**METODE PENELITIAN**

**LITERATUR RIVIEW JURNAL**

**“Analisis Forensik terhadap Citra Digital yang Mengandung Data Tersembunyi Menggunakan Metode NIST”**

Dosen Pengampu : Ir. Abdul Rachman Manga, S.Kom., MT.,MTA



Oleh :

Danda

13020220232

A7

**PROGRAM STUDI TEKNIK INFORMATIKA**

**FAKULTAS ILMU KOMPUTER**

**UNIVERSITAS MUSLIM INDONESIA**

**MAKASSAR**

**2025**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **No** | **Nama Penulis, Tahun Dan Judul Jurnal** | **Metode Penelitian** | **Tujuan Penelitian** | **Hasil Penelitian** | **Hubungan Dengan Topik Penelitian Anda** |
| 1 | Penelitian ini ditulis oleh Nasirudin, Sunardi, dan Imam Riadi pada tahun 2020 dengan judul "Analisis Forensik Smartphone Android Menggunakan Metode NIST dan Tool MOBILedit Forensic Express." | Metode yang digunakan dalam penelitian ini adalah metode National Institute of Standards and Technology (NIST), yang terdiri dari empat tahapan, yaitu: pertama, tahap Collection yang meliputi pengumpulan dan pendokumentasian barang bukti; kedua, tahap Examination yang mencakup backup data dan imaging system; ketiga, tahap Analysis yang bertujuan untuk menganalisis data yang telah diekstrak guna mendapatkan informasi yang berguna; dan keempat, tahap Reporting yang berfungsi untuk melaporkan hasil analisis, termasuk deskripsi kasus dan rekomendasi. | Tujuan dari penelitian ini adalah untuk melakukan proses investigasi menggunakan metode NIST pada Telegram messenger dengan memanfaatkan tool MOBILedit Forensic Express, sehingga dapat memperoleh data barang bukti digital dari smartphone yang digunakan dalam tindak kejahatan. | Kesimpulan dari penelitian ini menunjukkan bahwa hasil forensic dari smartphone berbasis Android, khususnya Samsung Galaxy A8, membuktikan bahwa metode NIST dan tool MOBILedit Forensic Express efektif dalam mendapatkan bukti digital yang relevan. Namun, hasil yang diperoleh masih memerlukan pengembangan lebih lanjut untuk memenuhi kebutuhan penyidikan kasus kejahatan digital. | Penelitian ini memiliki relevansi yang kuat dengan topik "Analisis Forensik Digital Mengenai Peredaran Informasi Palsu di TikTok melalui Metodologi National Institute of Standards and Technology (NIST)" karena metode NIST yang diterapkan dalam penelitian ini dapat digunakan untuk menganalisis bukti digital terkait informasi palsu di platform TikTok. Pendekatan yang sama dalam pengumpulan, analisis, dan pelaporan dapat diadaptasi untuk mengidentifikasi dan menyelidiki penyebaran informasi palsu di media sosial, sehingga memberikan dasar metodologis yang dapat diterapkan pada kasus-kasus lain yang melibatkan forensik digital di platform media sosial. |
| 2 | Penelitian ini ditulis oleh Ahmad Qayyum Ibnu Hidayat, Erick Irawadi Alwi, dan Andi Widya Mufila Gaffar pada tahun 2024 dengan judul "Studi Forensik Digital: Analisis Bukti Video TikTok dengan Metode DFRWS." | Penelitian ini ditulis oleh Ahmad Qayyum Ibnu Hidayat, Erick Irawadi Alwi, dan Andi Widya Mufila Gaffar pada tahun 2024 dengan judul "Studi Forensik Digital: Analisis Bukti Video TikTok dengan Metode DFRWS." | Tujuan dari penelitian ini adalah untuk menganalisis penyebaran konten video hoax yang terjadi di platform TikTok, dengan fokus pada rekonstruksi bukti digital yang dihapus dari smartphone pelaku, sehingga dapat digunakan sebagai barang bukti dalam proses persidangan. | Kesimpulan dari penelitian ini menunjukkan bahwa bukti digital yang berhasil ditemukan, termasuk video konten, pesan langsung, dan komentar yang ditinggalkan oleh pelaku, dapat diperoleh melalui metode DFRWS. Penelitian ini menegaskan pentingnya bukti digital dalam proses hukum terkait penyebaran hoaks melalui media sosial. | Penelitian ini sangat relevan dengan topik "Analisis Forensik Digital Mengenai Peredaran Informasi Palsu di TikTok melalui Metodologi National Institute of Standards and Technology (NIST)" karena metode DFRWS yang digunakan dalam penelitian ini dapat diadaptasi untuk menganalisis bukti digital terkait informasi palsu di TikTok. Pendekatan yang sistematis dalam pengumpulan dan analisis bukti digital ini memberikan kerangka kerja yang dapat diterapkan untuk menyelidiki penyebaran informasi palsu di platform media sosial, sejalan dengan metodologi NIST. |
| 3 | Penelitian ini ditulis oleh Anton Yudhana, Imam Riadi, dan Ikhwan Anshori pada tahun 2018 dengan judul "Identification of Digital Evidence Facebook Messenger on Mobile Phone with National Institute of Standards Technology (NIST) Method." | Metode penelitian yang digunakan dalam studi ini adalah metode National Institute of Standards and Technology (NIST), yang meliputi tahapan pengumpulan, pemeriksaan, analisis, dan pelaporan untuk mendapatkan bukti digital dari aplikasi Facebook Messenger yang terpasang di smartphone. | Tujuan dari penelitian ini adalah untuk mengidentifikasi dan mengumpulkan sebanyak mungkin bukti digital terkait kejahatan yang dilakukan melalui Facebook Messenger, guna mendukung proses penyelidikan dan penegakan hukum. Kesimpulan dari penelitian ini menunjukkan bahwa penggunaan alat forensik seperti Magnet AXIOM dan Oxygen Forensics Suite 2014 dengan metode NIST dapat menghasilkan bukti digital yang valid, termasuk akun pengguna, teks percakapan, dan gambar. | Kesimpulan dari penelitian ini menunjukkan bahwa penggunaan alat forensik seperti Magnet AXIOM dan Oxygen Forensics Suite 2014 dengan metode NIST dapat menghasilkan bukti digital yang valid, termasuk akun pengguna, teks percakapan, dan gambar. Penelitian ini juga menemukan bahwa Magnet AXIOM memiliki kinerja yang lebih baik dibandingkan dengan Oxygen Forensics Suite 2014 dalam proses akuisisi data. | Penelitian ini memiliki hubungan yang signifikan dengan topik "Analisis Forensik Digital Mengenai Peredaran Informasi Palsu di TikTok melalui Metodologi National Institute of Standards and Technology (NIST)" karena metode NIST yang diterapkan dalam penelitian ini dapat diadaptasi untuk menganalisis bukti digital terkait penyebaran informasi palsu di TikTok. Pendekatan sistematis dalam pengumpulan dan analisis bukti digital ini memberikan kerangka kerja yang relevan untuk menyelidiki kasus-kasus penyebaran informasi palsu di platform media sosial. |
| 4 | Penelitian ini ditulis oleh Rizdqi Akbar Ramadhan, Panji Rachmat Setiawan, dan Dedy Hariyadi pada tahun 2022 dengan judul "Digital Forensic Investigation for Non-Volatile Memory Architecture by Hybrid Evaluation Based on ISO/IEC 27037:2012 and NIST SP800-86 Framework." | Metode penelitian yang digunakan dalam studi ini adalah kombinasi dari standar ISO/IEC 27037:2012 dan NIST SP800-86, yang mencakup langkah-langkah dalam pengumpulan, pemeriksaan, analisis, dan pelaporan bukti digital dari media penyimpanan non-volatil. | Tujuan dari penelitian ini adalah untuk merancang kerangka kerja untuk investigasi forensik digital yang dapat digunakan dalam penanganan bukti digital non-volatil, serta untuk menggabungkan kedua standar tersebut menjadi satu panduan yang komprehensif bagi tim forensik digital. | Kesimpulan dari penelitian ini menunjukkan bahwa integrasi antara NIST SP800-86 dan ISO/IEC 27037:2012 menghasilkan kerangka kerja yang lebih efektif dalam menangani dan menyelidiki bukti digital, dengan mempertimbangkan berbagai faktor seperti kapasitas media penyimpanan dan urgensi situasi. Penelitian ini juga menekankan pentingnya prosedur yang tepat dalam pengumpulan dan analisis bukti untuk menjaga keaslian dan integritas data. | Penelitian ini memiliki hubungan yang erat dengan topik "Analisis Forensik Digital Mengenai Peredaran Informasi Palsu di TikTok melalui Metodologi National Institute of Standards and Technology (NIST)" karena kerangka kerja yang diusulkan dapat diterapkan untuk menganalisis bukti digital terkait penyebaran informasi palsu di TikTok. Metode yang sistematis dalam pengumpulan dan analisis bukti digital ini memberikan panduan yang relevan untuk menyelidiki kasus-kasus penyebaran informasi palsu di platform media sosial. |
| 5 | Penelitian ini ditulis oleh Agil Nofiyan dan Mushlihudin pada tahun 2020 dengan judul "Analisis Forensik pada Web Phishing Menggunakan Metode National Institute Of Standards And Technology (NIST)." | Metode penelitian yang digunakan dalam studi ini adalah metode National Institute of Standards and Technology (NIST), yang terdiri dari tahapan Collection, Examination, Analysis, dan Reporting untuk menganalisis proses investigasi digital dalam kasus cybercrime, khususnya phishing. | Tujuan dari penelitian ini adalah untuk menganalisis serangan web phishing yang dilakukan oleh pelaku dengan memanfaatkan teknik fake login, serta untuk mengidentifikasi dan mengumpulkan bukti digital yang relevan, seperti URL phishing, DNS, dan informasi pelaku. | Kesimpulan dari penelitian ini menunjukkan bahwa penggunaan metode NIST efektif dalam mengungkap bukti digital yang dapat digunakan dalam penyelidikan kasus kejahatan siber, serta menekankan pentingnya penggunaan alat seperti Wireshark dan Hashcalc dalam proses pengumpulan dan analisis bukti. | Penelitian ini memiliki hubungan yang erat dengan topik "Analisis Forensik Digital Mengenai Peredaran Informasi Palsu di TikTok melalui Metodologi National Institute of Standards and Technology (NIST)" karena metode NIST yang diterapkan dalam penelitian ini dapat diadaptasi untuk menganalisis bukti digital terkait penyebaran informasi palsu di TikTok. Pendekatan sistematis dalam pengumpulan dan analisis bukti digital ini memberikan kerangka kerja yang relevan untuk menyelidiki kasus-kasus penyebaran informasi palsu di platform media sosial.  Bookmark messageCopy messageExport |
| 6 | Penelitian ini ditulis oleh Desti Mualfah dan Rizdqi Akbar Ramadhan pada tahun 2021 dengan judul "Analisis Digital Forensik Rekaman Kamera CCTV Menggunakan Metode NIST (National Institute of Standards Technology)." | Metode penelitian yang digunakan dalam studi ini adalah metode NIST, yang meliputi tahapan pengumpulan, pemeriksaan, analisis, dan pelaporan untuk mengidentifikasi dan menganalisis bukti digital yang diperoleh dari rekaman kamera CCTV. | Tujuan dari penelitian ini adalah untuk menganalisis sentimen diskusi di Twitter mengenai Pemilu 2024. Penelitian ini bertujuan untuk memberikan wawasan mengenai pandangan masyarakat terhadap calon, partai, dan isu-isu yang terkait dengan pemilu. | Kesimpulan dari penelitian ini menunjukkan bahwa analisis video rekaman kamera CCTV dapat memberikan informasi terstruktur dan komprehensif yang dapat dipertanggungjawabkan dalam persidangan, serta menekankan pentingnya penerapan ilmu digital forensik untuk menjaga keaslian dan integritas bukti digital. | Penelitian ini memiliki hubungan yang erat dengan topik "Analisis Forensik Digital Mengenai Peredaran Informasi Palsu di TikTok melalui Metodologi National Institute of Standards and Technology (NIST)" karena metode NIST yang diterapkan dalam penelitian ini dapat digunakan untuk menganalisis bukti digital terkait penyebaran informasi palsu di TikTok. Pendekatan sistematis dalam pengumpulan dan analisis bukti digital ini memberikan kerangka kerja yang relevan untuk menyelidiki kasus-kasus penyebaran informasi palsu di platform media sosial. |
| 7 | Penelitian ini ditulis oleh Halimah Septya Mikayla, Ari Kusyanti, dan Primantara Hari Trisnawan pada tahun 2024 dengan judul "Analisis Forensik Digital untuk Investigasi Kasus Cyberbullying pada Media Sosial TikTok." | Metode penelitian yang digunakan dalam studi ini adalah model investigasi forensik digital yang berfokus pada jejaring sosial, yang mencakup tahapan perencanaan, pengintaian, pengumpulan, transportasi, pemeriksaan, identifikasi, analisis, klasifikasi, pelaporan, dan presentasi. | Tujuan dari penelitian ini adalah untuk mengumpulkan dan menganalisis bukti digital terkait kasus cyberbullying yang terjadi di platform TikTok, baik pada aplikasi Android maupun web, dengan harapan dapat memberikan pemahaman yang lebih baik tentang proses investigasi forensik digital dalam konteks media sosial. | Kesimpulan dari penelitian ini menunjukkan bahwa penelitian berhasil memperoleh bukti digital yang substansial untuk membuktikan kasus cyberbullying, dengan persentase keberhasilan pengumpulan bukti mencapai 68,8% dari perbandingan data awal skenario dengan data yang ditemukan melalui forensik digital. Penelitian ini juga menemukan perbedaan signifikan antara bukti digital yang diperoleh dari TikTok Android dan TikTok web. | Penelitian ini memiliki hubungan yang erat dengan topik "Analisis Forensik Digital Mengenai Peredaran Informasi Palsu di TikTok melalui Metodologi National Institute of Standards and Technology (NIST)" karena metode yang digunakan dalam penelitian ini dapat diadaptasi untuk menganalisis bukti digital terkait penyebaran informasi palsu di TikTok. Pendekatan sistematis dalam pengumpulan dan analisis bukti digital ini memberikan kerangka kerja yang relevan untuk menyelidiki kasus-kasus penyebaran informasi palsu di platform media sosial. |
