 %**
5	https://zenodo.org/records/14619174/files/Salsabila%20Amilda_2025_Proofreading.pdf	29 (2) 0.36 %
6	**https://archive.umsida.ac.id/index.php/archive/preprint/download/6908/49552/55331**	**27 (1) 0.34 %**
7	**https://widyasari-press.com/wp-content/uploads/2024/08/8.-Marcella-Putri-Josca-PELINDUNGAN-KONSUMEN-MELALUI-KEWAJIBAN-PENCANTUMAN-SERTIFIKAT-KEANDALAN-.pdf**	**25 (1) 0.31 %**
8	https://penasihathukum.com/bisa-membantu-proses-peradilan-apa-itu-alat-bukti-elektronik	25 (2) 0.31 %
9	https://icjr.or.id/wp-content/uploads/2022/11/Catatan-atas-Dikualifikasikannya-Barang-Bukti-sebagai-Alat-Bukti.pdf	22 (3) 0.28 %
10	https://repository.uksw.edu/bitstream/123456789/29310/10/T1_312019162_Bab%20II.pdf	21 (1) 0.26 %
11	https://ojs.unimal.ac.id/index.php/jimfh/article/download/19938/pdf	20 (2) 0.25 %
12	https://jurnal.unsur.ac.id/jhmj/article/download/2457/1745	13 (2) 0.16 %
13	https://simpelkan.lpsk.go.id/uploads/laporanharian/5a79aa4e575111abcd2a60244366ee0a.pdf	12 (1) 0.15 %
14	https://scholarhub.ui.ac.id/cgi/viewcontent.cgi?article=1233&context=notary	12 (1) 0.15 %
15	https://archive.umsida.ac.id/index.php/archive/preprint/download/5996/42693/47747	10 (1) 0.13 %
16	http://lib.unnes.ac.id/30106/1/8111412202.pdf	10 (2) 0.13 %
17	https://jurnalhukumperatun.mahkamahagung.go.id/index.php/peratun/article/download/159/34/	9 (1) 0.11 %
18	https://archive.umsida.ac.id/index.php/archive/preprint/download/5648/40137/44959	7 (1) 0.09 %
19	https://digilib.uin-suka.ac.id/id/eprint/45164/2/17103040040_BAB-I_IV-atau-V_DAFTAR-PUSTAKA1.pdf	6 (1) 0.08 %
20	https://journals.ums.ac.id/index.php/jurisprudence/article/download/10527/5932	5 (1) 0.06 %
21	https://htlegalconsult.com/pembuktian-elektronik-bagaimana-pengaturannya/	5 (1) 0.06 %

List of accepted fragments (no accepted fragments)

NO	CONTENTS	NUMBER OF IDENTICAL WORDS (FRAGMENTS)

Page | 2

Isabela Efendi 1), Emy Rosnawati *, 2) **1)Program Studi Ilmu Hukum, Universitas Muhammadiyah Sidoarjo, Indonesia 2)Program** Studi Teknik Informatika, Universitas **Muhammadiyah Sidoarjo, Indonesia *Email Penulis** Korespondensi: emyrosnawati@ umsida.ac.id **Abstract.** The advancement of digital technology has significantly contributed to the rise of online sexual crimes against children, particularly through cyber grooming. This study aims to analyze the forms and procedures for presenting digital evidence that are legally valid in proving online sexual crimes against children. The research applies a normative juridical method with statutory, systematic, grammatical, and futuristic interpretation approaches. The findings show that digital evidence such as screenshots, metadata, clone disks, and cloud content carries different levels of legal validity. Among these, clone disks acquired through proper forensic procedures are considered the most conclusive evidence. The study emphasizes the importance of ISO/IEC 27037 standards in the processes of identification, collection, acquisition, and preservation of digital evidence, along with the urgency of URL permanence and chain of custody documentation. Challenges include limited human resources, technical complexity, and difficulties in cross-platform cooperation. Therefore, strengthening the capacity of law enforcement and updating regulations is crucial to ensure the effectiveness of evidence presentation in court.
Keywords - Digital Forensics; Online Sexual Crime Against Children; Digital Evidence

Abstrak. Perkembangan teknologi digital membawa dampak serius dalam meningkatnya kasus kejahatan seksual daring terhadap anak, khususnya melalui modus cyber grooming. Penelitian ini bertujuan untuk menganalisis bentuk dan prosedur penyajian barang bukti digital yang sah dalam pembuktian tindak pidana seksual daring terhadap anak. Metode **yang digunakan adalah yuridis normatif dengan pendekatan perundang-undangan dan** penafsiran sistematis, gramatikal, serta futuristik. Hasil penelitian menunjukkan bahwa alat bukti digital seperti tangkapan layar, metadata, clone disk, dan konten cloud memiliki validitas berbeda di mata hukum. Clone disk dengan prosedur forensik yang tepat dinilai sebagai bukti konklusif paling kuat. Penelitian ini menekankan pentingnya standar ISO/IEC 27037 dalam proses identifikasi, koleksi, akuisisi, dan preservasi bukti digital, serta urgensi permanenisasi URL dan dokumentasi chain of custody. Kendala yang dihadapi mencakup keterbatasan sumber daya manusia, kompleksitas teknis, dan hambatan kerja sama lintas platform. Oleh karena itu, dibutuhkan peningkatan kapasitas aparat penegak hukum dan pembaruan regulasi guna menjamin efektivitas pembuktian di pengadilan.
Kata Kunci - Digital Forensik; Tindak Pidana Seksual Daring terhadap Anak; Barang Bukti Digital

I. Pendahuluan

Era digital telah membawa perubahan signifikan terhadap pola interaksi sosial manusia, terutama pada anak dan remaja sebagai generasi digital native. Perkembangan jaringan internet dan media sosial membuka ruang bagi tindak kejahatan siber, termasuk tindak kejahatan seksual terhadap anak secara daring dengan modus (grooming). Pelaku memanfaatkan platform digital seperti media sosial, aplikasi perpesanan, forum diskusi, dan game online.[1] Data dari Kementerian Pemberdayaan Perempuan dan Perlindungan Anak (2021) menunjukkan peningkatan sebesar 23% kasus eksploitasi anak melalui media sosial. UNICEF (2023) melaporkan sekitar 500.000 anak mengalami eksploitasi seksual dan perlakuan tidak pantas di dunia maya. Kejahatan seksual daring terhadap anak sering melibatkan manipulasi korban melalui media sosial seperti WhatsApp, Instagram, dan Telegram.[2] Kasus yang sempat viral pada tahun 2024 melalui akun X @olafaa_ menunjukkan seorang anak perempuan kelas 6 SD dilecehkan oleh pria berusia 20 tahun yang dikenalnya dari game Mobile Legends. Pemilik akun membagikan tangkapan layar dari pembicaraan adik temannya dengan seorang pria, dilihat dari tangkapan layar, pria tersebut memanipulasi korban menggunakan kata-kata yang tidak pantas dan berbau seksual hingga korban akhirnya mengirimkan foto tidak senonoh padanya. Awalnya, pelaku memuji korban setiap hari hingga luluh dan akhirnya meminta foto alat kelamin milik korban. Menurut keterangan akun tersebut, kakak korban telah melaporkan hal ini pada pihak berwajib, namun hingga saat ini masih belum mendapatkan solusi yang diharapkan.

Peran utama dalam menangani kasus ini terletak pada pembuktian dalam penegakan hukum. Pelaku sering menggunakan identitas palsu, bersifat anonim, dan menghapus jejak digital mereka setelah melakukan tindakan grooming. Digital forensik menjadi elemen penting untuk mengungkap bukti elektronik yang sering tersebar di berbagai platform dan memiliki sifat mudah hilang.[2] Pengumpulan bukti digital membutuhkan keahlian forensik digital yang khusus, yang belum dimiliki oleh semua penegak hukum. Hambatan birokrasi dan hukum dalam kerja sama dengan platform digital serta penyedia layanan internet turut memperlambat proses. Kurangnya pemahaman masyarakat dan kecenderungan menyalahkan korban, ditambah batasan perlindungan data dan privasi semakin memperumit proses pengumpulan bukti yang sah dan dapat diterima di pengadilan.[3] Meningkatnya penggunaan teknologi membuat forensik digital menjadi vital untuk mengungkap jejak pelaku.[4] Pembuktian melibatkan verifikasi bukti digital dan interpretasinya secara hukum. Mengingat dampak serius terhadap mental anak, diperlukan sistem hukum yang adaptif dan metode pembuktian yang andal untuk mengatasi kasus grooming online yang semakin meningkat.