| 8 | Penelitian ini ditulis oleh Rahmat Novrianda Dasmen, Muhammad Reihan Pratama, Husni Yasir, dan Ariff Budiman pada tahun 2024 dengan judul "Analisis Forensik Digital Pada Kasus Cyberbullying dengan Metode National Institute of Standards and Technology SP 800 - 86." | Metode penelitian yang digunakan dalam studi ini adalah metode National Institute of Standards and Technology (NIST) SP 800 - 86, yang meliputi tahapan pengumpulan, pemeriksaan, analisis, dan pelaporan untuk mengidentifikasi dan memulihkan bukti digital dari flashdisk yang terkait dengan kasus cyberbullying. | Tujuan dari penelitian ini adalah untuk mencari dan memulihkan data digital yang telah dihapus dari flashdisk yang digunakan sebagai media penyimpanan bukti dalam kasus cyberbullying, serta untuk memastikan keaslian dan integritas data yang ditemukan. | Kesimpulan dari penelitian ini menunjukkan bahwa penggunaan alat forensik Autopsy berhasil memulihkan 100% bukti digital yang dicari, yang terdiri dari 4 file dengan ekstensi PNG dan 1 file dengan ekstensi MP4, sehingga membuktikan efektivitas metode NIST dalam investigasi forensik digital. | Penelitian ini memiliki hubungan yang erat dengan topik "Analisis Forensik Digital Mengenai Peredaran Informasi Palsu di TikTok melalui Metodologi National Institute of Standards and Technology (NIST)" karena metode NIST yang diterapkan dalam penelitian ini dapat diadaptasi untuk menganalisis bukti digital terkait penyebaran informasi palsu di TikTok. Pendekatan sistematis dalam pengumpulan dan analisis bukti digital ini memberikan kerangka kerja yang relevan untuk menyelidiki kasus-kasus penyebaran informasi palsu di platform media sosial. |
| 9 | Penelitian ini ditulis oleh Riya Majalista dan Tata Sutabri pada tahun 2023 dengan judul "Analisis Pencarian Data Smartphone Menggunakan NIST untuk Penyelidikan Digital Forensik." | Metode penelitian yang digunakan dalam studi ini adalah metode National Institute of Standards and Technology (NIST), yang mencakup tahapan pengumpulan, pemeriksaan, analisis, dan pelaporan untuk menganalisis data yang hilang dari smartphone, khususnya data yang tersimpan di aplikasi WhatsApp. | Tujuan dari penelitian ini adalah untuk menganalisis informasi yang dapat digunakan sebagai dasar ilmu forensik dalam membantu penyelesaian kasus kejahatan dunia maya, dengan fokus pada pengumpulan bukti digital yang relevan dari smartphone yang terlibat dalam tindakan cybercrime. | Kesimpulan dari penelitian ini menunjukkan bahwa analisis forensik yang dilakukan dapat mengidentifikasi dan mengumpulkan bukti digital yang signifikan, termasuk kontak, percakapan, dan gambar dari aplikasi WhatsApp, yang dapat digunakan dalam proses penyelidikan kejahatan siber. Penelitian ini juga menekankan pentingnya penerapan hukum yang jelas untuk menekan angka cybercrime. | Penelitian ini memiliki hubungan yang erat dengan topik "Analisis Forensik Digital Mengenai Peredaran Informasi Palsu di TikTok melalui Metodologi National Institute of Standards and Technology (NIST)" karena metode NIST yang diterapkan dalam penelitian ini dapat diadaptasi untuk menganalisis bukti digital terkait penyebaran informasi palsu di TikTok. Pendekatan sistematis dalam pengumpulan dan analisis bukti digital ini memberikan kerangka kerja yang relevan untuk menyelidiki kasus-kasus penyebaran informasi palsu di platform media sosial. |
| 10 | Penelitian ini ditulis oleh Andi Muh Afdal, Yulita Salim, dan Abdul Rachman Manga pada tahun 2022 dengan judul "Analisis Bukti Digital Forensik pada Discord Menggunakan Metode National Institute of Standards Technology." | Metode penelitian yang digunakan dalam studi ini adalah metode National Institute of Standards and Technology (NIST), yang terdiri dari tahapan Collection, Examination, Analysis, dan Reporting untuk melakukan investigasi terhadap aplikasi Discord yang digunakan dalam kasus tindak pidana. | Tujuan dari penelitian ini adalah untuk menganalisis dan mengidentifikasi bukti digital yang dapat diperoleh dari aplikasi Discord, khususnya dalam konteks penyalahgunaan aplikasi untuk kegiatan terorisme, serta untuk memberikan panduan bagi aparat penegak hukum dalam proses penyelidikan. | Kesimpulan dari penelitian ini menunjukkan bahwa meskipun hanya berhasil mendapatkan bukti berupa gambar dan video dengan akurasi 38,46% dan 15,38% masing-masing, proses analisis yang dilakukan dengan menggunakan alat FTK Imager tetap dapat memberikan informasi yang berguna dalam penyelidikan kasus kejahatan. Penelitian ini juga menekankan bahwa teks percakapan dan identitas tidak dapat diperoleh, yang menunjukkan tantangan dalam pengumpulan bukti digital. | Penelitian ini memiliki hubungan yang erat dengan topik "Analisis Forensik Digital Mengenai Peredaran Informasi Palsu di TikTok melalui Metodologi National Institute of Standards and Technology (NIST)" karena metode NIST yang diterapkan dalam penelitian ini dapat diadaptasi untuk menganalisis bukti digital terkait penyebaran informasi palsu di TikTok. Pendekatan sistematis dalam pengumpulan dan analisis bukti digital ini memberikan kerangka kerja yang relevan untuk menyelidiki kasus-kasus penyebaran informasi palsu di platform media sosial. |
| 11 | Achmad Iqbal Yuladi dan Rini Indrayani pada tahun 2023 dengan judul "Analisis dan Perbandingan Tools Forensik Menggunakan Metode NIST dalam Penanganan Kasus Kejahatan Siber." | Metode penelitian yang digunakan dalam studi ini adalah metode National Institute of Standards and Technology (NIST), yang meliputi tahapan Collection, Examination, Analysis, dan Reporting untuk menganalisis dan membandingkan hasil dari dua alat forensik, yaitu MOBILedit Forensic Express dan Magnet Axiom, dalam konteks kasus cyberbullying di aplikasi WhatsApp. | Tujuan dari penelitian ini adalah untuk menganalisis efektivitas kedua alat forensik dalam mengumpulkan dan menganalisis bukti digital yang terkait dengan kasus kejahatan siber, serta untuk memberikan rekomendasi mengenai alat mana yang lebih baik digunakan dalam investigasi tersebut. | Kesimpulan dari penelitian ini menunjukkan bahwa Magnet Axiom memiliki akurasi yang lebih tinggi, yaitu 81,8%, dibandingkan dengan MOBILedit Forensic Express yang hanya mencapai 72,7% dalam kondisi objek yang tidak di-rooted. Penelitian ini juga menekankan pentingnya penggunaan metode NIST untuk memastikan keandalan dan validitas proses investigasi forensik digital. | Penelitian ini memiliki hubungan yang erat dengan topik "Analisis Forensik Digital Mengenai Peredaran Informasi Palsu di TikTok melalui Metodologi National Institute of Standards and Technology (NIST)" karena metode NIST yang diterapkan dalam penelitian ini dapat digunakan untuk menganalisis bukti digital terkait penyebaran informasi palsu di TikTok. Pendekatan sistematis dalam pengumpulan dan analisis bukti digital ini memberikan kerangka kerja yang relevan untuk menyelidiki kasus-kasus penyebaran informasi palsu di platform media sosial. |
| 12 | Imam Riadi, Rusydi Umar, dan Imam Mahfudl Nasrulloh, yang diterbitkan pada tahun 2017 dengan judul "Analisis Forensik Bukti Digital pada Frozen Solid State Drive dengan Metode National Institute of Standards and Technology (NIST)". | Metode penelitian yang digunakan dalam studi ini adalah metode pengambilan data secara statis dan tahapan analisis forensik yang mengikuti prosedur dari National Institute of Standards and Technology (NIST). | Tujuan dari penelitian ini adalah untuk menganalisis bukti digital yang tersimpan pada media penyimpanan utama, yaitu Solid State Drive (SSD), dalam kondisi sistem komputer yang terinstal software pembeku drive, serta untuk mendapatkan bukti digital yang valid dan dapat dipertanggungjawabkan. | Kesimpulan dari penelitian ini menunjukkan bahwa analisis forensik digital perlu dilakukan dengan prosedur yang tepat dan menggunakan berbagai tool forensik untuk mendapatkan bukti digital yang diharapkan, meskipun terdapat tantangan yang dihadapi akibat penggunaan software pembeku drive. | Penelitian ini relevan dengan topik analisis forensik digital mengenai peredaran informasi palsu di TikTok, karena metodologi NIST yang digunakan dalam penelitian ini dapat diterapkan untuk menganalisis bukti digital yang berkaitan dengan penyebaran informasi palsu, sehingga dapat membantu dalam investigasi dan penegakan hukum terhadap kejahatan siber yang terjadi di platform tersebut.  Bookmark messageCopy messageExport |
| 13 | Penelitian ini ditulis oleh Lina Alfaridah, Yuhandri, dan Sumijan pada tahun 2024 dengan judul "Implementasi Metode National Institute of Standards and Technology (NIST) dalam Analisis Forensik untuk Mendeteksi Keaslian Citra Digital". | Metode yang digunakan dalam penelitian ini adalah framework National Institute of Standards and Technology (NIST) dan Error Level Analysis (ELA), yang terdiri dari empat tahapan: collection, examination, analysis, dan reporting. | Tujuan dari penelitian ini adalah untuk mengidentifikasi kredibilitas keaslian citra digital menggunakan tools forensik, serta untuk memberikan pemahaman yang lebih baik mengenai bagaimana citra digital dapat dimanipulasi dan dideteksi keasliannya. | Kesimpulan dari penelitian ini menunjukkan bahwa implementasi metode NIST dapat efektif dalam mendeteksi keaslian citra digital, di mana perbedaan antara citra asli dan citra yang telah dimanipulasi dapat diidentifikasi melalui analisis ELA dan metadata. | Penelitian ini relevan dengan topik analisis forensik digital mengenai peredaran informasi palsu di TikTok, karena metodologi NIST yang diterapkan dapat digunakan untuk mendeteksi keaslian citra digital yang sering digunakan dalam penyebaran informasi palsu di platform tersebut. Dengan menggunakan pendekatan yang sama, analisis forensik dapat membantu dalam mengidentifikasi dan menangani konten yang dimanipulasi di TikTok. |
| 14 | Penelitian ini ditulis oleh Muhammad Ali Diko Putra dan rekan-rekannya pada tahun 2024 dengan judul "Analisis Forensik Pada Instagram dan Tik Tok Dalam Mendapatkan Bukti Digital Dengan Menggunakan Metode NIST 800 - 86". | Metode penelitian yang digunakan dalam studi ini adalah metode National Institute of Standards and Technology (NIST), yang terdiri dari empat tahapan: Collection, Examination, Analysis, dan Reporting. | Tujuan dari penelitian ini adalah untuk menentukan proses menemukan bukti digital pada aplikasi media sosial Instagram dan TikTok yang diakses melalui smartphone, serta untuk mengevaluasi efektivitas berbagai alat forensik dalam mengakuisisi bukti digital. | Kesimpulan dari penelitian ini menunjukkan bahwa alat FTK Imager adalah yang paling efektif dalam mengakuisisi bukti digital, dengan persentase akuisisi yang lebih tinggi dibandingkan dengan alat lainnya, yaitu 57% untuk Instagram dan 71% untuk TikTok. | Penelitian ini relevan dengan topik analisis forensik digital mengenai peredaran informasi palsu di TikTok, karena menggunakan metodologi NIST untuk mengidentifikasi dan menganalisis bukti digital yang dapat digunakan dalam investigasi kasus kejahatan siber, termasuk penyebaran informasi palsu. |
| 15 | Penulis dari jurnal ini adalah Imam Riadi, Sunardi, dan Takdir Ruslan, yang diterbitkan pada tahun 2023 dengan judul "Analisis Forensik Digital Pada Whatsapp Dan Facebook Menggunakan Metode NIST" | Metode penelitian yang digunakan dalam studi ini adalah metode static forensics dengan kerangka kerja yang dikembangkan oleh National Institute of Standards and Technology (NIST). | Tujuan dari penelitian ini adalah untuk mengambil barang bukti digital dan mengevaluasi kinerja alat forensik yang digunakan untuk mengembalikan data yang telah dihapus dalam bentuk multimedia audio dan video pada perangkat smartphone berbasis Android. | Kesimpulan dari penelitian ini menunjukkan bahwa alat forensik seperti Belkasoft, Magnet Axiom, dan Oxygen berhasil mengembalikan sebagian data yang terhapus dari aplikasi WhatsApp dan Facebook Messenger, sedangkan alat MOBILedit tidak berhasil mengembalikan data apapun. | Penelitian ini relevan dengan topik analisis forensik digital mengenai peredaran informasi palsu di TikTok melalui metodologi NIST, karena keduanya menggunakan pendekatan forensik untuk mengungkap dan menganalisis data digital yang berkaitan dengan kejahatan siber, meskipun fokusnya berbeda pada platform dan jenis data yang dianalisis. |
| 16 | Penelitian ini ditulis oleh Aidil Wijaya Kusuma, Erick Irawadi Alwi, dan Ramdaniah Ramdaniah pada tahun 2024 dengan judul "Analisis Bukti Digital Pada Media Penyimpanan Flash Disk Menggunakan Metode National Institute Of Standards And Technology (NIST)". | Metode penelitian yang digunakan dalam studi ini adalah metode National Institute of Standards and Technology (NIST), yang melibatkan tahapan pengumpulan, pemeriksaan, analisis, dan pelaporan bukti digital. | Tujuan dari penelitian ini adalah untuk memperoleh, mengambil, melestarikan, dan menyajikan data atau informasi terkait jejak aktivitas kasus cybercrime yang terdapat pada media penyimpanan flash disk yang telah dihapus, serta mendukung penyelidikan terhadap pelaku kejahatan dengan menerapkan prinsip-prinsip forensik digital. | Kesimpulan dari penelitian ini menunjukkan bahwa bukti digital yang telah dihapus pada media penyimpanan flash disk dengan perlakuan yang berbeda berhasil ditemukan dan direcovery menggunakan tools forensic FTK Imager dan Autopsy, di mana seluruh bukti digital yang ditemukan cocok dengan bukti digital yang telah dimasukkan ke dalam flash disk sesuai dengan skenario kasus kejadian. | Penelitian ini relevan dengan topik analisis forensik digital mengenai peredaran informasi palsu di TikTok melalui metodologi NIST, karena keduanya menekankan pentingnya pemulihan dan analisis bukti digital untuk mendukung investigasi kejahatan siber, termasuk dalam konteks penyebaran informasi palsu di platform media sosial. |
| 17 | Imam Riadi, Sunardi, dan Fitriyani Tella (2022) dalam jurnal berjudul "Analisis Forensik pada Email menggunakan Metode National Institute of Standards Technology" yang diterbitkan dalam JISKA (Jurnal Informatika Sunan Kalijaga). | Penelitian ini menggunakan metode *Live Forensics* dengan alur penelitian berdasarkan *National Institute of Standards and Technology (NIST)*, yang terdiri dari empat tahap utama: *Collection, Examination, Analysis,* dan *Reporting*. | Penelitian ini bertujuan untuk menganalisis *email spoofing* dengan mengidentifikasi bukti forensik digital seperti alamat IP, *header email*, dan waktu pengiriman, serta membandingkan akurasi tiga alat forensik (*tracer email analyzer, email dossier,* dan *mail header analysis*) dalam mendeteksi pemalsuan email. | Hasil penelitian menunjukkan bahwa *tracer email analyzer* merupakan alat yang paling efektif dalam mengungkap bukti forensik terkait *email spoofing*, seperti alamat IP pengirim, domain, dan lokasi geografis. Penelitian ini juga menekankan pentingnya analisis *header email* untuk membedakan email asli dan palsu. | Penelitian ini relevan dengan topik *"Analisis Forensik Digital Mengenai Peredaran Informasi Palsu di TikTok melalui Metodologi NIST"* karena keduanya berfokus pada pendekatan forensik digital untuk mengidentifikasi dan menganalisis konten palsu. Metode NIST yang digunakan dalam penelitian ini dapat diadaptasi untuk menyelidiki penyebaran informasi palsu di TikTok, sementara alat-alat forensik yang dibahas (seperti analisis *header* atau pelacakan sumber) dapat dimodifikasi untuk platform media sosial. Temuan terkait efektivitas alat tertentu juga memberikan wawasan untuk memilih tools yang sesuai dalam investigasi forensik digital di TikTok. |
| 18 | Nadila Hamid, Jeki Kuswanto, Dwi Nurani, Andriyan Dwi Putra, Fiyas Mahananing Puri, dan Surya Tri Atmaja Ramadhani (2024) dalam jurnal berjudul *"Forensic Recovery Techniques on Android Devices with the National Institute of Standards and Technology (NIST) Approach"* yang diterbitkan dalam *JTECS (Jurnal Sistem Telekomunikasi Elektronika Sistem Kontrol Power Sistem & Komputer)*. | Penelitian ini menggunakan metode forensik digital dengan pendekatan *National Institute of Standards and Technology (NIST)*, yang terdiri dari empat tahap utama: *Collection, Examination, Analysis,* dan *Reporting*. Alat forensik yang digunakan adalah *Mobiledit Forensic* dan *Oxygen Forensic SQLite Viewer* untuk mengekstrak bukti digital dari perangkat Android. | Penelitian ini bertujuan untuk mengimplementasikan teknik pemulihan data (*forensic recovery*) pada kasus prostitusi online yang dilakukan melalui aplikasi WhatsApp, dengan fokus pada pengumpulan bukti digital seperti pesan teks, gambar, log panggilan, dan kontak yang telah dihapus oleh pelaku. Tujuannya adalah membantu penegak hukum dalam mengungkap kejahatan digital dan menyediakan bukti yang valid untuk proses hukum. | Hasil penelitian menunjukkan bahwa penggunaan alat forensik *Mobiledit Forensic* dan *Oxygen Forensic SQLite Viewer* dengan metode NIST berhasil memulihkan bukti digital yang telah dihapus dengan akurasi 100%. Temuan ini membuktikan efektivitas pendekatan NIST dan alat forensik dalam mengungkap kejahatan prostitusi online melalui WhatsApp. | Penelitian ini relevan dengan topik *"Analisis Forensik Digital Mengenai Peredaran Informasi Palsu di TikTok melalui Metodologi NIST"* karena keduanya berfokus pada penggunaan metode NIST untuk investigasi forensik digital. Pendekatan NIST yang diterapkan dalam penelitian ini dapat diadaptasi untuk menganalisis penyebaran informasi palsu di TikTok, sementara alat forensik seperti *Mobiledit Forensic* dan *Oxygen Forensic SQLite Viewer* dapat dimodifikasi untuk mengekstrak bukti digital dari platform media sosial. Temuan terkait akurasi pemulihan data juga memberikan wawasan tentang efektivitas alat forensik dalam konteks yang berbeda, termasuk TikTok. |
| 19 | Penelitian ini ditulis oleh Dwi Putri Medianti, M. Abdul Haris, dan Mustamin Hamid pada tahun 2022 dengan judul "Analisa dan Pencarian Bukti Forensik Digital pada Aplikasi Media Sosial Twitter Menggunakan Metode National Institute Standard of Technology". | Metode penelitian yang digunakan dalam studi ini adalah metode National Institute of Standards and Technology (NIST), yang meliputi tahapan identifikasi, pengumpulan, pemeriksaan, analisis, dan pelaporan bukti forensik digital dari aplikasi media sosial. | Tujuan dari penelitian ini adalah untuk mengidentifikasi kerangka kerja yang tepat dalam menganalisis dan mengumpulkan bukti forensik dari aplikasi media sosial, dengan fokus pada keandalan, kecepatan, dan akurasi dalam proses analisis. | Kesimpulan dari penelitian ini menunjukkan bahwa penerapan metode NIST dalam analisis dan pencarian bukti forensik pada aplikasi media sosial dapat memberikan hasil yang memuaskan dalam hal keandalan dan akurasi, meskipun terdapat tantangan dalam hal kecepatan akibat kompleksitas data yang besar. | Penelitian ini memiliki hubungan yang erat dengan topik analisis forensik digital mengenai peredaran informasi palsu di TikTok melalui metodologi NIST, karena keduanya menggunakan pendekatan forensik digital untuk mengumpulkan dan menganalisis bukti yang relevan dalam konteks investigasi kejahatan di platform media sosial. |
| 20 | Rizqi Rahmansyah, Carudin, dan Azhari Ali Ridha (2021) dalam jurnal berjudul *"Perbandingan Hasil Investigasi Barang Bukti Digital pada Aplikasi Facebook dan Instagram dengan Metode NIST"* yang diterbitkan dalam *CyberSecurity dan Forensik Digital*. | Penelitian ini menggunakan metode *National Institute of Standards and Technology (NIST)* yang terdiri dari empat tahap: *Collection, Examination, Analysis,* dan *Reporting*. Alat forensik yang digunakan adalah *Magnet Axiom Process* dan *Magnet Axiom Examine* untuk mengekstrak dan menganalisis bukti digital dari perangkat Android. | Penelitian ini bertujuan untuk membandingkan efektivitas pemulihan bukti digital yang telah dihapus pada aplikasi Facebook dan Instagram dalam kasus penyebaran hoaks, serta mengevaluasi pengaruh waktu forensik terhadap hasil yang diperoleh. | Hasil penelitian menunjukkan bahwa Instagram berhasil memulihkan lebih banyak bukti digital (75%) dibandingkan Facebook (37,5%). Waktu pelaksanaan forensik setelah penghapusan juga memengaruhi jumlah bukti yang berhasil ditemukan. Alat *Magnet Axiom* terbukti efektif untuk pemulihan data, meskipun memiliki keterbatasan dalam mengekstrak pesan teks dan caption. | Penelitian ini relevan dengan topik *"Analisis Forensik Digital Mengenai Peredaran Informasi Palsu di TikTok melalui Metodologi NIST"* karena keduanya berfokus pada penggunaan metode NIST untuk investigasi forensik digital di platform media sosial. Temuan terkait efektivitas pemulihan bukti dan pengaruh waktu dapat menjadi acuan untuk mengeksplorasi penyebaran informasi palsu di TikTok. Selain itu, alat seperti *Magnet Axiom* dapat diadaptasi untuk analisis forensik di TikTok, sementara pendekatan NIST memastikan proses investigasi yang terstruktur dan valid. |
| 21 | Penelitian ini ditulis oleh Devkya Mutiara Syafitri dan Fahmi Fachri, dan dipublikasikan dalam jurnal RABIT: Jurnal Teknologi dan Sistem Informasi Univrab pada Januari 2025 dengan judul "Analisis Forensik Digital Telegram pada Android untuk Cybercrime dengan Kerangka National Institute of Standard Technology (NIST)". | Metode penelitian yang digunakan adalah kerangka kerja NIST, yang terdiri dari empat tahapan: Collection, Examination, Analysis, dan Reporting. | Tujuan dari penelitian ini adalah untuk melakukan analisis forensik digital pada aplikasi Telegram di smartphone Android, dengan fokus pada bentuk kejahatan penipuan penjualan handphone. Kesimpulan dari penelitian ini menunjukkan bahwa alat forensik MOBILedit Forensic berhasil menemukan bukti digital berupa video, foto, dan voice note, sedangkan FTK Imager hanya mampu memulihkan bukti chat. | Penelitian ini menekankan pentingnya pemilihan alat forensik yang tepat untuk memaksimalkan pengumpulan bukti digital dalam kasus kejahatan digital. | Penelitian ini relevan dengan topik analisis forensik digital mengenai peredaran informasi palsu di TikTok melalui metodologi NIST, karena keduanya menggunakan pendekatan forensik untuk mengidentifikasi dan menganalisis bukti digital yang berkaitan dengan kejahatan siber, meskipun fokusnya berbeda pada platform yang digunakan.  Bookmark messageCopy messageExport |
| 22 | Penelitian ini ditulis oleh Karolina Eka Purnama, Chaerur Rozikin, dan Azhari Ali Ridha pada tahun 2023 dengan judul "Analisis Forensik Citra Digital Menggunakan Teknik Error Level Analysis dan Metadata Berdasarkan Metode NIST" yang dipublikasikan dalam JATI (Jurnal Mahasiswa Teknik Informatika) Vol. 7 No. 2. | Metode penelitian yang digunakan dalam studi ini adalah metode National Institute of Standards and Technology (NIST), yang terdiri dari tahapan pengumpulan data, pemeriksaan, analisis, dan pelaporan. | Tujuan dari penelitian ini adalah untuk membuktikan keaslian bukti digital melalui analisis forensik citra digital, dengan fokus pada identifikasi dan analisis foto yang telah dimanipulasi. | Kesimpulan dari penelitian ini menunjukkan bahwa salah satu dari dua foto yang dijadikan barang bukti merupakan hasil manipulasi, di mana foto asli teridentifikasi berasal dari kamera Canon EOS 700D dan dinyatakan sebagai foto original, sedangkan foto manipulasi menunjukkan bahwa foto tersebut telah diedit menggunakan Adobe Photoshop. | Penelitian ini relevan dengan topik analisis forensik digital mengenai peredaran informasi palsu di TikTok, karena menggunakan metodologi NIST untuk mendeteksi keaslian citra digital, yang dapat diterapkan untuk mengidentifikasi dan menganalisis konten yang dimanipulasi di platform media sosial seperti TikTok.  Bookmark messageCopy messageExport |
| 23 | Penelitian ini ditulis oleh Wahyudi Agustiono, Dini Wulan Suci, dan Novi Prastiti pada tahun 2024 dengan judul "Analisis Forensik Digital Menggunakan Metode NIST untuk Memulihkan Barang Bukti yang Dihapus," yang dipublikasikan dalam Jurnal Teknologi dan Informasi (JATI) Volume 14 Nomor 2. | Metode penelitian yang digunakan dalam studi ini adalah metode National Institute of Standards and Technology (NIST) SP 800-86, yang terdiri dari empat tahapan: Pengumpulan, Pemeriksaan, Analisis, dan Pelaporan. | Tujuan dari penelitian ini adalah untuk menyelidiki cara memulihkan data yang telah dihapus dari media penyimpanan digital, seperti flashdisk dan harddisk, dengan menggunakan teknik forensik digital. | Kesimpulan dari penelitian ini menunjukkan bahwa data yang dihapus menggunakan metode Shift+Delete dapat dipulihkan sepenuhnya dengan tingkat keberhasilan 100%, sedangkan data yang dihapus melalui pemformatan tidak dapat dipulihkan, dengan tingkat keberhasilan 0%. | Penelitian ini memiliki hubungan yang erat dengan topik analisis forensik digital mengenai peredaran informasi palsu di TikTok, karena metodologi NIST yang digunakan dapat diterapkan untuk memulihkan dan menganalisis bukti digital yang berkaitan dengan konten yang dimanipulasi atau disebarkan di platform tersebut. |
| 24 | Yudharta Arif, Erick Irawadi Alwi, Muhammad Arfah Asis. (2023). Analisis Bukti Digital Direct Message Pada Twitter Menggunakan Metode National Institute Of Justice (NIJ) | Penelitian ini menggunakan metode kualitatif dengan pendekatan National Institute of Justice (NIJ), yang meliputi tahap:  Persiapan - Mempersiapkan alat dan bahan untuk investigasi. Koleksi - Mengumpulkan dokumen dan barang bukti elektronik.  Pemeriksaan Memeriksa bukti secara digital. Analisis Menganalisis bukti yang diperoleh. Pelaporan - Melaporkan hasil analisis. | Tujuan utama dari penelitian ini adalah untuk melakukan investigasi forensik pada aplikasi Direct Message di Twitter dan menentukan tingkat keberhasilan alat forensik dalam menemukan data yang telah dihapus. | penggunaan alat forensik seperti Magnet AXIOM dan MOBILedit berhasil menemukan bukti digital dengan tingkat keberhasilan total sebesar 66,66%. Alat Magnet AXIOM menemukan bukti berupa teks percakapan yang telah dihapus, sedangkan MOBILedit berhasil menemukan gambar yang dihapus. | Penelitian ini relevan dengan topik saya karena fokus pada media sosial menciptakan kesamaan, di mana Twitter dan TikTok menjadi platform yang relevan untuk menangani isu cybercrime. keduanya membahas masalah cybercrime, meskipun dengan fokus yang berbeda; satu pada pornografi dan penipuan, dan yang lainnya pada penyebaran informasi palsu |