Berbagai penelitian terdahulu telah mengkaji isu cyber grooming dan peran digital forensik dalam penegakan hukum, meskipun masing-masing memiliki fokus yang berbeda. Pertama penelitian yang dilakukan oleh Anjeli Holivia dan Teguh **Suratman** dengan judul " Child **Cyber Grooming Sebagai Bentuk Modus Baru Cyber Space Crimes"** Hasil penelitian ini adalah bagaimana penanganan kasus Child Cyber Grooming di Indonesia lebih banyak bersifat preventif daripada represif. Dimana masih banyak memerlukan keterlibatan berbagai elemen masyarakat, terutama orang tua, dalam pengawasan penggunaan media sosial oleh anak-anak.[5] Penelitian terdahulu kedua ditulis oleh Nadhilah Ishmah dengan judul "Meninjau Eksistensi Kebijakan Pemerintah Terhadap Kerentanan Cyber Child Grooming" Hasil penelitian ini menunjukkan kelemahan regulasi yang dinilai tidak efektif karena proses hukum hanya bisa dilakukan jika ada bukti fisik yang menyebar.[6]

Penlitian terdahulu ketiga dilakukan oleh Amsori, Fakhri Awaluddin, dan Momon Mulyana yang berjudul "Tantangan dan Peran Digital Forensik dalam Penegakan Hukum terhadap Kejahatan di Ranah Digital" Hasil penelitian ini menjelaskan bahwa digital forensik memainkan peranan penting dalam pembuktian kasus cybercrime. Meskipun beberapa tahun terkahir mengalami peningkatan jumlah kasus kejahatan siber, salah satunya tindak kejahatan asusila di dunia maya. Dimana penanganan kasus cybercrime lebih kompleks dibandingakan dengan kejahatan konvensional karena membutuhkan keahlian dalam analisis bukti digital, dan seringkali pelaku cybercrime mencoba menghilangkan jejak digital mereka.[7]

Penelitian ini memiliki kebaruan (novelty) dibadingkan dengan penelitian terdahulu dengan menganalisis secara spesifik mengenai penyajian barang bukti digital dalam pembuktian kasus tindak pidana seksual daring terhadap anak. Berbeda dengan penelitian terdahulu yang lebih fokus pada upaya preventif seperti pengawasan masyarakat atau regulasi. Penelitian yang sedang dilakukan saat ini dengan judul “Analisis Yuridis Digital Forensik dalam

Pembuktian Kasus Tindak Pidana Seksual Daring Terhadap Anak" berfokus pada teknik penyajian barang bukti digital yang sesuai dalam peraturan per undang-undangan, serta kendala teknis dalam pengumpulan bukti digital yang tidak banyak diulas dalam literatur sebelumnya.
Penelitian ini bertujuan untuk menganalisis prosedur penyajian bukti digital dalam pembuktian kasus tindak pidana seksual daring terhadap anak, dengan menyoroti tantangan teknis seperti volatilitas bukti digital dan enkripsi, serta metode penyajian informasi yang akurat dalam barang bukti yang akan digunakan di pengadilan. Penelitian ini juga bertujuan untuk mengidentifikasi kendala dalam proses pengumpulan dan analisis bukti digital serta merumuskan rekomendasi strategis guna mengoptimalkan sistem peradilan, termasuk pengembangan metode pembuktian hukum yang adaptif terhadap perkembangan teknologi. Penelitian ini penting, mengingat kasus tindak pidana seksual daring terhadap anak memerlukan pendekatan khusus dalam pembuktian. Bukti digital yang mudah hilang, tersebar di berbagai platform, dan terenkripsi membutuhkan teknik forensik digital yang andal. Kemajuan teknologi menuntut adanya pembaruan dalam metode pengumpulan dan analisis bukti agar tetap selaras dengan sistem peradilan yang berlaku.

Rumusan Masalah
1. Bagaimana bentuk penyajian barang bukti digital sesuai dengan peraturan perundang-undangan terkait tindak pidana pelecehan seksual terhadap anak?Kategori SDGs: Sesuai ketentuan indikator Sustainable Development Goals (SDGs) ke-16 yaitu Peace, Justice, and Strong Institutions.

II. Metode
Penelitian ini menggunakan metode yuridis normatif dengan pendekatan perundang-undangan (Statute Approach) dan penafsiran sistematis, gramatikal, futuristik. Bahan hukum primer meliputi Undang-Undang Nomor 19 Tahun 2016 Perubahan Atas Undang-Undang Nomor 11 Tahun 2008 Tentang Informasi Dan Transaksi Elektronik, Peraturan Pemerintah Nomor 71 Tahun 2019 tentang Penyelenggaraan Sistem dan Transaksi Elektronik (PSTE), RPM KOMINFO, UU Perlindungan Anak Nomor 35 Tahun 2014, KUHP, dan Peraturan Kapolri Nomor 10 Tahun 2009 tentang Barang Bukti Elektronik. Bahan hukum sekunder, seperti literatur, artikel jurnal, buku hukum, dan pendapat ahli yang mendukung penelitian ini. Analisis bahan hukum menggunakan analisa deduktif.
III. Hasil dan Pembahasan
1. Regulasi yang Mengatur Barang Bukti Digital dalam Kasus Pelecehan Seksual Daring terhadap Anak
Perkembangan teknologi meningatkan kerentanan anak terhadap kejahatan seksual daring melalui media sosial, aplikasi pesan, game online, dan platfrom digital lainnya. Khususnya melalui modus child grooming, yaitu manipulasi psikologis yang biasa dilakukan oleh pelaku kepada anak dibawah umur untuk melakukan eksploitasi sexual yang menuntut kejelasan regulasi mengenai keberlakuan barang bukti digital sebagai alat pembuktian dalam proses hukum pidana. Modus ini biasanya diawali dengan orang dewasa yang mengunjungi forum di mana anak-anak sedang berinteraksi, selanjutnya menjalin pertemanan dengan anak muda, kemudian mendapatkan kepercayaan dari anak-anak tersebut dengan cara memberikan perhatian, bujukan, hadiah, dan berbagai macam bentuk perhatian lainnya.[5] Manipulasi tersebut berkembang menjadi hubungan seksual dan berakhir pada pengendalian serta eksploitasi terhadap korban, yang biasanya berujung pada percakapan pornografi. Tindak kejahatan seperti ini dapat menimbulkan tantangan besar dalam proses pembuktian hukum karena barang bukti yang ditinggalkan tidak berwujud fisik, melainkan berbentuk digital dan sering kali berisfat sementara.
Konteks hukum Indonesia khususnya tindak pidana seksual terhadap anak secara daring, alat bukti yang dominan digunakan berupa data digital yang tersimpan dalam perangkat elektronik atau dikirim melalui sistem elektronik. Maka dari itu, pengakuan terhadap barang bukti digital sebagai alat bukti secara sah diatur dalam Undang-Undang Nomor 19 Tahun 2016 tentang perubahan atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (UU ITE), khususnya pada Pasal 5 ayat (1) yang menyatakan bahwa informasi elektronik dan/atau dokumen elektronik dan/atau hasil cetaknya merupakan alat bukti hukum yang sah. Pasal 6 menambahkan bahwa informasi elektronik dianggap setara dengan dokumen tertulis selama informasi di dalamnya dapat diakses, ditampilkan, dijamin keutuhannya, dan dapat dipertanggungjawabkan secara hukum. Penafsiran atas ketentuan ini menekankan pentingnya prinsip integritas dan autentikasi terhadap bukti digital. Oleh karena itu, validitas suatu bukti elektronik tidak hanya ditentukan oleh keberadaannya, melainkan juga oleh prosesdur teknis yang menjamin tidak adanya modifikasi terhadap data sejak pertama kali ditemukan hingga dipresentasikan di pengadilan.
Penguatan konsep ini juga terlihat dalam Perataruran Pemerintah Nomor 71 Tahun 2019 tentang Penyelenggaraan Sistem dan Transaksi Elektronik (PSTE), yang mengatur tata kelola sistem elektronik dan integritas bukti digital dalam penyelenggaraan transaksi elektronik. Penafsiran terhadap ketentuan ini menjelaskan bahwa bukti digital yang diajukan harus berasal dari sistem yang andal dan telah memenuhi standar keamanan informasi. Hal ini berkaitan erat dengan prinsip auditability, yaitu kemampuan suatu sistem untuk ditelusuri dan diaudit integritasnya oleh pihak independen. Sebagai dukungan dalam praktik di lapangan, Rancangan Peraturan Menteri Komunikasi dan Informatika tentang Tata Cara Penanganan Pertama Bukti Elektronik (RPM KOMINFO) mengatur secara teknis bagaimana bukti elektronik harus ditangani agar dapat dipertanggung jawabkan secara hukum. RPM memuat prinsip-prinsip utama bukti elektronik, seperti relevansi, keandalan, dan kecukupan. Bukti elektronik tidak boleh hanya sekedar dapat diakses, tetapi juga harus mencerminkan kondisi autentik, tidak berubah, serta meunjukkan adanya hubungan logis dengan tindak pidana yang sedang diperiksa. Penafsiran terhadap prinsip ini mengharuskan adanya dokumentasi forensik yang komprehensif serta keterlibatan tenaga ahli dalam proses validasi.
Undang-Undang Nomor 35 Tahun 2014 tentang Perlindungan Anak, khususnya Pasal 76E, melarang setiap orang melakukan atau membiarkan terjadinya perbuatan cabul terhadap anak, baik melalui kekerasan, tipu muslihat, bujukan, maupun dalam bentuk komunikasi digital. Penafsiran terhadap ketentuan ini memperluas seksual eksplisit melalui media sosial atau aplikasi pesan yang dapat dikualifikasikan sebagai tindakan piadan. Konteks pembuktian bukti elektronik seperti pesan teks, gambar, video, tangkapan layar, hingga metadata dari media sosial dapat menjadi alat pembuktian dalam menjerat pelaku. Pengaturan teknis lebih lanjut mengenai barang bukti digital juga dapat ditemukan dalam Peraturan Kepala Kepolisian Negara Republik Indonesia Nomor 10 Tahun 2009 tentang Tata Cara dan Persyaratan Pengelolaan Barang Bukti Elektronik di Lingkungan Kepolisian Negara Republik Indonesia. Penafsiran terhadap regulasi ini mengatur secara rinci mengenai standar prosedur dalam penanganan barang bukti digital, mulai dari proses identifikasi, pengamanan, penyimpanan, hingga penyajiannya di persidangan. Tujuan utama dari regulasi ini adalah untuk menjaga keaslian (authenticity), integritas (integrity), dan keutuhan (completeness) barang bukti elektronik.[8]
Kitab Undang-Undang Hukum Acara Pidana (KUHAP), melalui Pasal 184 ayat (1) adalah suatu bentuk pengakuan yuridis atas bukti digital yang dapat dikaji dari sudut hukum acara pidana. Sistem ini menyebutkan bahwa alat bukti yang sah meliputi: keterangan saksi, keterangan ahli, surat, petunjuk, dan keterangan terdakwa. Dalam praktiknya, informasi atau dokumen elektronik dapat dikategorikan sebagai alat bukti berupa "surat" atau "petunjuk", apabila diperoleh melalui prosedur yang sah dan dapat dipertanggungjawabkan sesuai dengan ketentuan hukum acara pidana.
Selain ketentuan nasional, dalam praktik penanganan kasus oleh aparat penegak hukum keberadaan Standart Nasional Indonesia (SNI) dan standart internasional seperti ISO/IEC 27037 tentang " Guidelines for Identification, Collection, Acquisition and Preservation of Digital Evidence". ISO memberikan pedoman untuk identifikasi, koleksi, akuisisi, dan preservasi alat bukti digital yang sah, mulai dari tahap pertama pengambilan bukti di