| 25 | Doni Karseno, Billy Hendrik. (2024). Investigasi dan Analisis Pengembalian Pesan Whatsapp yang Sudah Terhapus Menggunakan Metode National Institute of Justice (NIJ) | Penelitian ini menggunakan metode National Institute of Justice (NIJ) yang terdiri dari empat tahap:  Assessment (Penilaian),  Acquisition (Akuisisi),  Examination (Pemeriksaan),  Documenting & Reporting (Pendokumentasian & Pelaporan) | Penelitian ini bertujuan untuk:  Mengetahui cara melakukan digital forensics pada aplikasi WhatsApp.  Menganalisis hasil digital menggunakan tools MOBILEedit dan Oxygen Forensic dalam pencarian bukti digital terkait tindak kejahatan dunia maya. | Proses akuisisi pada WhatsApp menggunakan MOBILEedit mengikuti tahap-tahap NIJ.  Hasil penelitian menunjukkan bahwa bukti digital berhasil ditemukan, meskipun informasi yang diperoleh dari MOBILEedit terbatas pada beberapa data seperti file gambar dan informasi lainnya. | Penelitian ini relevan dengan topik saya karena Keduanya menggunakan metodologi NIJ yang sistematis untuk melakukan penyelidikan digital, sehingga menunjukkan konsistensi dalam pendekatan analisis forensik. Fokus utama dari kedua penelitian adalah pada pentingnya bukti digital untuk membuktikan tindak kejahatan di dunia maya. |
| 26 | Desti Mualfah, Muhammad Iqbal Syam, Baidarus. (2023). Analisis perbandingan tools mobile forensic menggunakan metode national institute of justice (NIJ) | Metode yang digunakan dalam penelitian ini adalah National Institute of Justice (NIJ). Metode ini terdiri dari lima tahapan:  Identification (Identifikasi), Collection (Pengumpulan), Examination (Pemeriksaan), Analysis (Analisis), Reporting (Pelaporan) | Tujuan dari penelitian ini adalah untuk membandingkan kinerja dua tools forensik, yaitu Oxygen Forensic Detective dan Belkasoft Evidence Center, dalam mengembalikan data yang telah dihapus dan bukti digital lainnya pada kasus transaksi jual beli narkoba. | Oxygen Forensic Detective berhasil mendapatkan 5 dari 6 bukti digital (83,33%), sementara Belkasoft Evidence Center hanya mendapatkan 4 dari 6 bukti digital (66,67%).  Oxygen Forensic Detective lebih informatif dan mampu menampilkan rincian informasi perangkat, sedangkan Belkasoft Evidence Center tidak dapat menemukan bukti digital tertentu, seperti file audio. Oxygen Forensic Detective direkomendasikan sebagai alat yang lebih unggul dalam akuisisi bukti digital pada perangkat smartphone. | Penelitian ini relevan dengan topik saya karena Keduanya fokus pada forensik digital, dengan tujuan mengidentifikasi dan menganalisis bukti digital yang relevan. Penelitian sebelumnya berfokus pada transaksi narkoba, sementara penelitian Anda menyoroti penyebaran informasi palsu di media sosial. M |
| 27 | Dwi Putri Medianti, M. Abdul Haris, Mustamin Hamid. (2024). Analisa dan Pencarian Bukti Forensik Digital pada Aplikasi Media Sosial Twitter Menggunakan Metode National Institute Standard of Technology (NIST) | Metode yang digunakan dalam penelitian ini adalah metode National Institute of Standards and Technology (NIST). Penelitian ini melibatkan pengumpulan data melalui wawancara, observasi, dan studi pustaka untuk menganalisis dan mengumpulkan bukti forensik dari aplikasi media sosial Twitter. | Tujuan penelitian ini adalah untuk mengidentifikasi kerangka kerja yang tepat untuk menganalisis dan mengumpulkan bukti forensik digital dari aplikasi media sosial, dengan fokus pada keandalan, kecepatan, dan akurasi. | penerapan metode NIST dalam analisis dan pencarian bukti forensik pada aplikasi media sosial dapat memberikan hasil yang memuaskan dalam hal keandalan dan akurasi. Namun, terdapat tantangan terkait kecepatan dan kompleksitas data yang harus diatasi untuk meningkatkan efisiensi proses analisis. | Penelitian ini relevan dengan topik saya karena menggunakan metodologi berbasis standar yang diakui, yaitu NIST dan NIJ, untuk analisis forensik digital. Berfokus pada media sosial sebagai platform penyebaran informasi menunjukkan relevansi dalam konteks investigasi digital. |
| 28 | Imanuel Gilbert Rian Mailangkay, Elia Zakharia, Abdul Hadi. (2022). Komparasi Analisis Bukti Digital Tiktok Lite Menggunakan Metode National Institute of Justice (NIJ) | Metode National Institute of Justice (NIJ): Penelitian ini menggunakan metode NIJ yang terdiri dari lima tahapan: Identification, Collection, Examination, Analysis, dan Reporting. Metode ini diterapkan untuk mengakuisisi dan menganalisis bukti digital terkait penggunaan aplikasi Tiktok Lite. | Tujuan penelitian ini adalah untuk mendapatkan bukti digital berupa pesan percakapan dan data akun dari aplikasi Tiktok Lite, serta untuk menganalisis perbedaan hasil akuisisi bukti digital pada smartphone yang telah di-root dan yang tidak di-root. | smartphone yang dalam kondisi root dapat memberikan akses penuh untuk mengakuisisi bukti digital, sedangkan smartphone yang tidak di-root tidak dapat menemukan bukti digital apapun. Penggunaan tool Belkasoft Evidence Center dan Magnet Axiom pada smartphone yang di-root dapat menghasilkan 100% bukti digital, sementara tool MOBILedit Forensics Express tidak menemukan bukti digital sama sekali pada kedua kondisi smartphone. | Penelitian ini relevan dengan topik saya karena Kedua penelitian menggunakan metode NIJ, memberikan pendekatan sistematis untuk akuisisi dan analisis bukti digital. Fokus pada aplikasi Tiktok sebagai platform relevan muncul dalam konteks yang berbeda—cyberbullying dan peredaran informasi palsu. Isu keamanan dan etika di media sosial juga diangkat, menyoroti dampak negatif dari penyalahgunaan aplikasi. |
| 29 | Ikhwan Anshori, Khairina Eka Setya Putri, Umar Ghoni. (2021). Analisis Barang Bukti Digital Aplikasi Facebook Messenger Pada Smartphone Android Menggunakan Metode (NIJ) | Penelitian ini menggunakan metode National Institute Of Justice (NIJ). Metode ini meliputi beberapa tahapan dasar dalam proses forensik, yaitu:  Persiapan: Identifikasi masalah dan pengumpulan informasi. Koleksi: Pengumpulan bukti elektronik yang relevan. Pemeriksaan: Uji coba terhadap smartphone yang terlibat. Analisis: Evaluasi hasil pemeriksaan untuk mendapatkan bukti digital. Pelaporan: Penyusunan laporan hasil analisis. | Tujuan dari penelitian ini adalah untuk menganalisis bukti digital yang dapat diperoleh dari aplikasi Facebook Messenger yang berjalan pada smartphone Android, serta untuk menilai kinerja beberapa alat forensik dalam mengumpulkan bukti digital. | MOBILedit Forensic Express dan Magnet AXIOM memiliki kinerja yang baik dalam mendapatkan bukti digital, termasuk akun, chat, dan gambar. Oxygen Forensic Suite 2014 menunjukkan kinerja yang kurang baik, terutama dalam mengakses data chat. Proses forensik dengan metode NIJ dapat digunakan secara efektif untuk ekstraksi bukti dari aplikasi Facebook Messenger pada perangkat Android. | Penelitian ini relevan dengan topik saya karena kedua penelitian menggunakan metode yang sama, yaitu National Institute of Justice (NIJ), sebagai kerangka kerja sistematis untuk investigasi forensik. Berfokus pada pengumpulan dan analisis bukti digital dari platform media sosial menunjukkan relevansi dalam konteks pengungkapan data digital. |
| 30 | Rahmat Novrianda Dasmen, Arief Rahman, Anugrah Dwi Putra, Muchlis Saputra. (2024). Analisis Digital Forensik Recovery File yang Dihapus Menggunakan Tools Autopsy dengan Metode National Institute of Justice (NIJ) | Penelitian ini menggunakan metode National Institute of Justice (NIJ) dengan lima tahap: identifikasi, pengumpulan, survei, analisis, dan pelaporan. Metode ini diterapkan untuk menganalisis kinerja aplikasi Autopsy dalam memulihkan data yang terhapus dari flashdisk. | Tujuan dari penelitian ini adalah untuk menggunakan software forensik digital Autopsy dalam melakukan analisis forensik digital untuk pemulihan data yang dihapus, khususnya dalam kasus penghapusan bukti transaksi. | Aplikasi Autopsy berhasil mengembalikan berbagai jenis file yang terhapus, termasuk DOCX, XLSX, PDF, dan PNG. Hasil analisis ini dapat digunakan sebagai bukti digital yang sah secara ilmiah dan hukum. Penelitian juga menyimpulkan bahwa Autopsy memiliki kinerja yang lebih baik dibandingkan dengan Belkasoft Evidence Center dalam hal pemulihan data yang dihapus. | Penelitian ini relevan dengan topik saya karena Keduanya fokus pada kejahatan digital, dengan dokumen membahas pemulihan file yang dihapus dan artikel Anda menyoroti peredaran informasi palsu di TikTok. Penggunaan alat forensik seperti Autopsy dalam dokumen juga relevan untuk teknik yang dapat diterapkan dalam analisis bukti digital tentang informasi palsu. |
| 31 | Sang Putu Febri Wira Pratama, I Gusti Ngurah Anom Cahyadi Putra, Muhammad Akbar Hamid, Calvin Christiana, I Ketut Kusuma Merdana. (2022).  Analisis Forensik Digital pada Aplikasi Twitter di Android sebagai Bukti Digital dalam Penanganan Kasus Prostitusi Online | Metode National Institute of Justice (NIJ): Metode ini terdiri dari lima tahapan yaitu:  Preparation (Persiapan),  Collection (Pengumpulan),  Examination (Pemeriksaan),  Analysis (Analisis),  Reporting (Pelaporan). | Tujuan dari penelitian ini adalah untuk membantu penyidik dalam menyelesaikan masalah prostitusi online yang terjadi di aplikasi Twitter dengan menggunakan perangkat lunak forensik untuk memperoleh bukti digital yang sah. | Penelitian ini menunjukkan bahwa dengan metode NIJ, penyidik dapat menemukan percakapan yang berkaitan dengan prostitusi online dalam database aplikasi Twitter. Hasil analisis tersebut dapat digunakan sebagai bukti digital yang dapat dipertanggungjawabkan secara hukum. | Penelitian ini relevan dengan topik saya karena penelitian menggunakan metode NIJ yang sama, menawarkan kerangka sistematis untuk analisis forensik digital. Penelitian tentang prostitusi online maupun informasi palsu menunjukkan pentingnya penanganan kejahatan siber, yang memerlukan pengumpulan dan analisis bukti digital. |
| 32 | Imam Riadi, Rusydi Umar, Muhammad Irwan Syahib. (2021). Akuisisi Bukti Digital Viber Messenger Android Menggunakan Metode National Institute of Standards and Technology (NIST) | Penelitian ini menggunakan metode NIST yang terdiri dari empat tahap: Collection, Examination, Analysis, dan Reporting. Metode ini diterapkan untuk mengumpulkan dan menganalisis bukti digital dari aplikasi Viber di smartphone Android. Tiga alat forensik yang digunakan adalah MOBILedit Forensic Express, Belkasoft, dan Autopsy. | Untuk membuktikan apakah bukti digital yang dihapus dari aplikasi Viber dapat diakuisisi kembali menggunakan alat forensik, serta untuk mengevaluasi kinerja masing-masing alat dalam proses akuisisi tersebut. | Penelitian menunjukkan bahwa MOBILedit Forensic Express dan Belkasoft berhasil mengakuisisi bukti digital dengan tingkat keberhasilan 100% untuk akun, kontak, gambar, dan video. Namun, keduanya hanya berhasil mendapatkan 50% dari bukti percakapan teks. Sementara itu, Autopsy tidak memberikan hasil yang diharapkan, dengan hasil nol (zero result) karena tidak mampu membuka enkripsi file database Viber. | Penelitian ini relevan dengan topik saya karenamenggunakan metodologi forensik digital, yaitu NIST dan NIJ, menunjukkan kesamaan dalam pendekatan untuk mengumpulkan dan menganalisis bukti. Fokus pada aplikasi media sosial menjadi sentral, di mana Viber dan Tiktok berfungsi sebagai platform yang relevan dalam konteks kejahatan siber. |
| 33 | Sunardi, Imam Riadi, Joko Triyanto. (2021). Forensics Mobile Layanan WhatsApp pada Smartwatch Menggunakan Metode National Institute of Justice | Penelitian ini menggunakan metode National Institute of Justice (NIJ) yang meliputi tahapan:  Identification: Pemilihan dan pemilahan barang bukti digital.  Collection: Pengumpulan data dari sumber yang akurat. Examination: Pemeriksaan data untuk memastikan keaslian. Analysis: Analisis data yang diperoleh. Reporting: Pelaporan hasil analisis. | Tujuan dari penelitian ini adalah untuk mengungkap barang bukti digital dalam identifikasi kejahatan siber yang menggunakan aplikasi WhatsApp pada perangkat smartwatch. Penelitian ini bertujuan untuk mengevaluasi efektivitas metode forensik dalam mengumpulkan data digital | Penelitian menunjukkan bahwa menggunakan metode NIJ dan alat Wondershare Dr. Fone, penelitian berhasil mengumpulkan data berupa foto, video, kontak, dan dokumen dengan tingkat keberhasilan 100%. Namun, penelitian juga menemukan bahwa alat tersebut tidak dapat mengakses riwayat panggilan dan chat messenger, yang menunjukkan keterbatasan dalam pengembalian data yang hilang. | Penelitian ini relevan dengan topik saya karena kedua penelitian menggunakan metode NIJ, yang menyediakan kerangka kerja sistematis untuk analisis forensik digital. Fokus pada kejahatan siber menunjukkan relevansi dalam konteks penyalahgunaan platform digital. Selanjutnya, keduanya dapat menggunakan alat forensik serupa untuk mengumpulkan bukti digital. |
| 34 | Wahyudi Agustiono, Dini Wulan Suci, Novi Prastiti. (2024). Analisis Forensik Digital Menggunakan Metode NIST untuk Memulihkan Barang Bukti yang Dihapus | Penelitian ini menggunakan metode NIST SP 800-86, yang terdiri dari empat tahapan: Pengumpulan (Collection): Mengidentifikasi dan mengamankan barang bukti. Pemeriksaan (Examination): Menggunakan alat forensik untuk mengekstrak informasi relevan.  Analisis (Analysis): Menganalisis hasil pemeriksaan untuk mendapatkan informasi yang diperlukan. Pelaporan (Reporting): Menyusun laporan berdasarkan hasil analisis. | Tujuan penelitian ini adalah untuk menyelidiki dan memulihkan data yang telah dihapus menggunakan metode NIST SP 800-86, serta membuktikan efektivitas dan batasan metode tersebut dalam pemulihan barang bukti digital. | Penelitian menunjukkan bahwa data yang dihapus menggunakan metode Shift+Delete dapat dipulihkan sepenuhnya dengan tingkat keberhasilan 100% pada media flashdisk dan harddisk. Namun, data yang dihapus melalui formatting tidak dapat dipulihkan, menunjukkan bahwa metode penghapusan ini lebih permanen. | Penelitian ini relevan dengan topik saya karena keduanya menggunakan metodologi forensik untuk menganalisis data digital, meskipun dengan pendekatan berbeda. Penelitian pertama fokus pada pemulihan data yang dihapus dalam konteks kejahatan siber, sedangkan artikel Anda berfokus pada peredaran informasi palsu di media sosial. |
| 35 | Desti Mualfah, Afdel Viransa, Hasanatul Fu’adah Amran. (2023). Akuisisi Bukti Digital pada Aplikasi TamTam Messenger Menggunakan Metode National Institute of Justice (NIJ) | Penelitian ini menggunakan metode National Institute of Justice (NIJ) untuk proses digital forensik, khususnya mobile forensik, dalam mengidentifikasi dan mengakuisisi bukti digital yang dihapus dari aplikasi TamTam Messenger. | Untuk menemukan dan mengembalikan bukti digital yang telah dihapus dari aplikasi TamTam Messenger dengan menggunakan tools forensik MobileEdit dan metode NIJ. | Penelitian menunjukkan bahwa metode NIJ dan penggunaan tools MobileEdit berhasil mengembalikan bukti digital yang dihapus oleh pelaku kejahatan cyberbullying di aplikasi TamTam Messenger. Metode ini efektif dalam proses identifikasi dan akuisisi bukti digital pada smartphone. | Penelitian ini relevan dengan topik saya karena kedua penelitian menggunakan metode National Institute of Justice (NIJ) yang sama, menekankan penerapan metodologi forensik yang sistematis. Keduanya berfokus pada pengumpulan dan analisis bukti digital, |
| 36 | Pande Aditya Pratama Putra, Ni Kadek Sukerti, I Ketut Putu Suniantara. (2024). Akusisi Forensik Digital Pada Aplikasi Google Drive Sebagai Bukti Digital Dalam Penyelidikan Kasus Pornografi | Penelitian ini menggunakan metode National Institute of Justice (NIJ) yang meliputi lima fase:  Identification: Mengklasifikasikan barang bukti.  Collection: Mengumpulkan data dari sumber yang relevan. Examination: Memeriksa keaslian data. Analysis: Menganalisis bukti digital. Reporting: Melaporkan hasil analisis dan memberikan rekomendasi. | Tujuan penelitian ini adalah untuk mengumpulkan bukti forensik digital yang kuat guna menangani penyebaran konten pornografi melalui aplikasi Google Drive pada perangkat Android, serta untuk menanggapi dampak negatif dari kejahatan tersebut. | Penelitian menunjukkan bahwa penggunaan tools MobilEdit Forensics dan Magnet AXIOM efektif dalam mengumpulkan bukti digital dari aplikasi Google Drive. Hasil yang diperoleh dapat digunakan sebagai alat bukti dalam penanganan kasus pornografi. | Penelitian ini relevan dengan topik saya karena kedua penelitian menggunakan metode National Institute of Justice (NIJ), yang menyediakan kerangka kerja sistematis untuk pengumpulan dan analisis bukti digital. Kedua, fokus pada bukti digital sangat penting, dengan penelitian Anda menangani informasi palsu di TikTok sementara penelitian sebelumnya berfokus pada konten pornografi di Google Drive. |
| 37 | Dedek Julian, Tata Sutabri. (2023). Analisa Kinerja Aplikasi Digital Forensik Autopsy untuk Pengembalian Data Menggunakan Metode NIST SP 800-86 | NIST SP 800-86: Metode ini meliputi empat tahapan: pengumpulan bukti (collection), pemeriksaan (examination), analisis (analysis), dan pelaporan (reporting). Penelitian ini menggunakan aplikasi Autopsy untuk mengembalikan data dari flashdisk yang telah diformat. | Menganalisis kinerja aplikasi Autopsy dalam mengembalikan 70 file yang dihapus, termasuk dokumen, video, dan gambar, sebagai bukti digital dalam konteks pencurian data. | Aplikasi Autopsy berhasil mengembalikan 81,42% dari total 70 file yang dihapus, dengan rincian berupa 10 DOCX, 10 XLSX, 10 PDF, 6 TXT, 1 MP3, 10 MP4, dan 10 PNG. Kinerja aplikasi ini menunjukkan bahwa Autopsy merupakan alat yang efektif untuk pemulihan data dalam konteks forensik digital. | Penelitian ini relevan dengan topik saya karena keduanya menggunakan metodologi yang diakui, yaitu NIST SP 800-86 dan NIJ, untuk melakukan investigasi sistematis terhadap kasus kejahatan digital. Meskipun fokusnya berbeda—pencurian data dalam penelitian pertama dan penyebaran informasi palsu di TikTok dalam artikel kedua—keduanya bertujuan untuk mengidentifikasi dan menganalisis bukti digital yang relevan |
| 38 | Syifa Riski Ardiningtias, Sunardi, Herman. (2021). Investigasi Digital pada Facebook Messenger Menggunakan National Institute of Justice | Metode yang digunakan dalam penelitian ini adalah kerangka kerja National Institute of Justice (NIJ) untuk melakukan investigasi digital. Penelitian membandingkan dua alat forensik, yaitu MOBILEdit Forensics dan Wondershare Dr. fone, untuk memperoleh bukti digital terkait penyebaran konten pornografi. | Tujuan penelitian ini adalah untuk melakukan investigasi forensik terhadap aplikasi Facebook Messenger, khususnya dalam konteks penyebaran konten pornografi, dan membandingkan efektivitas dua alat forensik dalam mengembalikan data yang dihapus. | Penelitian menunjukkan bahwa MOBILEdit Forensics lebih efektif dalam mengidentifikasi dan mendapatkan bukti digital dibandingkan Wondershare Dr. fone, dengan tingkat keberhasilan 85,71% dibandingkan 28,57%. Hasil ini dapat digunakan sebagai bukti oleh investigator dalam menangani kasus kejahatan terkait penyebaran konten pornografi. | Penelitian ini relevan dengan topik saya karena menggunakan metode National Institute of Justice (NIJ) sebagai kerangka kerja untuk melakukan investigasi forensik digital, menunjukkan pendekatan sistematis dalam pengumpulan bukti. Meskipun fokus platformnya berbeda—Facebook Messenger dan TikTok—keduanya merupakan media sosial yang sering disalahgunakan untuk menyebarkan konten negatif. |
| 39 | Muhammad Fadil Fadillah dan Trihastuti Yuniati. (2023). Perbandingan Hasil Recovery Tools Mobile Forensic Di Smartphone Android Menggunakan Metode National Institute Of Justice (NIJ) | Penelitian ini menggunakan metode National Institute of Justice (NIJ), yang terdiri dari lima tahap: assessment, acquisition, examination, documentation, dan reporting. Penelitian ini menguji dua alat forensik mobile: Andriller (open source) dan MOBILedit Forensic Express Pro (berbayar). | Tujuan penelitian adalah untuk membandingkan efektivitas dua alat pemulihan data pada smartphone Android guna menentukan tingkat recovery data yang dapat dilakukan oleh masing-masing alat untuk keperluan penyelidikan dan akademis. | Dari hasil penelitian, MOBILedit Forensic Express Pro menunjukkan tingkat recovery data lebih tinggi (83,33%) dibandingkan dengan Andriller (50%). Kedua alat dapat digunakan tanpa akses root, tetapi MOBILedit mampu memulihkan data yang telah dihapus, sementara Andriller tidak. | Penelitian ini relevan dengan topik saya karena menggunakan metode National Institute of Justice (NIJ), yang menyediakan pendekatan sistematis untuk pengumpulan dan analisis bukti digital. Fokus utama pada forensik digital dalam kedua penelitian menunjukkan pentingnya analisis bukti untuk mendukung penyelidikan. |
| 40 | Faiz Muqorrir Kaffah, Siti Nur, Adi Fitrianto, Undang Syaripudin, Darwan. (2022). Analisis Live Forensics Pada SSD SATA Fungsi TRIM Menggunakan Metode National Institute of Justice (NIJ) | Penelitian ini menggunakan metode kualitatif dengan penerapan teknik Live Forensics. Metode yang digunakan adalah National Institute of Justice (NIJ) yang terdiri dari lima tahapan: identification, collection, examination, analysis, dan reporting | Tujuan dari penelitian ini adalah untuk mengetahui tahapan pemeriksaan dan analisis pada SSD yang memiliki fungsi TRIM, serta untuk mengevaluasi efektivitas pemulihan file dalam keadaan TRIM enable dan disable. | Pemulihan file dapat dilakukan dengan baik ketika fungsi TRIM dinonaktifkan, dengan tingkat akurasi 90%. Ketika fungsi TRIM diaktifkan, hanya satu file dengan ekstensi .txt yang berhasil dipulihkan. File lainnya tidak dapat diakses atau rusak. Software Belkasoft tidak berhasil memulihkan file dalam kedua kondisi TRIM. | Penelitian ini relevan dengan topik saya karena berfokus pada forensik digital, meskipun objeknya berbeda; satu pada pemulihan data dari SSD dan yang lain pada analisis informasi palsu di TikTok. Penelitian ini menunjukkan pentingnya forensik digital dalam menangani kejahatan, tantangan yang serupa terkait perkembangan teknologi. |
| 41 | Syaza Dyah Utami, Carudin, Azhari Ali Ridha. (2021). Analisis Live Forensic pada Whatsapp Web untuk Pembuktian Kasus Penipuan Transaksi Elektronik | Penelitian ini menggunakan metodologi NIST (National Institute of Standards and Technology) yang terdiri dari tahapan:  Collection: Pengumpulan dan dokumentasi barang bukti. Examination: Pemeriksaan data digital yang diperoleh.  Analysis: Analisis bukti digital menggunakan tools seperti FTK Imager dan Browser History Viewer. Reporting: Pelaporan hasil analisis dan evaluasi bukti. | Tujuan penelitian ini adalah untuk membuktikan kasus penipuan transaksi elektronik pada Whatsapp Web dengan menggunakan metode live forensic, serta untuk mencari bukti digital yang relevan dari perangkat yang masih dalam keadaan menyala. | Penelitian berhasil menemukan bukti digital berupa teks percakapan, timestamp, dan informasi identitas korban dan pelaku. Bukti digital yang diperoleh dinyatakan sah berdasarkan UU Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik. | Penelitian ini relevan dengan topik saya karena keduanya menggunakan metodologi sistematis untuk mengumpulkan, menganalisis, dan melaporkan bukti digital. Penelitian pertama berfokus pada Whatsapp, sedangkan artikel Anda meneliti TikTok, mencerminkan relevansi dalam memahami kejahatan siber di berbagai media. Pencarian dan analisis bukti digital, serta keabsahan bukti yang dapat digunakan di pengadilan. |
| 42 | Imam Riadi, Sunardi, Takdir Ruslan. (2022). Forensik Multimedia Berbasis Mobile Menggunakan Metode National Institute of Justice (NIJ) | Penelitian ini menggunakan metode National Institute of Justice (NIJ) yang mencakup tahapan identifikasi, solusi, uji coba, evaluasi, dan laporan hasil. | Tujuan penelitian adalah untuk memperoleh bukti digital terkait skenario penjualan obat secara online melalui Facebook Messenger dan WhatsApp dengan menggunakan empat alat forensik: Belkasoft, Oxygen, MOBILedit, dan Magnet Axiom. | Data multimedia berupa audio dan video yang dihapus dari WhatsApp dan Facebook Messenger masih bisa dikembalikan menggunakan aplikasi Belkasoft, Oxygen, dan Magnet Axiom. Sementara itu, MOBILedit tidak mampu mengembalikan data yang dihapus. | Penelitian ini relevan dengan topik saya karena keduanya menggunakan metode NIJ sebagai kerangka kerja penelitian. Kedua, fokus pada platform digital berbeda, dengan penelitian pertama pada aplikasi pesan instan seperti WhatsApp dan Facebook Messenger, sedangkan artikel Anda berfokus pada Tiktok. |
| 43 | Irfan Maulana, Ardi Pujiyanta. (2024). Analisis Forensik Aplikasi Penipuan Berbasis Android Menggunakan Metode NIST | Penelitian ini menggunakan metode National Institute of Standards and Technology (NIST), yang terdiri dari empat tahapan:  Collection: Pengumpulan data dan bukti. Examination: Pemeriksaan data yang telah dikumpulkan.  Analysis: Analisis hasil pemeriksaan.  Reporting: Pelaporan hasil analisis. | Tujuan dari penelitian ini adalah untuk melakukan analisis forensik terhadap aplikasi penipuan berbasis Android yang menggunakan platform WhatsApp, serta untuk mendapatkan informasi digital yang relevan sebagai bukti dalam kasus penipuan. | Penelitian ini menyimpulkan bahwa aplikasi berbahaya yang dikirimkan melalui WhatsApp bertujuan untuk mencuri data pribadi korban, termasuk SMS yang berisi kode OTP dari rekening bank. Proses ekstraksi dan analisis database percakapan WhatsApp menunjukkan bahwa aplikasi tersebut mengandung malware yang dapat mengakses dan mencuri informasi penting dari korban. | Penelitian ini relevan dengan topik saya karena keduanya menggunakan metodologi forensik yang terstandarisasi, yaitu NIST dan NIJ, untuk menganalisis bukti digital. Kedua, fokus utama dari kedua penelitian adalah pada kejahatan digital, dengan penelitian pertama mengatasi penipuan melalui aplikasi Android dan yang kedua membahas penyebaran informasi palsu di TikTok. |