tempat kejadian perkara hingga proses analisis di laboratorium forensik. Dalam rangka menjawab tantangan perkembangan teknologi dan kejahatan siber, dibutuhkan sinkronisasi antara hukum positif nasional dan best practice internasional.[9] Penafsiran terhadap ISO ini adalah bahwa setiap tahapan penanganan bukti digital harus mengikuti standar yang dapat diverifikasi, direproduksi, dan diaudit oleh pihak ketiga sebagai bentuk jaminan objektivitas dan legalitas. Oleh karena itu, dapat disimpulkan bahwa regulasi pengakuan barang bukti digital dalam perkara kejahatan seksual daring terhadap anak telah tersedia dalam bentuk hukum positif nasional. Namun, masih dibutuhkan sinkronisasi antara **regulasi yang ada dengan praktik di lapangan,** terutama dalam menguatkan kapasitas aparat penegak hukum dalam memahami, mengelola, dan mempertanggungjawabkan alat bukti digital secara sah di pengadilan.

2. Bentuk dan Jenis Barang Bukti Digital dalam Tindak Pidana Seksual Daring Terhadap Anak

Tindak pidana seksual daring terhadap anak, pelaku sering memanfaatkan ruang-ruang digital seperti media sosial, aplikasi pesan, dan forum daring untuk melakukan pendekatan, manipulasi emosional, hingga eksploitasi seksual terhadap korban.[10] Dengan demikian, barang bukti digital menjadi instrumen utama dalam mengungkap dan membuktikan kejahatan tersebut di hadapan hukum. Maka dari itu, barang bukti digital menjadi komponen utama dalam proses pembuktian hukum. Berikut bentuk-bentuk barang bukti digital dalam konteks ini meliputi:

1. Tangkapan layar (screenshot) percakapan.
2. Metadata file yang memuat informasi teknis seperti tanggal pembuatan, lokasi GPS, dan jenis perangkat.
3. Clone disk atau salinan menyeluruh dari perangkat elektronik.
4. Log aktivitas dari sistem atau aplikasi yang menunjukkan pola penggunaan dan interaksi daring.
5. Rekaman video/audio termasuk voice note atau panggilan video.
6. URL permanen dari konten atau akun yang terkait dengan tindak pidana.
7. Konten cloud yang tersimpan pada penyimpanan digital daring.

Keberadaan barang bukti digital harus didukung oleh dokumentasi dan prosedur forensik yang sesuai dengan standar, salah satunya adalah ISO/IEC 27037. Standar ini mengatur proses mulai dari identifikasi, koleksi, akuisisi, hingga preservasi barang bukti elektronik. Barang bukti yang tidak diperoleh atau disimpan sesuai prosedur berisiko dinyatakan tidak sah di pengadilan. Sebagai contoh konkret, kasus yang sempat viral pada tahun 2024 melalui akun media sosial X (Twitter) dengan nama pengguna @olafaa_ nyata bagaimana barang bukti seperti tangkapan layar percakapan dapat tersebar luas namun belum tentu sah secara hukum jika tidak didukung dengan prosedur forensik yang memadai. Kasus ini mempertegas pentingnya penggunaan metode forensik yang sesuai seperti clone disk dan pengumpulan metadata untuk memperkuat posisi alat bukti di mata hukum.

Keberadaan barang bukti dalam praktik hukum harus memenuhi prinsip keotentikan dan integritas agar dapat diterima di persidangan. Barang bukti digital seperti tangkapan layar, metadata, atau rekaman elektronik dapat dikualifikasikan sebagai alat bukti yang sah sepanjang diperoleh melalui cara yang sah dan memenuhi ketentuan hukum acara. Berdasarkan **Pasal 184 ayat (1) KUHAP,** bukti digital dapat **dikategorikan sebagai alat bukti** berupa surat atau petunjuk, tergantung pada bentuk, isi, dan cara penyajiannya. Barang bukti digital dalam perkara kejahatan seksual daring memiliki karakteristik yang kompleks dan mudah diubah, sehingga memerlukan penanganan khusus. Klasifikasi jenis bukti harus dilakukan secara hati-hati, dan teknik pengumpulan harus mengikuti standar forensik agar tidak terjadi kontaminasi atau keraguan atas keasliannya.[11]

3. Validitas dan Kekuatan Alat Bukti Digital di Mata Hukum

Sistem pembuktian hukum pidana Indonesia, alat bukti harus memenuhi unsur keabsahan formil dan materiil agar dapat diterima dan dipertimbangkan oleh hakim dalam proses peradilan. Seiring berkembangnya kejahatan berbasis elektronik, termasuk dalam tindak pidana seksual daring terhadap anak, maka alat bukti digital harus dinilai secara khusus, baik dari sisi bentuk maupun kekuatan pembuktiannya. Dalam hal ini, klasifikasi level kekuatan alat bukti digital menjadi penting sebagai panduan bagi aparat penegak hukum untuk menilai sejauh mana bukti tersebut dapat diandalkan. Secara normatif, dalam kerangka hukum acara pidana, barang bukti digital dapat dikualifikasikan ke dalam tiga tingkatan kekuatan pembuktian, yakni: bukti indikatif, bukti pendukung, dan bukti konklusif. Klasifikasi ini tidak hanya mencerminkan bobot nilai pembuktian dari setiap alat bukti, tetapi juga menentukan sejauh mana bukti digital tersebut dapat diterima dan dijadikan dasar pertimbangan hukum oleh hakim dalam proses peradilan pidana.[12]