| 44 | Rizqi Rahmansyah, Carudin, Azhari Ali Ridha. (2021). Perbandingan Hasil Investigasi Barang Bukti Digital pada Aplikasi Facebook dan Instagram dengan Metode NIST | Metode yang digunakan dalam penelitian ini adalah metode NIST (National Institute of Standards and Technology) yang terdiri dari empat tahap: Collection: Pengumpulan data dan barang bukti.  Examination: Penyortiran dan penyeleksian data yang diperoleh.  Analysis: Analisis barang bukti yang telah dikategorikan.  Reporting: Pelaporan hasil analisis barang bukti digital. | Tujuan penelitian ini adalah untuk membandingkan jumlah barang bukti digital yang berhasil ditemukan dari aplikasi Facebook dan Instagram setelah dilakukan proses penghapusan oleh pelaku penyebaran hoaks dengan menggunakan metode mobile forensic. | bahwa aplikasi Instagram berhasil mendapatkan 75% dari total barang bukti digital, sedangkan Facebook hanya 37,5%. Ini membuktikan bahwa Instagram lebih efektif dalam menyimpan barang bukti digital dibandingkan Facebook. Selain itu, waktu pelaksanaan forensik setelah penghapusan juga mempengaruhi hasil yang diperoleh. | Penelitian ini relevan dengan topik saya karena fokus pada isu peredaran informasi palsu yang semakin marak di media sosial. Metodologi NIJ yang digunakan dalam analisis forensik digital memberikan kerangka kerja sistematis untuk mengidentifikasi dan menganalisis bukti terkait informasi palsu. Penelitian ini juga menekankan pentingnya teknik forensik dalam melacak jejak digital, |
| 45 | Meyti Eka Apriyani, Rahmad Alfian Maskuri, Muhammad Hasyim Ratsanjani, Agung Nugroho Pramudhita, Rawansyah. (2023). Digital Forensic Investigates Sexual Harassment on Telegram using Naïve Bayes | Metode penelitian yang digunakan adalah National Institute of Justice (NIJ) untuk analisis forensik, serta algoritma Naïve Bayes untuk mengklasifikasikan percakapan yang mengandung pelecehan seksual di aplikasi Telegram. | Tujuan penelitian ini adalah untuk mengevaluasi efektivitas alat forensik digital dan metode Naïve Bayes dalam mengidentifikasi percakapan yang mengandung pelecehan seksual di Telegram.. | bahwa algoritma Naïve Bayes dapat digunakan untuk mengklasifikasikan percakapan dengan tingkat akurasi yang tinggi (91.3%), dengan precision 100% dan recall 90%. Temuan ini menyoroti pentingnya penggunaan metode yang tepat dalam investigasi forensik digital untuk mengatasi masalah pelecehan seksual di platform online. | Penelitian ini relevan dengan topik saya karena keduanya meneliti aplikasi populer, yaitu Telegram dan TikTok, sebagai tempat terjadinya tindakan yang memerlukan analisis. Masing-masing penelitian bertujuan untuk mengidentifikasi dan mengklasifikasikan konten bermasalah, baik itu pelecehan seksual maupun informasi palsu |
| 46 | Budun Sarsono, Rini Indrayani. (2024). Analisis Live Forensics Keamanan Browser pada Marketplace (Studi Kasus: Tokopedia dan Bukalapak) | Metode yang digunakan adalah National Institute of Justice (NIJ), yang terdiri dari lima tahapan: Identification, Collection, Examination, Analysis, dan Reporting. Penelitian ini menerapkan skenario kasus pada 30 akun email di 30 perangkat berbeda untuk menganalisis penggunaan browser saat mengakses layanan belanja online. | Tujuan penelitian ini adalah untuk menganalisis dan mengevaluasi tingkat keamanan data saat mengakses layanan belanja online melalui browser, serta untuk membandingkan keamanan antara berbagai browser (Mozilla Firefox, Google Chrome, dan Opera). | Hasil penelitian menunjukkan bahwa Mozilla Firefox memiliki indeks keamanan tertinggi saat mengakses Tokopedia dan Bukalapak, sedangkan Google Chrome memiliki indeks keamanan terendah. Penelitian ini merekomendasikan penggunaan Mozilla Firefox untuk akses yang lebih aman ke kedua platform marketplace tersebut. | Penelitian ini relevan dengan topik saya karena keduanya menyoroti isu keamanan data dalam konteks digital, dengan fokus pada teknik forensik untuk mengungkap artefak yang relevan. Meskipun satu penelitian berfokus pada keamanan saat berbelanja online, dan yang lainnya pada penyebaran informasi palsu di media social. |
| 47 | Singgih Mitro S. dan Dadan Sukma. (2023). Penerapan Metode NIJ untuk Analisis Serangan DoS pada Perangkat IoT | Penelitian ini menggunakan metode National Institute of Justice (NIJ) yang mencakup tahapan:  Persiapan, Penanganan insiden, Identifikasi koleksi, Pengumpulan, Pemeriksaan, Analisis, Pelaporan | Tujuan dari penelitian ini adalah untuk menerapkan metode NIJ dalam menganalisis serangan Denial of Service (DoS) pada perangkat Internet of Things (IoT). Penelitian ini bertujuan untuk memahami karakteristik serangan DoS dan membantu dalam mengambil tindakan pencegahan. | Penelitian menunjukkan bahwa metode NIJ efektif untuk menganalisis serangan DoS pada perangkat IoT. Metode ini membantu dalam mendeteksi dan menganalisis serangan, serta memberikan dasar untuk tindakan pencegahan terhadap serangan di masa depan. | Penelitian ini relevan dengan topik saya karena keduanya berfokus pada pengumpulan dan analisis data yang diperlukan untuk mengidentifikasi bukti digital, baik dalam konteks serangan siber maupun penyebaran informasi palsu. Selain itu, tujuan keduanya adalah meningkatkan keamanan, dengan penelitian pertama mencegah serangan pada perangkat IoT dan artikel Anda mencegah penyebaran informasi palsu. |
| 48 | Imam Riadi, Anton Yudhana, Mush’ab Al Barra. (2021). Forensik Mobile pada Layanan Media Sosial LinkedIn | Penelitian ini menggunakan metode forensik statis yang diadopsi dari NIST (National Institute of Standard and Technology). Metode ini terdiri dari empat tahapan:  Pengumpulan (Collection),  Pemeriksaan (Examination),  Analisis (Analysis),  Presentasi (Presentation). | Tujuan penelitian ini adalah untuk menambah wawasan dan keterampilan di bidang forensik digital, khususnya dalam forensik mobile, serta untuk menemukan bukti digital terkait dengan kasus hoax lowongan kerja di LinkedIn. | Penelitian ini berhasil menemukan berbagai bukti digital, termasuk log aktivitas, status update, 17 password WiFi, 117 riwayat unduhan, dan 263 panggilan telepon. Hasil tersebut menunjukkan bahwa metode forensik yang diterapkan efektif dalam mengungkap bukti digital di media sosial. | Penelitian ini relevan dengan topik saya karena kedua penelitian menggunakan metodologi forensik yang diakui, yaitu NIST dan NIJ, untuk menemukan dan menganalisis bukti digital. fokus pada platform media social, LinkedIn dan TikTok. menunjukkan relevansi dalam konteks penyebaran informasi menyesatkan. |
| 49 | Alfiansyah Imanda Putra, Rusydi Umar, Abdul Fadlil. (2021). Penerapan Metode Localization Tampering dan Hashing untuk Deteksi Rekayasa Video Digital | Penelitian ini menggunakan metode digital forensik dengan pendekatan NIST untuk menganalisis video yang diduga telah dimanipulasi. Proses yang dilakukan meliputi:  Akuisisi data dari video yang dicurigai. Ekstraksi data untuk analisis lebih lanjut. Penggunaan algoritma Localization Tampering dan Hashing untuk mendeteksi perusakan video. Analisis histogram untuk membandingkan nilai histogram video asli dan video yang dimanipulasi. | Tujuan dari penelitian ini adalah untuk mendeteksi adanya manipulasi pada video digital dan memastikan keaslian video dengan menggunakan metode analisis yang tepat, yaitu analisis frame dan hash. | Bahwa beberapa frame video mengalami berbagai jenis manipulasi, seperti cropping, tiktoking, dan rotation. Analisis histogram dan nilai hash SHA-1 menunjukkan perbedaan signifikan antara video asli dan yang telah dimanipulasi, membuktikan bahwa video tersebut telah mengalami tampering. | Penelitian ini relevan dengan topik saya karena kedua penelitian berfokus pada digital forensik untuk mendeteksi manipulasi informasi digital. Kedua, meskipun menggunakan metodologi berbeda (NIST dan NIJ), keduanya bertujuan memastikan keabsahan analisis forensik. Selanjutnya, deteksi perubahan pada video menjadi tujuan utama, yang sangat relevan untuk mengidentifikasi konten manipulatif di TikTok. |
| 50 | Nyimas Chairunnisa Febriani, Alek Wijaya. (2023). Komparasi Kejahatan di Twitter dan Instagram dengan Pendekatan Digital Forensic Investigation | Penelitian ini menggunakan metode National Institute of Justice (NIJ), yang terdiri dari empat tahap:  Collection (Pengumpulan),  Examination (Pemeriksaan),  Analysis (Analisis),  Reporting (Laporan) | Tujuan penelitian ini adalah untuk Menganalisis dan membandingkan kejahatan yang terjadi di platform media sosial Twitter dan Instagram.  Menggunakan pendekatan digital forensic investigation untuk menghasilkan bukti digital yang dapat menunjukkan perbandingan kejahatan di kedua platform tersebut. | Kejahatan penipuan jual beli di Twitter lebih banyak menarik perhatian dibandingkan dengan penipuan di Instagram, terutama yang berkaitan dengan produk yang diiklankan oleh public figure. Di Instagram, penipuan yang paling banyak dilaporkan berasal dari akun online shop reseller grosir. | Penelitian ini relevan dengan topik saya karena menggunakan metodologi National Institute of Justice (NIJ), yang memberikan pendekatan sistematis dalam pengumpulan dan analisis data digital. Selain itu, kedua penelitian berfokus pada kejahatan digital di media sosial, dengan penelitian pertama menganalisis penipuan di Twitter dan Instagram, sementara artikel Anda mengeksplorasi informasi palsu di Tiktok. |
| 51 | Harno Supardin, Ramdan Satra, Muh. Arfah Asis, Ming Foey Teng. (2022). Comparison Analysis of Digital Forensic Tools on Instagram Messenger using The National Institute of Standards and Technology (NIST) Method | Penelitian ini menggunakan metode NIST (National Institute of Standards and Technology) yang meliputi empat tahap:  Collection,  Examination,  Analysis,  Reporting. | Tujuan dari penelitian ini adalah untuk membandingkan kinerja alat forensik digital dalam memperoleh bukti digital dari Instagram Messenger, serta untuk menentukan akurasi masing-masing alat dalam mengembalikan data yang dihapus. | Penelitian menunjukkan bahwa alat Magnet Axiom Forensic memiliki kinerja yang lebih baik dengan akurasi 76.92%, dibandingkan dengan MOBILedit Forensic yang hanya mencapai 69.23%. Meskipun kedua alat tersebut tidak sepenuhnya efektif dalam mengembalikan pesan teks yang dihapus, mereka mampu memulihkan gambar dan video dengan baik. | Penelitian ini relevan dengan topik saya karena keduanya menggunakan metodologi terstruktur untuk analisis forensik, meskipun berbeda dalam pendekatan—NIST dan NIJ. Fokus utama dari kedua penelitian adalah pada media sosial, di mana penelitian sebelumnya menyoroti cybercrime di Instagram, sementara artikel Anda mengkaji informasi palsu di Tiktok. |
| 52 | Nabilla Fatmah dan Rini Indrayani. (2022). Analisis Forensik Digital pada Solid State Drive Fungsi TRIM Menggunakan Tools Autopsy dan OSForensics | Metode statis dengan menerapkan standar forensik digital SNI Acquisition 27037:2014. Proses akuisisi dilakukan pada SSD dengan fungsi TRIM diaktifkan dan dinonaktifkan, diikuti oleh proses recovery menggunakan tools Autopsy dan OSForensics. | Tujuan penelitian ini adalah untuk menganalisis perbandingan efektivitas akuisisi dan recovery data pada SSD dengan fungsi TRIM yang diaktifkan dan dinonaktifkan, serta untuk menentukan waktu akuisisi dan tingkat keberhasilan recovery menggunakan dua tools tersebut. | Tool OSForensics memiliki waktu akuisisi yang lebih cepat dibandingkan Autopsy, dengan 228 menit pada SSD TRIM enable dan 231 menit pada TRIM disable. Sementara itu, tingkat keberhasilan recovery pada kedua tools adalah 0% untuk SSD TRIM enable dan 100% untuk TRIM disable, menunjukkan bahwa recovery data lebih berhasil pada kondisi TRIM dinonaktifkan. | Penelitian ini relevan dengan topik saya karena keduanya membahas forensik digital, yaitu analisis dan pemulihan data yang hilang atau dihapus, meskipun dengan fokus yang berbeda. Metodologi yang digunakan juga beragam, dengan Anda menerapkan NIJ dan penelitian sebelumnya menggunakan SNI Acquisition 27037:2014. Tujuan utama dari kedua penelitian adalah untuk mengidentifikasi dan memulihkan informasi yang relevan. |
| 53 | Soni, Regiolina Hayami, Muhammad Hamadi. (2022). Akuisisi Bukti Digital Pada Aplikasi Michat di Smartphone Menggunakan Metode National Institute of Standards and Technology (NIST) | Penelitian ini menggunakan metode National Institute of Standards and Technology (NIST) untuk melakukan analisis digital forensik terhadap aplikasi Michat pada smartphone. Metode ini meliputi tahapan seperti pengumpulan (collection), pemeriksaan (examination), analisis (analysis), dan pelaporan (reporting) bukti digital. | Tujuan dari penelitian ini adalah untuk mendapatkan bukti digital pada aplikasi Michat yang dapat digunakan sebagai barang bukti kejahatan, serta untuk mengevaluasi hasil akuisisi menggunakan berbagai alat forensik. | Penelitian menunjukkan bahwa menggunakan MobileEdit Forensic lebih efektif dibandingkan Wondershare Dr.Fone dalam mengembalikan data yang telah dihapus. MobileEdit berhasil mengembalikan 40 data dari 41 yang dipersiapkan, sementara Wondershare hanya berhasil mengembalikan 23 data. Hasil ini merekomendasikan penggunaan MobileEdit sebagai alat forensik yang lebih handal dalam kasus kejahatan digital. | Penelitian ini relevan dengan topik saya karena keduanya menggunakan pendekatan forensik digital, dengan NIST pada penelitian Michat dan NIJ pada artikel Anda, untuk memastikan akurasi dan integritas bukti. Penelitian pertama berfokus pada Michat dalam konteks cybercrime, sedangkan artikel Anda meneliti Tiktok dan informasi palsu, menunjukkan relevansi platform digital dalam kejahatan. |
| 54 | Muhammad Immawan Aulia, Panggah Widiandana, Latifah Iriani, Muhammad Fauzan Gustafi, Muhammad Azam Hasani. (2024). Application of Data Recovery Tools in Flash Drive Forensic Data Acquisition | Metode yang digunakan dalam penelitian ini adalah Statik Forensik. Penelitian ini berfokus pada pemeriksaan salinan disk untuk mengeluarkan konten memori, seperti file yang dihapus dan riwayat pengguna, menggunakan alat pemulihan data seperti Disk Drill. | Tujuan penelitian ini adalah untuk memulihkan data dari flash drive yang tidak dapat diakses setelah dicabut secara paksa. Penelitian ini bertujuan untuk menunjukkan efektivitas alat pemulihan data dan metode forensik dalam mengatasi masalah kehilangan data. | Penelitian ini menyimpulkan bahwa pemulihan data dari flash drive yang tidak dapat diakses dapat dilakukan menggunakan metode Forensik Statik dan aplikasi pemulihan data seperti Disk Drill. Dalam studi kasus ini, 7629 file berukuran 17,3 GB berhasil dipulihkan, dengan 49 file terpilih yang memiliki berbagai ekstensi. Alat ini terbukti efektif dalam mendukung investigasi digital. | Penelitian ini relevan dengan topik saya karena berada dalam ranah forensik digital, yang bertujuan untuk mengidentifikasi dan menganalisis bukti digital. Kedua, meskipun menggunakan metodologi yang berbeda—metode forensik statik dan metodologi National Institute of Justice (NIJ)—keduanya mengikuti prosedur sistematis dalam pengolahan bukti |
| 55 | Ermin, Muhammad Rizki Setyawan, Fitriyani Tella. (2023). Forensic Analysis Of Dana Applications Using The ACPO Framework | Penelitian ini menggunakan metode static forensik dengan framework dari Association of Chief Police Officers (ACPO). Proses penelitian meliputi:  Plan, Capture,  Analysis, Present. | Tujuan penelitian ini adalah untuk melakukan analisis forensik terhadap aplikasi DANA guna mengidentifikasi artefak yang dapat digunakan sebagai bukti digital dalam kasus kejahatan siber. | Penelitian menyimpulkan bahwa penggunaan framework ACPO efektif dalam memperoleh artefak. Namun, hasil analisis menunjukkan bahwa:  Belkasoft Evidence Center tidak berhasil menemukan artefak yang dapat dijadikan bukti digital.  MobilEdit Forensic Express Pro hanya berhasil menemukan foto pengguna dan screenshot transaksi. | Penelitian ini relevan dengan topik saya karena keduanya berada dalam ranah forensik digital, bertujuan untuk mengidentifikasi dan menganalisis bukti digital terkait kejahatan siber. Metodologi yang digunakan berbeda, yaitu framework ACPO untuk DANA dan metodologi NIJ untuk artikel Anda, tetapi keduanya memberikan panduan sistematis dalam proses forensik. |
| 56 | Sari Amanda Putri, M. Wandriansyah, Fito Nardian, Alif Syahputra. (2023). Penerapan Keyword Search Module pada Autopsy | Metode yang digunakan dalam penelitian ini adalah analisis. Penelitian dilakukan melalui langkah-langkah seperti pengumpulan data dan informasi, analisis data menggunakan Autopsy, dan implementasi modul pencarian kata kunci. | Tujuan penelitian adalah untuk mendokumentasikan dan mengevaluasi penerapan modul pencarian kata kunci pada Autopsy, serta untuk mengeksplorasi efektivitasnya dalam mendukung proses investigasi forensik digital. | Pencarian kata kunci pada Autopsy berhasil mengidentifikasi bukti digital yang relevan. Hasil analisis memberikan pemahaman lebih lanjut tentang aktivitas pada perangkat digital, waktu kejadian, dan potensi bukti yang dapat mendukung penyelidikan forensik. Penelitian ini menyarankan untuk melakukan validasi lebih lanjut dan memperluas pencarian untuk meningkatkan efektivitas analisis. | Penelitian ini relevan dengan topik saya karena keduanya berada dalam ranah forensik digital, dengan fokus pada identifikasi bukti relevan dari data digital. Penelitian pertama menggunakan modul pencarian kata kunci untuk menemukan bukti dengan efisien, sedangkan artikel Anda mengadopsi metodologi National Institute of Justice (NIJ) untuk menganalisis informasi palsu. |
| 57 | Anton Yudhana, Imam Riadi, Budi Putra. (2022). Analisis Kinerja Perangkat Lunak Forensic Imaging Pada Sistem Operasi Linux Menggunakan Metode Static Forensic | Penelitian ini menggunakan metode static forensic, yang merupakan standar dalam penanganan barang bukti setelah perangkat dimatikan. Kerangka kerja yang digunakan adalah kerangka kerja dari National Institute of Standards and Technology (NIST), yang mencakup langkah-langkah collection, examination, analysis, dan reporting. | Tujuan penelitian ini adalah untuk menganalisis dan menemukan perbedaan kinerja antara perangkat lunak forensic imaging yang berjalan pada sistem operasi Linux, dengan penekanan pada keberhasilan duplikasi yang harus sesuai dengan keaslian barang bukti. | Hasil penelitian menunjukkan bahwa FTK Imager CLI memiliki waktu proses yang lebih cepat dibandingkan dengan DC3DD dan DDrescue. Meskipun FTK Imager menghasilkan file dengan ekstensi yang berbeda, semua perangkat lunak berhasil melakukan imaging dengan validasi hash yang sama, membuktikan integritas data. | Penelitian ini relevan dengan topik saya karena menggunakan metodologi standar dalam analisis bukti digital, dengan penelitian Anda berlandaskan pada National Institute of Justice (NIJ) dan penelitian sebelumnya pada National Institute of Standards and Technology (NIST). Fokus utama mereka adalah pada forensik digital, meskipun di konteks yang berbeda—satu pada imaging bukti, dan yang lainnya pada validitas informasi palsu. |
| 58 | Kadek Dwi Oka Mahendra dan I Komang Ari Mogi. (2021). Digital Forensic Analysis of Michat Applications on Android as Digital Proof in Handling Online Prostitution Cases | Metode National Institute of Justice (NIJ): Metode ini memiliki lima tahap dasar dalam proses forensik, yaitu persiapan, pengumpulan, pemeriksaan, analisis, dan pelaporan. | Menganalisis bukti digital dari aplikasi MiChat yang digunakan dalam kasus prostitusi online, serta memberikan solusi untuk mengatasi masalah tersebut melalui analisis forensik. | Penelitian ini berhasil menunjukkan bahwa dengan menggunakan metode NIJ, data penting dapat ditemukan dan dianalisis dari aplikasi MiChat, yang dapat digunakan sebagai bukti digital dalam penanganan kasus prostitusi online. | Penelitian ini relevan dengan topik saya karena metode ini memberikan kerangka kerja yang sistematis untuk melakukan analisis forensik digital, yang membantu dalam pengumpulan dan analisis data untuk mengidentifikasi bukti. |
| 59 | Anton Yudhana, Imam Riadi, Budi Putra. (2022). Analisis Kinerja Perangkat Lunak Forensic Imaging Pada Sistem Operasi Linux Menggunakan Metode Static Forensic | Metode yang digunakan adalah static forensic, yang merupakan standar penanganan setelah barang bukti dimatikan. Penelitian ini juga mengikuti kerangka kerja dari National Institute of Standards and Technology (NIST), yang terdiri dari empat langkah: collection, examination, analysis, dan reporting. | Tujuan penelitian ini adalah untuk menganalisis dan menemukan perbedaan kinerja di antara perangkat lunak forensic imaging yang berjalan pada sistem operasi Linux, dengan indikator keberhasilan duplikasi sesuai dengan keaslian barang bukti. | Penelitian menunjukkan bahwa FTK Imager memiliki waktu proses yang lebih cepat dibandingkan dengan DC3DD dan DDrescue. FTK Imager lebih cepat 2 menit 18 detik dari DC3DD dan 12 detik dari DDrescue. Semua perangkat lunak berhasil menghasilkan nilai hash yang valid, membuktikan bahwa mereka dapat digunakan untuk mengakuisisi barang bukti dalam kasus kejahatan siber. | Penelitian ini relevan dengan topik saya karena kedua penelitian menggunakan kerangka kerja dari lembaga terkemuka, yaitu NIST untuk penelitian pertama dan NIJ untuk artikel Anda, yang menunjukkan komitmen terhadap standar forensik. Selanjutnya, keduanya fokus pada forensik digital, dengan penelitian pertama menganalisis perangkat lunak untuk akuisisi bukti, sementara artikel Anda berfokus pada peredaran informasi palsu. |
| 60 | Nadia Ayu Isroh Maniar, Trihastuti Yuniati. (2022). Implementasi Mobile Forensik Pada Aplikasi MiChat dan Telegram Dengan Framework NIST 800-101 | Penelitian ini menggunakan metode NIST Special Publication 800-101 Revision 1, yang terdiri dari tahapan:  Preservation,  Acquisition ,  Examination & Analysis, Reporting. | Tujuan penelitian ini adalah untuk: Mengumpulkan dan menganalisis data dari aplikasi MiChat dan Telegram sebagai bukti dalam penyelidikan kasus kejahatan siber. | Kesimpulan dari penelitian ini adalah:  FTK Imager berhasil memperoleh lebih banyak barang bukti digital dibandingkan MOBILedit Forensic.  Bukti digital yang ditemukan termasuk gambar, video, dan voice note, sementara pesan teks tidak berhasil ditemukan. | Penelitian ini relevan dengan topik saya karena merupakan kerangka kerja yang diakui dalam analisis forensik. Meskipun fokus kejahatan berbeda—kejahatan siber di MiChat dan Telegram versus penyebaran informasi palsu di TikTok—keduanya menekankan pentingnya pengumpulan bukti digital untuk mendukung proses hukum |
| 61 | Khoirul Anam Dahlan, Anton Yudhana, Herman Yuliansyah. (2024). Analisis File Carving Solid State Drive Menggunakan Metode National Institute of Standards and Technology | Metode NIST: Metode ini digunakan untuk analisis forensik digital yang mencakup pengumpulan, pemeriksaan, analisis, dan pelaporan bukti digital. Dalam penelitian ini, perangkat lunak seperti Foremost dan Autopsy digunakan untuk melakukan file carving pada SSD yang telah dihapus. | Menyediakan solusi untuk mengembalikan file yang hilang dari Solid State Drive (SSD) menggunakan teknik file carving yang diperbarui, serta membandingkan tingkat keberhasilan dua perangkat lunak, yaitu Foremost dan Autopsy. | Setiap SSD memiliki karakteristik unik dalam hal teknologi dan sistem keamanan, sehingga hasil penelitian tidak dapat digeneralisasi untuk semua merek SSD. Meskipun tingkat keberhasilan pemulihan tidak mencapai 100%, ada harapan untuk perbaikan di masa depan dalam teknik pemulihan SSD. | Penelitian ini relevan dengan topik saya karena berfokus pada forensik digital dan penggunaan metodologi untuk analisis bukti. Artikel Anda membahas teknik untuk mengidentifikasi dan menganalisis informasi palsu di media sosial, khususnya TikTok, menggunakan kerangka dari NIJ untuk memastikan validitas analisis. |
| 62 | Reski Badillah, Andi Yulia Muniar, Abd. Rahman, Febri Hidayat Saputra, Mansyur, Supriadi Sahibu. (2023). Digital Forensic Evidence Analysis in Revealing Defamation on Social Media (Twitter) Using the Static Forensics Method | Penelitian ini menggunakan metode forensik statis untuk mengidentifikasi, mengumpulkan, dan menganalisis bukti digital terkait pencemaran nama baik di media sosial, khususnya Twitter. Prosesnya mencakup identifikasi, pengumpulan data dari perangkat target, analisis data menggunakan perangkat lunak forensik, dan pelaporan hasil analisis. | Tujuan dari penelitian ini adalah untuk menyelidiki dan mengidentifikasi bukti digital dalam kasus pencemaran nama baik di Twitter, serta mengoptimalkan proses penemuan bukti. Penelitian ini bertujuan untuk mengungkap bukti digital yang mungkin telah dihapus atau tidak lagi terlihat. | Penelitian ini berhasil menemukan 22 dari 28 data yang dilaporkan, dengan tingkat akurasi mencapai 79%. Penelitian menunjukkan bahwa metode forensik statis efektif dalam mengungkap bukti digital yang relevan dalam kasus pencemaran nama baik di media sosial, dan prosedur investigasi yang dilakukan sejalan dengan rantai bukti, menjamin keandalan bukti yang dikumpulkan. | Penelitian ini relevan dengan topik saya karena penelitian mengenai informasi palsu di TikTok sangat relevan dalam konteks forensik digital, karena platform media sosial ini sering digunakan untuk menyebarkan informasi yang tidak akurat. Metodologi National Institute of Justice menawarkan kerangka kerja yang sistematis untuk menyelidiki dan menganalisis bukti digital. |