Pertama, yang dimaksud dengan bukti indikatif adalah bentuk awal dari barang bukti digital yang berfungsi sebagai petunjuk atau indikasi adanya dugaan tindak pidana. Bukti ini bersifat permulaan dan belum memiliki daya pembuktian yang berdiri sendiri untuk membuktikan unsur-unsur delik secara lengkap. Contoh dari bukti indikatif antara lain, tangkapan layar (screenshot) percakapan elektronik, alamat URL dari situs atau akun media sosial yang terindikasi digunakan untuk melakukan perbuatan pidana, atau cuplikan konten digital yang beredar di publik namun belum melalui proses validasi. Tangkapan layar atau foto percakapan elektronik sendiri hanya dapat dianggap sebagai bukti permulaan apabila tidak diperkuat dengan proses digital forensik yang sah, karena sifatnya yang mudah dimanipulasi dan tidak terverifikasi keasliannya.[13] URL yang tidak dipermanenkan melalui mekanisme seperti web archive atau hash validation juga hanya berfungsi sebagai petunjuk awal, bukan bukti hukum yang berdiri sendiri.[14] Praktik penyidikan bukti indikatif kerap digunakan sebagai dasar untuk melakukan tindakan awal penyelidikan, namun belum cukup kuat untuk dijadikan dasar penetapan tersangka secara yuridis tanpa dukungan dari bukti lainnya yang lebih kuat.[15]

Kedua, bukti pendukung adalah barang bukti digital yang digunakan untuk menguatkan atau menegaskan bukti utama yang telah diperoleh secara sah. Bukti ini tidak memiliki kedudukan utama, namun berperan penting dalam memperkuat logika hukum pembuktian, yang termasuk dalam kategori ini misalnya metadata dokumen elektronik, log aktivitas sistem perangkat digital, data lokasi (geolocation), dan riwayat komunikasi daring, yang diperoleh melalui proses forensik digital yang sah.[16] Kekuatan pembuktian bukti pendukung akan meningkat secara signifikan apabila diperoleh dan diproses berdasarkan prosedur forensik yang sesuai standar internasional, seperti ISO/IEC 27037, dan didukung dengan rekam jejak prosedural yang dapat diaudit. Metadata dan log file sendiri merupakan sumber informasi yang kritikal dalam menyusun kembali peristiwa digital, selama akuisisinya dilakukan dengan teknik forensik yang sah dan terdokumentasi.[17]

Ketiga, bukti konklusif adalah barang bukti digital yang telah diperoleh melalui prosedur yang sah secara hukum dan forensik, yang memiliki kekuatan pembuktian tertinggi karena memenuhi prinsip-prinsip keutuhan (integrity), keaslian (authenticity), dan keterkaitan langsung dengan unsur tindak pidana (relevance). Bukti ini diperoleh melalui metode akuisisi forensik seperti clone disk dalam bentuk bitstream image, diverifikasi melalui hash value (misalnya SHA-256), serta didokumentasikan melalui sistem chain of custody yang terdokumentasi secara lengkap.[18] Praktik peradilan pidana, bukti konklusif mampu berdiri sendiri sebagai dasar hukum untuk menetapkan seseorang sebagai tersangka atau terdakwa. Misalnya, salinan forensik dari perangkat pelaku, file digital yang ditemukan dalam cloud storage atau dokumen elektronik hasil intersepsi yang dilakukan secara sah oleh penyidik, dapat dijadikan alat bukti utama yang sangat menentukan hasil pembuktian di pengadilan.[19] Menguatkan bahwa proses akuisisi yang mengikuti standar ISO/IEC 27037 memungkinkan data yang diambil dari penyimpanan daring (cloud) memiliki validitas tinggi sebagai bukti utama, dapat disimpulkan bahwa clone disk berbasis bit-by-bit acquisition memberikan salinan bukti digital yang lengkap dan dapat diverifikasi, sehingga tidak dapat dengan mudah disangkal keabsahannya di pengadilan.[20]

Berdasarkan sudut pandang hukum acara pidana dan berdasarkan ketentuan **Pasal 5 dan Pasal 6 Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik, sebagaimana telah diubah dengan Undang-Undang Nomor 19 Tahun 2016,** maka alat bukti digital dapat dikatakan sah apabila diperoleh melalui prosedur yang menjamin keutuhan dan pertanggungjawaban hukum. Berdasarkan pertimbangan tersebut, berikut ini disajikan Tabel 1 yang memuat jenis-jenis barang bukti digital, sumber atau medianya, keterangan fungsionalnya, serta tingkat validitasnya menurut prinsip pembuktian hukum pidana dan standar forensik digital:

No	Jenis Barang Bukti Digital	Contoh Media/Sumber	Keterangan	Tingkat Validitas
1.	Tangkapan layar percakapan	WhatsApp, Instragram, Telegram	Gambar digital dari isi percakapan	Indikatif
2.	Metadata File digital, log perangkat		Berisi data teknis seperti waktu, lokasi, perangkat	Pendukung
3.	Clone Disk	Smartphone, laptop, HDD	Salinan bitstream dari seluruh isi perangkat	Konklusif
4.	URL permanen	Media sosial, forum online	Tautan ke konten digital yang telah diarsipkan	Indikatif - Pendukung
5.	Log aktivitas	Aplikasi, sistem server	Jejak interaksi pengguna dengan sistem atau aplikasi	Pendukung
6.	Rekaman audio/video	Voice note, video call	File multimedia dari komunikasi antara pelaku-korban	Pendukung
7.	Konten cloud	Google Drive, Dropbox	File daring yang diunggah/diunduh oleh pelaku	Konklusif

Tabel 1. Jenis barang bukti dan tingkat validitasnya

4. Teknik Permanenisasi URL dan Validasi Bukti Elektronik

Perkara kejahatan seksual daring terhadap anak, konten bukti digital tidak selalu tersimpan secara lokal pada perangkat, melainkan banyak ditemukan dalam bentuk tautan atau URL yang mengarah ke konten daring, seperti unggahan media sosial, forum, atau situs tertentu. Karena sifatnya yang dinamis dan mudah dihapus, bukti dalam bentuk URL memerlukan tindakan permanenisasi untuk menjamin keutuhannya sebagai alat bukti yang sah.[21] Permanenisasi URL adalah proses mengarsipkan konten digital dari suatu alamat situs atau platform agar dapat diakses kembali dalam bentuk yang tetap, meskipun konten aslinya telah dihapus atau dimodifikasi. Proses ini dilakukan untuk memastikan bahwa isi dari URL tetap dapat ditelusuri dan diverifikasi pada saat dibutuhkan dalam proses pembuktian. Langkah-langkah permanenisasi umumnya meliputi:

1. Pengambilan tangkapan layar secara menyeluruh dari konten yang ditautkan oleh URL.
2. Penyimpanan metadata waktu akses, IP pengakses, dan alamat lengkap URL.
3. Penggunaan layanan arsip web seperti Archive.today, WebPreserver, atau Hunchly untuk mengarsipkan versi statis dari halaman.
4. Pencatatan hash value dari file hasil arsip untuk menjaga keutuhan dan validitas data.
5. Penyimpanan hasil arsip ke dalam media digital yang aman dan dapat diverifikasi.

Praktik hukum di Indonesia belum secara spesifik mengatur permanenisasi URL belum secara spesifik diatur dalam undang-undang, namun proses ini dapat dianggap sebagai bagian dari akuisisi dan preservasi barang bukti digital sebagaimana tercakup dalam ISO/IEC 27037 dan didukung melalui prinsip integritas bukti yang dijelaskan dalam Pasal 6 UU ITE. Hal ini diperkuat pula dengan ketentuan dalam Rancangan Peraturan Menteri Komunikasi dan Informatika tentang Tata Cara Penanganan Pertama Bukti Elektronik yang mewajibkan setiap tindakan pengamanan bukti elektronik harus dilakukan secara terdokumentasi dan dapat diaudit. Permanenisasi menjadi krusial ketika bukti digital berupa URL menjadi satu-satunya rujukan yang dapat menunjukkan komunikasi atau tindakan pelaku. Tanpa proses permanenisasi, tautan URL berisiko tidak dapat diverifikasi di kemudian hari karena konten sudah dihapus atau tidak lagi tersedia secara publik. Permanenisasi URL bukan hanya tindakan teknis semata, melainkan juga menjadi bentuk perlindungan hukum terhadap validitas bukti digital. Penyidik dan pihak yang berkepentingan dalam penegakan hukum perlu memahami pentingnya metode ini agar tidak kehilangan alat bukti krusial yang dapat membuktikan unsur tindak pidana secara tepat di hadapan hukum.[22]

5. Tahapan dan Prinsip Digital Forensik Berbasis ISO/IEC 27037

Pembuktian dalam hukum pidana merupakan salah satu kebijakan **kriminal sebagai science of response yang** mencakup bermacam disiplin **ilmu. Hal ini disebabkan oleh luasnya kuasa** serta tipe kejahatan yang terjadi pada **teknologi** informasi. Seringkali **penegak hukum di Indonesia mengalami kesulitan** untuk memberikan hukuman kepada pelaku **kejahatan** pelecehan sexual daring terhadap anak karena bukti tidak memenuhi syarat ketentuan sistem peradilan pidana di Indonesia. Sementara upaya penjeratan terhadap para pelaku kejahatan sexual daring terhadap anak harus tetap dilakukan. Proses digital forensik menjadi penting dilakukan dalam penyajian bukti elektronik yang sah dan dapat diterima di pengadilan.[23]

Digital forensik tidak hanya **dapat digunakan untuk mengungkap bukti kejahatan digital tapi kejahatan konvensional yang memiliki barang bukti elektronik.** Digital forensik adalah serangkaian prosedur dalam mengumpulkan, menganalisis, dan membuat laporan dalam data digital untuk mendukung proses penegakan hukum. Bidang forensik digunakan untuk menyelidiki kejahatan menggunakan ilmu yang terkait dengan bukti digital. Meskipun tidak berfungsi sebagai alat bukti langsung, digital forensik membantu penegak hukum dalam proses penegakannya. Dalam pelaksanaan digital forensik, proses pengelolaannya harus dilakukan sesuai dengan standar yang diakui secara internasional, sebagaimana dijelaskan dalam ISO/IEC 27037 yang memberikan panduan teknis mengenai proses identifikasi, koleksi, akuisisi, dan preservasi bukti digital.

Tahap pertama adalah identifikasi, yaitu proses menentukan dan mengenali perangkat digital atau sistem yang diduga mengandung informasi yang relevan dengan tindak pidana. Pada tahap ini, penyidik mencatat lokasi barang bukti, jenis perangkat, status perangkat (aktif atau mati), dan kondisi fisiknya.[24] Identifikasi dilakukan sejak di tempat kejadian perkara dan menjadi fondasi awal dari keseluruhan proses forensik. Setelah identifikasi, dilanjutkan dengan koleksi atau pengumpulan barang bukti digital. Koleksi dilakukan dengan mengamankan perangkat dari tempat kejadian perkara secara hati-hati untuk menghindari perubahan data. Semua proses dilakukan secara terdokumentasi, termasuk pencatatan waktu, pengambilan gambar perangkat, dan pengemasan dalam wadah anti-statis sesuai prosedur.[21]

Langkah berikutnya adalah akuisisi, yaitu proses pembuatan salinan data digital secara menyeluruh (bitstream image) dari perangkat yang telah dikoleksi. Akuisisi dilakukan menggunakan write-blocker agar data asli tidak berubah selama proses penyalinan. Setelah salinan selesai dibuat, dilakukan verifikasi dengan menghitung hash value (seperti MD5 atau SHA-256) untuk memastikan bahwa salinan tersebut identik dengan data aslinya.[25] Tahap terakhir adalah preservasi, yakni penyimpanan barang bukti digital dan salinannya dalam media penyimpanan yang aman dan tahan gangguan. Penyimpanan ini harus menjamin keutuhan data hingga tahap persidangan, serta dilengkapi dengan dokumentasi lengkap seperti chain of custody dan daftar siapa saja yang memiliki akses terhadap bukti tersebut.

Keempat tahapan ini harus dilakukan secara sistematis, terdokumentasi, dan sesuai dengan prosedur agar barang bukti digital memiliki kekuatan pembuktian yang tidak diragukan. Apabila salah satu tahapan tidak dijalankan dengan benar, maka risiko batalnya alat bukti dalam proses peradilan menjadi sangat tinggi. Standar ISO/IEC 27037 memberikan pedoman sistematis dalam menangani bukti digital yang sah. Untuk menggambarkan proses ini secara visual, berikut disajikan Gambar 1 yang menggambarkan alur proses identifikasi, koleksi, akuisisi, dan preservasi bukti digital:

Gambar 1. Flowchart Alur Tahapan Digital Forensik

Melalui Gambar 1 tersebut, dapat dipahami bahwa setiap tahap harus dilaksanakan dengan dokumentasi yang lengkap agar memenuhi prinsip chain of custody. Tahapan digital forensik berbasis ISO/IEC 27037 merupakan pedoman teknis yang sekaligus berfungsi sebagai jaminan integritas dan legalitas alat bukti elektronik dalam proses hukum pidana, khususnya dalam menangani kejahatan seksual daring terhadap anak. Mengikuti tahapan dalam SNI ISO/IEC 27037, proses digital forensik di Indonesia dapat dilaksanakan secara profesional dan sesuai standar internasional. Hal ini akan meningkatkan kepercayaan pengadilan terhadap bukti digital dan mendukung efektivitas pembuktian dalam perkara tindak pidana seksual daring **terhadap** anak. Oleh **karena itu,** mengikuti tahapan digital forensik berdasarkan ISO/IEC 27037 dan didukung dengan prinsip-prinsip dasar yang diterapkan secara disiplin, barang bukti digital dapat disajikan secara sah, akurat, dan dapat digunakan untuk membuktikan tindak pidana pelecehan seksual daring terhadap anak. Standarisasi ini menjadi bagian penting dalam penegakan hukum modern yang berbasis teknologi.

Mengikuti tahapan digital forensik berdasarkan ISO/IEC 27037, aparat penegak hukum dapat memastikan bahwa barang bukti digital yang diperoleh memiliki validitas hukum tinggi. Proses ini menjadi kunci untuk menghadirkan keadilan dalam perkara kejahatan seksual daring terhadap anak. Teknik permanenisasi URL merupakan langkah krusial dalam mempertahankan keabsahan konten digital sebagai alat bukti.[27] Tanpa metode ini, bukti dari dunia maya tidak memiliki kekuatan hukum yang memadai untuk mendukung pembuktian di pengadilan pidana. Bukti digital seperti tangkapan layar dan metadata hanya dapat dianggap sah jika diperoleh melalui metode yang dapat diverifikasi dan diaudit. Oleh karena itu, clone disk menjadi bentuk bukti digital yang paling kuat dan wajib digunakan dalam proses pembuktian pidana, terutama dalam perkara seksual daring terhadap anak.[28]

Standar Operasional Prosedur (SOP) formal untuk investigasi digital forensik belum tersedia. Penegak hukum telah mengembangkan berbagai metode guna menstandarkan proses, dan organisasi seperti International Standardization Organization (ISO) mulai menyusun kerangka tersebut.[23] Standarisasi ini diharapkan dapat memberikan pedoman yang lebih jelas dan seragam dalam pelaksanaan digital forensik diberbagai negara. Digital forensik terbukti penting dalam investigasi modern, baik untuk kejahatan digital maupun konvensional. Prosesnya yang berlandaskan pada prinsip-prinsip dasar, tahapan yang terstruktur, serta penggunaan barang bukti elektronik yang valid, menjadikan digital forensik sebagai elemen yang tak terpisahkan dalam penegakan hukum di era teknologi ini.

6. Prosedur Clone Disk dan Validitasnya dalam Pembuktian

Proses pembuktian tindak pidana seksual daring terhadap anak, integritas barang bukti digital menjadi sangat penting. Salah satu metode utama yang digunakan dalam pengamanan dan akuisisi barang bukti digital adalah prosedur clone disk, yaitu penyalinan yang dilakukan secara menyeluruh dari perangkat penyimpanan yang diduga mengandung data relevan. Prosedur ini tidak hanya digunakan untuk menjaga keutuhan data, tetapi juga memastikan bahwa salinan tersebut dapat diterima sebagai alat bukti yang sah secara hukum. Clone disk adalah proses pembuatan salinan identik dari seluruh isi media penyimpanan seperti hard disk, SSD, atau perangkat seluler dalam bentuk bitstream image. Berbedaa dengan penyalinan file biasa, salinan bitstream mencakup seluruh sektor penyimpanan, termasuk data yang telah dihapus (delate files), ruang tidak teralokasi (unallocated space), partisi tersembunyi, serta metadata sistem file. Oleh karena itu, metode ini mampu menduplikasikan bukti digital secara menyeluruh tanpa resiko mengubah atau merusak data asli.[16]

Secara forensik, prosedur clone disk dapat mengikuti beberapa tahapan penting yang harus dilakukan oleh penyidik atau tenaga ahli digital forensik yang memiliki otoritas. Langkah pertama dalam proses ini adalah persiapan dan pengamanan perangkat digital yang diperlukan, termasuk perangkat lunak maupun keras dan media yang akan di cloning oleh penyidik, menggunakan writer-blocker agar media asli tidak dapat ditulis atau dimodifikasi pada saat proses akuisisi. Tahap berikutnya adalah proses cloning menggunakan perangkat forensik yang telah disiapkan untuk membuat salinan bit-by-bit dari media penyimpanan asli ke media tujuan, mencakup semua data termasuk file yang telah dihapus. Setelah cloning dilakukan, proses verifikasi dilakukan dengan menghitung dan mencocokkan nilai hash (misalnya SHA-256 atau MD5) dari media asli dan hasil salinan. Kemudian dilakukan penyimpanan hasil clone dalam media digital yang aman serta pencatatan prosedur secara rinci dalam formulir dokumentasi atau berita acara pemeriksaan untuk memastikan tidak terjadi perubahan bit data selama proses akuisisi.[29] Berikut disajikan Gambar 2 untuk memperjelas langkah-langkah prosedur clone disk:

Gambar 2. Flowchart Alur Tahapan Digital Forensik

Seluruh proses ini tidak hanya bersifat teknis, tetapi juga harus terdokumentasi secara administratif sebagai bagian dari prinsip chain of custody. Dokumentasi ini menjadi alat pembuktian bahwa barang bukti digital yang diajukan di persidangan tidak mengalami perubahan, kehilangan, atau kontaminasi sejak pertama kali ditemukan hingga digunakan di pengadilan.[11] Dalam konteks hukum di Indoneisa, prosedur clone disk sejalan dengan ketentuan **Pasal 5 dan Pasal 6 Undang-Undang Informasi dan Transaksi Elektronik (UU ITE),** yang **menyatakan bahwa informasi elektronik dan/atau dokumen elektronik serta hasil cetaknya adalah alat bukti hukum yang sah,** selama dapat dibuktikan keutuhannya dan dapat dipertanggungjawabkan. Hal ini diperkuat dengan Rancangan Peraturan Menteri Komunikasi dan Informatika tentang Tata Cara Penanganan Pertama Bukti Elektronik, yang menegaskan bahwa proses akuisisi dan analisi bukti digital harus dapat diuji secara teknis dan audit secara hukum.[30]

Apabila clone disk dilakukan tanpa prosedur yang sah, atau tanpa dokumentasi lengkap, maka keabsahan alat bukti tersebut dapat dengan mudah digugurkan dalam persidangan. Begitupun sebaliknya, jika dibuat dengan prosedur standart yang benar dan dapat diverifikasi melalui hash value serta laporan forensik resmi, clone disk memiliki kedudukan sebagai alat bukti konklusif. Salinan ini juga dapat mengungkap bukti penting seperti riwayat komunikasi pelaku, pengunduhan file ilegal, serta aktivitas digital lainnya yang mendukung unsur tindak pidana. Prosedur clone disk yang mengikuti standar internasional dan praktik forensik yang sah merupakan fondasi penting dalam menjaga keabsahan serta kekuatan pembuktian dari barang bukti digital. Pada kasus kejahatan seksual daring terhadap anak, prosedur ini sering kali menjadi satu-satunya cara untuk membuktikan keterlibatan pelaku secara digital, sehingga menjadikannya krusial dalam proses peradilan yang adil dan akuntabel.

7. Proses Akuisisi dan Pengamanan Bukti (Chain of Custody)

Seperti yang telah dijelaskan dalam hukum acara pidana, setiap alat bukti yang diajukan kepengadilan harus memiliki unsur keabsahan secara formil dan materil. Berlaku terhadap barang bukti digital dalam perkara tindak pidana seksual daring terhadap anak. Salah satu prinsip penting yang menjamin keabsahan barang bukti digital adalah chain of custody, yaitu dokumentasi menyeluruh dan terverifikasi atas setiap tahapan penguasaan, pemindahan, dan penyimpanan barang bukti sejak pertama kali ditemukan hingga dihadirkan di persidangan.[31] Secara umum, chain of custody berfungsi untuk memastikan bahwa barang bukti digital yang diharapkan adalah bukti yang sama seperti saat pertama kali ditemukan oleh penyidik, tanpa adanya perubahan, kerusakan, atau manipulasi. Prinsip ini sangat krusial dalam konteks digital karena data elektronik sangat mudah untuk diubah, dipindahkan, atau dimodifikasi secara tidak sah tanpa jejak fisik yang jelas. Untuk memvisualisasikan, berikut disajikan Gambar 3 mengenai alur proses chain of custody:

Gambar 3. Proses Chain of Custody

Proses chain of custody sendiri meilputi beberapa aspek utama. Tahap pertama pengumpulan data (data collection), proses ini melibatkan identifikasi, termasuk penandaan perangkat (labeling), pencatatan nomor seri, jenis media, serta lokasi dan waktu perolehan data dari semua sumber yang memungkinkan untuk menjaga integritas data dan bukti yang dikumpulkan. Kedua, pemeriksaan (examination), yaitu proses dokumentasi segala proses yang dilakukan. Pengambilan gambar layar selama proses berlangsung, serta pencatatan siapa yang pertama kali mengakses dan menangani bukti tersebut, dan siapa saja yang terlibat dalam alih tangannya dari satu pihak ke pihak lainnya, termasuk tanggal dan waktu.[32] Ketiga, analisis (analysis), yaitu memberikan hasil dari tahapan pemeriksaan. Pada tahap ini metode dan teknik yang dapat dibenarkan secara hukum digunakan untuk memperoleh informasi yang berguna guna menjawab pertanyaan yang diajukan dalam kasus tertentu. Keempat pelaporan (reporting), yaitu proses dokumentasi dari tahap pemeriksaan dan analisis, di mana seluruh dokumentasi harus dapat ditelusuri kembali dan diaudit oleh pihak independen jika diperlukan. Dokumen chain of custody biasanya dituangkan dalam formulir yang berisi informasi sebagai berikut:

1. Deskripsi media penyimpanan (jenis, kapasitas, kondisi).
2. Tanggal dan waktu penemuan/pengambilan.
3. Nama dan tanda tangan petugas forensik atau penyidik.
4. Catatan serah terima (transfer history) antar pihak.
5. Lokasi penyimpanan dan log akses.

Praktik internasional menempatkan chain of custody sebagai elemen yang tidak dapat ditawar dalam proses digital forensik. Hal ini juga tercermin dalam ISO/IEC 27037 yang menekankan pentingnya maintaining a documented chain of custody sebagai bagian dari prinsip integritas dan akuntabilitas. Di Indonesia, meskipun belum ada aturan eksplisit dalam KUHAP yang menyebut istilah chain of custody secara langsung, prinsip ini tetap dapat diterapkan berdasarkan asas keabsahan alat bukti, terutama dalam penerapan Pasal 5 dan 6 UU ITE dan berdasarkan asas umum hukum acara pidana.[33] Jika chain of custody tidak diterapkan dengan benar, maka barang bukti digital bisa dianggap cacat secara hukum karena tidak dapat dipastikan bahwa data tersebut belum mengalami perubahan. Hal ini dapat dimanfaatkan oleh pihak pembela untuk mengajukan keberatan terhadap keabsahan bukti, yang pada akhirnya dapat mengakibatkan alat bukti tersebut ditolak oleh hakim.

Untuk memperjelas prosedur pengamanan dan dokumentasi bukti digital melalui sistem chain of custody, berikut ini disajikan flowchart alur yang menggambarkan tahapan secara berurutan dan terdokumentasi bagaimana barang bukti digital dilakukan melalui proses chain of custody.[11] Proses akuisisi dan pengamanan barang bukti digital melalui mekanisme chain of custody merupakan syarat mutlak dalam pembuktian perkara tindak pidana berbasis elektronik. Implementasi yang tepat tidak hanya menjaga kekuatan pembuktian, tetapi juga mencerminkan proses hukum yang adil, transparan, dan dapat dipertanggungjawabkan.

8. Kendala dalam Pengumpulan dan Penyajian Bukti Digital

Bukti digital diakui sebagai alat bukti yang sah dalam sistem peradilan, proses pengumpulan dan penyajiannya dalam kasus kejahatan seksual daring terhadap anak masih menghadapi berbagai tantangan, baik dari segi teknis internal maupun eksternal. Salah satu kendala teknis internal adalah keterbatasan pemahaman dan keahlian penyidik dalam bidang teknologi informasi akibat kurangnya tenaga ahli digital forensik. Sumber daya manusia yang kompeten sangatlah penting untuk memastikan kelancaran proses penyelidikan, penyidikan, hingga penangkapan pelaku.[34] Kurangnya pelatihan dan standarisasi prosedur bagi aparat penegak hukum juga menjadi tantangan tersendiri, tidak semua penyidik memiliki keterampilan dalam menganalisis bukti digital, padahal kejahatan seksual daring terhadap anak semakin marak terjadi. Ketidakseimbangan antara jumlah kasus dan tenaga ahli yang tersedia menghambat proses penyelidikan dan penyidikan, bahkan menyebabkan banyak kasus tidak terungkap.

Lambatnya proses penyidikan dan penuntutan akibat keterbatasan akses terhadap alat bukti juga menjadi kendala signifikan. Proses hukum yang berkepanjangan dapat menghambat keadilan bagi korban.[35] Keterbatasan fasilitas dan teknologi forensik memperburuk situasi, terutama dalam pengumpulan bukti kejahatan seksual daring terhadap anak. Kurangnya pemahaman penyidik dalam menangani kasus ini, terutama dalam akuisisi, analisis, serta penyajian bukti digital, turut memperumit proses penyidikan. Berbeda dengan barang bukti fisik dalam tindak pidana konvensional, barang bukti digital memerlukan perlakuan khusus. Kesalahan dalam penaganan software, seperti mematikan atau mencabut perangkat elektronik yang digunakan pelaku dapat mengakibatkan hilangnya bukti yang tersimpan, sementara kode enkripsi yang telah diatur oleh pelaku dapat mengubah atau menghilangkan data saat diakses oleh penyidik.[36]

Kendala eksternal dalam mengumpulkan bukti digital kasus kejahatan seksual daring terhadap anak memperoleh kesulita, menyebabkan proses penyelidikan dan penyidikan terhenti. Kejahatan siber menyebabkan Tempat Kejadian Perkara (TKP) berada di ranah digital, penyidik harus melakukan penelusuran secara daring dan bekerja sama dengan berbagai instansi. Jika bukti yang diperoleh tidak cukup, proses penyelidikan terpaksa dihentikan. Anonimitas dan identitas palsu yang digunakan oleh pelaku juga menjadi hambatan besar. Pelaku dengan mudah membuat akun menggunakan nama dan alamat palsu, berpindah tempat, serta menggunakan perangkat canggih untuk menghindari pelacakan. Penyidik juga kesulitan mengakses isi komunikasi karena enkripsi end-to-end yang diterapkan oleh banyak platform digital dapat memperumit penyidikan.[37] Pelaku sering kali menghapus jejak digital, seperti membuang kartu SIM atau menggunakan fitur pesan yang dapat terhapus secara otomatis, seperti dalam aplikasi WhatsApp dan Telegram. Fragmentasi data memperparah situasi, sebab bukti digital tersebar dalam berbagai format dan perangkat, seperti tangkapan layar, metadata file, rekaman video, serta data yang tersimpan di cloud. Penyidik harus mampu menghubungkan berbagai elemen ini agar bukti dapat tersusun secara utuh dan diterima di pengadilan.

Aparat penegak hukum menerapkan berbagai langkah teknis, baik internal maupun eksternal. Secara internal, peningkatan kapasitas sumber daya manusia menjadi prioritas, dengan memberikan pelatihan kepada penyidik agar mampu menangani kasus kejahatan siber secara profesional. Penguatan sarana dan prasarana investigasi digital seperti perangkat lunak forensik digital serta sistem pemantauan aktivitas daring, sangat diperlukan guna mendukung investigasi yang lebih efektif. Dalam proses penyelidikan, penyidik harus mampu mengenali barang bukti elektronik di TKP dan memastikan prosedur penyitaan yang tepat agar tidak merusak atau menghilangkan data digital. Pengamanan bukti dilakukan melalui dokumentasi awal, pencatatan dalam berita acara penyitaan, serta pembungkusan bukti sesuai standar. Penyidik harus segera mengamankan perangkat sebelum tersangka dapat mengaksesnya, serta melakukan penggeledahan menyeluruh terhadap barang yang berkaitan. Dalam beberapa kasus, penyitaan akun media sosial, email, atau situs web yang digunakan oleh pelaku juga diperlukan, termasuk pelacakan alamat IP untuk mengetahui lokasi perangkat yang digunakan. Kerja sama dengan berbagai pihak menjadi langkah penting dalam mengatasi kendala eksternal. Kolaborasi dengan Kementerian Komunikasi dan Informatika serta Internet Service Provider (ISP) diperlukan untuk mendeteksi dan menghapus konten ilegal.[38] Institusi akademik dan pakar digital forensik juga dapat membantu dalam menganalisis bukti digital. Evaluasi terhadap setiap kasus yang ditangani penting dilakukan guna mengidentifikasi kelemahan dan meningkatkan efektivitas penyidikan di masa mendatang. Tantangan dalam penegakan hukum terhadap kejahatan seksual daring

terhadap anak membutuhkan pendekatan yang komprehensif dan adaptif. Penguatan kompetensi penyidik, pengembangan teknologi investigasi, serta kerja sama antarlembaga diharapkan mampu mendorong upaya pemberantasan kejahatan ini berjalan lebih efektif dan memberikan perlindungan maksimal bagi anak-anak sebagai kelompok rentan.

VII. Kesimpulan

Barang bukti digital memegang peranan penting dalam pembuktian tindak pidana seksual daring terhadap anak. Jenis bukti seperti tangkapan layar, metadata, rekaman audio/video, clone disk, dan konten cloud memiliki nilai pembuktian yang berbeda, dengan clone disk sebagai bukti konklusif yang paling kuat. Validitas bukti digital sangat bergantung pada prosedur forensik yang sesuai standar, seperti permanenisasi URL, penggunaan write-blocker, verifikasi hash, serta dokumentasi chain of custody. Penerapan standar ISO/IEC 27037 menjadi landasan teknis dalam menjaga keabsahan bukti digital melalui tahapan identifikasi, koleksi, akuisisi, dan preservasi. Kendala dalam proses pembuktian masih banyak ditemukan, seperti keterbatasan SDM, minimnya pemahaman teknis, serta tantangan dari sisi teknologi dan anonimitas pelaku. Sebagai penutup, digital forensik harus diakui sebagai instrumen hukum penting dalam menanggapi kejahatan seksual daring. Diperlukan penguatan kapasitas aparat, pembaruan regulasi, dan kerja sama lintas sektor untuk menjamin bukti digital dapat digunakan secara sah dan efektif di pengadilan. Hal ini menjadi langkah strategis dalam melindungi anak sebagai kelompok rentan dan memperkuat sistem hukum pidana di era digital.

Ucapan Terima Kasih

Segala puji dan syukur saya panjatkan kepada Allah SWT atas segala nikmat, kekuatan, dan ketenangan yang diberikan sepanjang proses penyusunan skripsi ini. Terima kasih yang tak terhingga saya sampaikan kepada Mama dan Papa atas cinta, doa, dan dukungan tanpa henti yang menjadi sumber kekuatan terbesar dalam hidup saya. Untuk sahabat-sahabat yang selalu hadir memberi semangat, pelukan hangat, dan dorongan di saat saya mulai lelah, terima kasih telah menjadi bagian dari perjalanan ini. Dan yang paling dalam, terima kasih untuk diri saya sendiri, karena telah bertahan, berjuang, dan tetap percaya bahwa saya mampu sampai di titik ini.

Referensi

[1] K. A. Indriany, “ **Upaya Penanggulangan Tindak Pidana Pelecehan Seksual Anak di Media Sosial (Studi di Kepolisian Daerah Polda Metro Jaya),”** Inov. Pembang. J. Kelitbangan, vol. 11, no. 01, hlm. 87, Apr 2023, doi: 10.35450/jip v11i01.345.

[2] **K.** Khairunnisak dan W. Widodo, **“Digital Forensic Tools And Techniques For Handling Digital Evidence,” J. Resist. Rekayasa** Sist. Komput., vol. 6, **no.** 1, hlm. **1-11,** Apr 2023, **doi: 10.31598/jurnalresistor.v6i1.1266.**

[3] A. S. Nuryah, “Child Grooming pada Media Sosial Sebagai Modus Baru Pelecehan Seksual Anak di Desa Kedungpeluk,” vol. 7, 2023.

[4] D. Z. Solihah, K. Nyawiji, Fera, dan D. Z. Solihah, “Kajian Normatif terhadap Efektivitas Peraturan Perlindungan Anak dalam Penanggulangan Eksploitasi Anak di Dunia Maya,” Perkara J. Ilmu Huk. Dan Polit., vol. 2, no. 4, hlm. 603-614, Jan 2025, doi: 10.51903/perkara.v2i4.2232.

[5] A. Holivia dan T. **Suratman, “Child Cyber Grooming Sebagai Bentuk Modus Baru Cyber Space Crimes,” Bhirawa** Law J., **vol. 2,** no. 1, hlm. 1-13, Mei 2021, doi: 10.26905/blj.v2i1.5847.

[6] N. Ishmah, A. F. Putri, E. Sicillia, N. P. V. L. P. Arimbawa, dan A. Y. Ramadhana, “Meninjau Eksistensi Kebijakan Pemerintah Terhadap Kerentanan Cyber child grooming,” JIIP J. Ilm. Ilmu Pemerintah., vol. 9, no. 1, hlm. 24-39, Mar 2024, doi: 10.14710/jiip.v9i1.20620.

[7] F. Awaluddin, Amsori, dan M. Mulyana, “Tantangan dan Peran Digital Forensik dalam Penegakan Hukum terhadap Kejahatan di Ranah Digital,” HUMANIORUM, vol. 2, no. 1, hlm. 14-19, Jan 2024, doi: 10.37010/hmr.v2i1.35.

[8] T. Arifiyadi, “Cyber Crime, Bukti Elektronik, dan Digital Forensic”. MCIT, 2020.

[9] V. Veronika dan B. H. Simanjuntak, “Implementasi ISO 27037 Dalam Pemeriksaan Investigatif Dengan Teknik Forensik Digital untuk Memperoleh Bukti Audit di Badan Pemeriksa Keuangan (BPK),” J. Magister Akunt. Trisakti, vol. 9, no. 2, hlm. 89-104, Sep 2022, doi: 10.25105/jmat.v9i2.13343.

[10] M. I. M. Javiery dan M. E. Lyanthi, “Perlindungan Hukum Bagi Korban Penyebaran Vidio Berkonten Kekerasan Seksual,” vol. 5, no. 03, 2025.

[11] S. Respationo, B. Simatupang, dan R. Nofrial, “Analisis Yuridis Penggunaan Informasi/ **Dokumen Elektronik Sebagai Alat** Bukti Dalam Penegakan Hukum Pidana **(Studi Perkara Putusan Nomor: 192/Pid.B/2023/PN Btm),”** vol. 3, no. 1, 2024.

[12] H. F. Gemilang, “Meninjau Ilmu Digital Forensik Terhadap Bukti Elektronik Dalam Tindak Pidana Informasi dan Transaksi Elektronik,” PERAHU PENERANGAN Huk. J. ILMU Huk., vol. 12, no. 2, Jan 2025, doi: 10.51826/perahu.v12i2.984.

[13] V. Roussev, A. Barreto, dan I. Ahmed, “Forensic Acquisition of Cloud Drives,” 26 Januari 2016, arXiv: arXiv:1603.06542. doi: 10.48550/arXiv.1603.06542.

[14] W. Agustiono, D. W. Suci, dan N. Prastiti, “Analisis Forensik Digital Menggunakan Metode NIST untuk Memulihkan Barang Bukti yang Dihapus,” J. Teknol. Dan Inf., vol. 14, no. 2, hlm. 174-185, Sep 2024, doi: 10.34010/jati.v14i2.12952.

[15] P. A. R. Manik, “Jurnal Hukum dan Kewarganegaraan Vol 14 No 2 **Tahun** 2025 Prefixdoi. org/10.3783/causa.v2i 9.246,” vol. 14, no. 2, 2025.

[16] A. W. Malik, D. **S. Bhatti, T.-J. Park, H. U. Ishtiaq, J.-C.** Ryou, dan K.-I. **Kim,** “ **Cloud Digital Forensics: Beyond Tools, Techniques, and Challenges,”** Sensors, vol. **24,** no. 2, hlm. 433, Jan 2024, doi: 10.3390/s24020433.

[17] A. Setya dan A. Suganda, “ **Design of Digital Evidence Collection Framework in Social Media Using SNI 27037: 2014,”** JUITA J. Inform., vol. 10, no. 1, hlm. 127, Mei 2022, doi: 10.30595/juita.v10i1.13149.

[18] **M. N. Al Jumah, B. Sugiantoro,** dan **Y. Prayudi, “Penerapan Metode Composite Logic Untuk Perancangan Framework Pengumpulan Bukti Digital Pada Media Sosial,” Ilk. J. Ilm., vol. 11, no.** 2, hlm. **135-142,** Agu **2019, doi:** 10.33096/ilkom.v11i2.442.135-142.

[19] D. R. A. Romadhon, “Kekuatan Pembuktian dari Foto Percakapan Whatsapp Tanpa Melalui Proses Digital Forensik yang Digunakan Dalam Berita Acara Pemeriksaan Perkara Pidana dan Dalam Paradigma Hukum Islam di Indonesia”.

[20] A. Y. Nasution, H. Hartono, dan R. Rosnelly, “Challenges and Strategies in Forensic Investigation: Leveraging Technology for Digital Security Using Log/Event Analysis Method,” J. Tek. Inform., vol. 18, no. 1, hlm. 53-63, Apr 2025, doi: 10.15408/jti.v18i1.42815.

[21] Aidil Wijaya Kusuma, Erick Irawadi Alwi, dan Ramdaniah Ramdaniah, “Analisis Bukti Digital Pada Media Penyimpanan Flash Disk Menggunakan Metode National Institute Of Standards And Technology (NIST),” Cyber Secur. Dan Forensik Digit., vol. 7, no. 1, hlm. 18-24, Nov 2024, doi: 10.14421/csecurity.2024.7.1.4345.

[22] M. Sugi Hartono dan N. P. Rai Yuliartini, “Penggunaan Bukti Elektronik Dalam Peradilan Pidana,” J. Komun. Huk. JKH, vol. 6, no. 1, hlm. 281, Feb 2020, doi: 10.23887/jkh.v6i1.23607.

[23] J. D. Ponno, “ **Penerapan Digital Forensik Dalam Pembuktian Pencemaran Nama Baik di Dunia Maya”.**

[24] R. Prasetyawan dan R. Indrayani, “Analisis dan Recovery Bukti Digital pada Media Sosial di Perangkat Mobile Berbasis Android,” Explore, vol. 13, no. 2, hlm. 74-78, Jul 2023, doi: 10.35200/ex.v13i2.29.

[25] W. **Prasetya** dan P. Priyana, **“Pertimbangan Hakim Atas Penghadiran Bukti Digital Forensik dalam Perkara Kejahatan Fraud,”** Wajah Huk., vol. 5, no. 2, hlm. **448,** Okt 2021, doi: **10.33087/wjh v5i2.472.**

[27] D. Mualfah dan R. A. Ramadhan, "Analisis Forensik Metadata Kamera CCTV Sebagai Alat Bukti Digital," Digit. Zone J. Teknol. Inf. Dan Komun., vol. 11, no. 2, hlm. 257-267, Nov 2020, doi: 10.31849/digitalzone.v11i2.5174.
[28] Moh. A. Fattah Ys, B. Parga Zen, dan D. E. Wasitarini, "Penerapan Sistem Manajemen Keamanan Informasi ISO 27001 pada Perpusnas RI dalam mendukung Keamanan Tata Kelola Teknologi Informasi," Cyber Secur. Dan Forensik Digit., vol. 6, no. 2, hlm. 76-82, Feb 2024, doi: 10.14421/csecurity.2023.6.2.4190.
[29] J. Sachowski, "Implementing Digital Forensic Readiness: From Reactive to Proactive Process", IN: Wiley, 2003.
[30] D. Schweitzer, Incident response: computer forensics toolkit. Indianapolis, IN: Wiley, 2003.
[31] R. A. Ramadhan, Abdul Kudus Zaini, dan Jerika Mardafora, "Pelatihan Investigasi Digital Forensik," J. Pengabdi. Masy. Dan Penerapan Ilmu Pengetah., vol. 3, no. 2, hlm. 1-6, Nov 2022, doi: 10.25299/jpmpip.2022.11003.
[32] R. R. Andarek, "Penerapan Forensic Science Dalam Proses Penyidikan Kasus Pembunuhan Vina Dan Risky: Antara Bukti Ilmiah Dan Keadilan Substantif," vol. 5, no. 5, 2025, doi: https://doi.org/10.59188/jurnalsostech.v5i5.32152
[33] E. Casey, Digital evidence and computer crime: forensic science, computers and the Internet, 3rd ed. Waltham, MA: Academic Press, 2011.
[34] M. A. Saragih dan J. Simamora, "Peranan Kejaksaan Terhadap Kasus Tindak Pidana Pelecehan Seksual Anak Dibawah Umur," vol. 6, no. 2, 2025, doi: https://doi.org/10.55338/jumin.v6i2.5360.
[35] N. Suryani, Achmad Megantara, dan Najmuddin, "Analisis Perubahan Barang Bukti Menjadi Alat Bukti Dalam Undang-Undang Nomor 12 Tahun 2022 Tentang Tindak Pidana Kekerasan Seksual," J. Huk. Soll., vol. 10, no. 2, hlm. 86-103, Des 2024, doi: 10.32520/das-sollen.v10i2.3715.
[36] D. Frananda, . F., dan H. Bakir, "Strategi Penyidik Mengatasi Kendala Dalam Mengumpulkan Alat Bukti Tindak Pidana Pornografi Melalui Media Elektronik," UNES J. Swara Justisia, vol. 5, no. 3, hlm. 261, Okt 2021, doi: 10.31933/ujsj.v5i3.217.
[37] Sayid Muhammad Rifki Noval Et Al., " The Fusion of Blockchain, Pornography and Human Trafficking in a Global Digital Dragnet that Forms the Online Child Sex Trafficking.," Russ. Law J., vol. 11, no. 5s, Apr 2023, doi: 10.52783/rlj.v11i5s.891.
[38] Y. Winiari W. dan F. Laily Mufid, "Techno Prevention sebagai Upaya Pencegahan Terhadap Pelaku Child Grooming melalui Media Sosial," J. RECHTENS, vol. 11, no. 1, hlm. 109-122, Jun 2022, doi: 10.56013/rechtens.v11i1.1385.