| 63 | I Putu Denny Indra Putra, I Ketut Gede Suhartana. (2021). Cyberbullying Analysis On Whatsapp Messenger Using The National Institute Of Justice (NIJ) Method | Penelitian ini menggunakan metode National Institute of Justice (NIJ) yang terdiri dari lima tahap yaitu Preparation (Persiapan), Collection (Pengumpulan), Examination (Pemeriksaan), Analysis (Analisis), Reporting (Pelaporan) | Tujuan dari penelitian ini adalah untuk membantu menyelesaikan masalah cyberbullying di media sosial, khususnya di WhatsApp Messenger, melalui tindakan forensik mobile menggunakan metode NIJ. | Penelitian ini berhasil menunjukkan bahwa dengan menggunakan metode NIJ dan perangkat lunak forensik seperti MOBILedit Forensic dan DB Browser for SQLite, dapat diperoleh bukti digital berupa pesan bullying antara pelaku dan korban. Hasil analisis ini dapat digunakan sebagai bukti dalam kasus | Penelitian ini relevan dengan topik saya karena analisis forensik digital mengenai cyberbullying di WhatsApp Messenger dan peredaran informasi palsu di TikTok, menggunakan metode National Institute of Justice (NIJ) sebagai kerangka kerja. Keduanya berfokus pada media sosial sebagai platform yang dapat disalahgunakan, dengan penelitian pertama menangani cyberbullying dan yang kedua mengatasi informasi palsu. |
| 64 | Muhammad Immawan Aulia, Panggah Widiandana, Latifah Iriani, Muhammad Fauzan Gustafi, Muhammad Azam Hasani. (2022). Penerapan Tool Recovery Data dalam Akuisisi Data Forensik Flashdrive | Penelitian ini menggunakan metode **Forensik Statik**, yang berfokus pada pemeriksaan duplikat media penyimpanan untuk mengeluarkan konten memori, termasuk file yang dihapus dan riwayat aktivitas. Alat yang digunakan dalam penelitian ini adalah **Disk Drill** untuk melakukan pemulihan data dari flashdrive yang tidak dapat diakses. | Tujuan dari penelitian ini adalah untuk mendemonstrasikan bagaimana data yang hilang dari flashdrive dapat dipulihkan setelah dicabut secara paksa selama proses transfer data, serta untuk menunjukkan efektivitas alat pemulihan data dalam menemukan dan memulihkan file yang hilang. | Bahwa pemulihan data dari flashdrive yang tidak dapat diakses dapat dilakukan dengan metode Forensik Statik dan alat pemulihan data yang tepat. Alat Disk Drill berhasil memulihkan 7629 file dengan total ukuran 17,3 GB dari partisi yang tidak teralokasikan, serta berhasil memulihkan 49 file terpilih dengan berbagai ekstensi, menunjukkan kemampuan alat tersebut dalam membantu investigasi digital dan pemulihan data. | Penelitian ini relevan dengan topik saya karena berfokus pada pengumpulan dan analisis data digital untuk tujuan investigasi, meskipun menggunakan metodologi yang berbeda; penelitian pemulihan data menggunakan metode Forensik Statik, sedangkan artikel Anda menggunakan metodologi National Institute of Justice (NIJ). |
| 65 | Latifah Iriani dan Muhammad Nasir Hafizh. (2023). Analisis Forensik Jaringan Terhadap Serangan Spoofing Menggunakan Metode Network Forensic Development Life Cycle | Penelitian ini menggunakan metode Network Forensics Development Life Cycle (NFDLC). Metode ini terdiri dari beberapa tahapan yang terstruktur dan berurutan, yaitu Initiation, Acquisition, Implementation, Operation, Disposition | Tujuan dari penelitian ini adalah untuk menemukan informasi bukti serangan Address Resolution Protocol (ARP) Spoofing termasuk alamat MAC address penyerang dan korban serta waktu terjadinya serangan. | Penelitian ini berhasil mendeteksi serangan ARP Spoofing pada komputer korban dengan identitas pelaku yang memiliki IP Address 192.168.10.254 dan MAC Address E4-8D-8C-A4-88-06. Metode NFDLC terbukti efektif dalam tahapan investigasi serangan ARP Spoofing, mulai dari identifikasi hingga pelaporan. | Penelitian ini relevan dengan topik saya karena pada forensik digital untuk menganalisis dan mengidentifikasi bukti dari aktivitas ilegal di dunia digital. Meskipun menggunakan metodologi yang berbeda, NFDLC untuk penelitian pertama dan NIJ keduanya bertujuan memberikan kerangka kerja sistematis dalam analisis forensik. |
| 66 | Bagas Yoga Prasetyo, Imam Riadi. (2021). Investigation Cyberbullying on Kik Messenger using National Institute of Standards Technology Method | Penelitian ini menggunakan metode National Institute of Standards Technology (NIST), Pengumpulan, Uji Coba, Analisis, Pelaporan. | Tujuan dari penelitian ini adalah untuk menganalisis proses investigasi atau forensik digital dalam kasus cyberbullying yang terjadi di aplikasi Kik Messenger dan menghasilkan bukti digital menggunakan metode NIST. | Penelitian menunjukkan bahwa terdapat bukti cyberbullying dalam percakapan grup di Kik Messenger, dengan 26 kalimat mengandung kata "buluk," yang mencerminkan tindakan bullying. Persentase kalimat yang mengandung kata tersebut adalah 5,92% dari total percakapan. | Penelitian ini relevan dengan topik saya karena keduanya menggunakan metode forensik untuk mengidentifikasi dan menganalisis bukti dari media sosial, dengan fokus pada platform yang berbeda; Kik Messenger dan TikTok. Isu keamanan yang diangkat, seperti cyberbullying dan penyebaran informasi palsu |
| 67 | Rizdqi Akbar Ramadhan, Desti Mualfah. (2021). Implementasi Metode National Institute of Justice (NIJ) Pada Fitur TRIM SOLID STATE DRIVE (SSD) Dengan Objek Eksperimental Sistem Operasi Windows, Linux dan Macintosh | Penelitian ini menggunakan metode Digital Forensik berdasarkan framework National Institute of Justice (NIJ) yang terdiri dari lima tahapan: Identification, Collection, Examination, Analysis, Reporting. | Tujuan dari penelitian ini adalah untuk menganalisis efektivitas fitur TRIM pada SSD dalam konteks digital forensik, serta membandingkan kemampuan recovery data antara sistem operasi Windows, Linux, dan Macintosh. | Penelitian menunjukkan bahwa Windows memiliki potensi recovery data yang lebih baik dibandingkan Linux dan Macintosh.  Pada konfigurasi TRIM enable, data di Windows dapat terdeteksi meskipun dalam status corrupt, sedangkan pada Linux dan Macintosh, recovery tidak berhasil. | Penelitian ini relevan dengan topik saya karena keduanya menggunakan metodologi NIJ sebagai kerangka kerja untuk analisis forensik digital, yang mencakup identifikasi, pengumpulan, pemeriksaan, analisis, dan pelaporan bukti. Kedua, fokus pada investigasi digital menjadi pusat perhatian, di mana kedua penelitian menunjukkan pentingnya teknik forensik dalam menghadapi tantangan di dunia digital. |
| 68 | Novi Krisdayanti dan Indra Gunawan, (2022). Analisis Keamanan Aplikasi Chat Android Pihak Ketiga Atau Non Playstore Menggunakan Digital Forensics | Penelitian ini menggunakan dua metode:  Analisis Statis: Menggunakan Wireshark untuk merekam aktivitas jaringan.  Analisis Dinamis: Menggunakan Network Miner untuk mengumpulkan data lalu lintas jaringan. | Tujuan dari penelitian ini adalah untuk mengetahui tingkat keamanan dari aplikasi chat GB WhatsApp, Telegram Mod, MiChat Mod, WeChat Mod, dan Line Mod. | Penelitian menunjukkan bahwa semua aplikasi yang diteliti memiliki izin akses yang berbahaya dan terdapat bukti kebocoran data dalam chat pribadi, dengan tingkat keamanan yang masih rendah (Level 1). | Penelitian ini relevan dengan topik saya karena pentingnya keamanan data dan privasi pengguna menjadi fokus utama dalam kedua penelitian. Analisis data dilakukan untuk mengevaluasi risiko, baik dalam kebocoran data aplikasi chat maupun penyebaran informasi palsu. |
| 69 | Imam Riadi, Sunardi, Panggah Widiandana. (2022). Cyberbullying Detection on Instant Messaging Services using Rocchio and Digital Forensics Research Workshop Framework | Penelitian ini menggunakan:  Digital Forensics Research Workshop (DFRWS) Framework: Sebagai metode ilmiah untuk akuisisi dan analisis bukti digital. Rocchio Method: Digunakan untuk mengidentifikasi kasus cyberbullying melalui umpan balik relevansi dan perhitungan TF-IDF untuk analisis teks. | Tujuan penelitian ini adalah untuk:  Mengakuisisi bukti digital dari aplikasi WhatsApp.  Mendeteksi dan menganalisis kasus cyberbullying dalam grup pesan menggunakan metode Rocchio. | Terdapat bukti valid yang menunjukkan terjadinya cyberbullying dalam skenario yang diteliti, dengan nilai tertinggi (0.25) yang melebihi ambang batas (0.15), menandakan adanya beberapa pelaku bullying dalam grup tersebut. | Penelitian ini relevan dengan topik saya karena fokus utama keduanya adalah pada pengumpulan dan analisis bukti dari aplikasi berbasis digital, di mana satu berfokus pada WhatsApp dan yang lainnya pada TikTok. Selain itu, kedua penelitian ini bertujuan untuk mendeteksi dan mencegah kejahatan siber, baik itu cyberbullying maupun penyebaran informasi palsu. |
| 70 | Muhardinata, Ahmad Luthfi, Erika Ramadhani. (2023). Teknik Disk Carving untuk Recovery Solid State Drive Volume ReFS dan NTFS dengan Fitur TRIM | Penelitian ini menggunakan metode forensik langsung sesuai dengan Standar Nasional Indonesia (SNI) 27037:2014. Metode ini dipilih untuk memungkinkan pengambilan data secara lebih efektif dengan menggunakan alat seperti FTK Imager. | Tujuan dari penelitian ini adalah untuk menguji pengaruh Teknik Disk Carving pada SSD dengan volume ReFS dan NTFS, serta untuk memahami bagaimana fitur TRIM mempengaruhi pemulihan data yang telah dihapus secara permanen. | Penelitian menunjukkan bahwa teknik disk carving dapat digunakan untuk memulihkan data dari file sistem yang rusak. Hasil menunjukkan bahwa pada SSD dengan TRIM diaktifkan, data yang berhasil dipulihkan sekitar 9% untuk NTFS dan 0% untuk ReFS. | Penelitian ini relevan dengan topik saya karena Kedua penelitian menggunakan pendekatan forensik, dengan artikel Anda mengadopsi metodologi National Institute of Justice (NIJ), menunjukkan konsistensi dalam standar forensik yang digunakan. Teknik pemulihan data yang efektif sangat penting untuk mengidentifikasi dan membuktikan peredaran informasi palsu. |
| 71 | Arman Syah Putra, Nurul Aisyah, Safrizal. (2022). Analisis Pengolahan Data Forensik pada Solid State Drive (SSD) Menggunakan Framework GRR Rapid Response | Metode yang digunakan dalam penelitian ini adalah Literature Review, Mengkaji referensi yang relevan terkait pengolahan data forensik. Uji Coba Melakukan percobaan pada Solid State Drive (SSD) menggunakan metode tertentu untuk mengevaluasi respons HDD dalam pencarian data. | Tujuan Penelitian ini adalah untuk Menemukan data yang hilang dan data yang telah dihapus pada SSD dengan tindakan khusus. Menguji efektivitas framework GRR Rapid Response dalam pengujian data forensik. | Terdapat keberhasilan dalam pengujian yang menunjukkan klaim lebih dari 90% data yang akurat dapat ditemukan. Framework yang diuji dapat digunakan sebagai metode untuk pengambilan data forensik yang efektif. | Penelitian ini relevan dengan topik saya karena kedua penelitian menggunakan pendekatan forensik untuk menganalisis data digital, dengan tujuan mengumpulkan dan menganalisis bukti yang relevan. meskipun menggunakan metode dan tools yang berbeda—framework GRR dan metode NIJ dengan tools Autopsy—kedua penelitian berusaha membuktikan bahwa data digital dapat dianalisis untuk keperluan hukum. |
| 72 | Panji Wisnu Nugroho dan Nur Farida Liyana. (2024). Optimasi Pendapatan Pajak Melalui Kegiatan Forensik Digital untuk Tujuan Pajak | Metode Tinjauan Pustaka Untuk memahami implementasi kegiatan forensik digital. Metode Penelitian Lapangan Melalui wawancara dengan ahli forensik digital dan akademisi yang berpengalaman dalam penegakan hukum pajak. | Meninjau pelaksanaan kegiatan forensik digital dan dampaknya terhadap pendapatan pajak di Direktorat Jenderal Pajak, khususnya di Kantor Wilayah Pajak Jakarta Selatan I. | Implementasi kegiatan forensik digital telah sesuai dengan SOP yang berlaku, tetapi belum memberikan dampak signifikan terhadap pendapatan pajak. Terdapat beberapa hambatan, seperti jumlah ahli forensik digital yang terbatas dan kemampuan sumber daya manusia yang tidak merata. | Penelitian ini relevan dengan topik saya karena metode National Institute of Justice (NIJ) yang diterapkan dalam artikel Anda menunjukkan kesesuaian prosedur forensik di berbagai bidang. Ketiga, keduanya berupaya meningkatkan efektivitas penegakan hukum, meskipun dalam konteks yang berbeda. |
| 73 | Rauhulloh Ayatulloh Khomeini Noor Bintang, Rusydi Umar, Anton Yudhana. (2021). Assess of Forensic Tools on Android Based Facebook Lite with the NIST Method | Penelitian ini menggunakan metode NIST (National Institute of Standards and Technology) yang terdiri dari empat tahap Collection,  Examination,  Analysis, Reporting. | Tujuan penelitian ini adalah untuk mengevaluasi kinerja alat forensik dalam memperoleh bukti digital dari aplikasi Facebook Lite yang digunakan di smartphone berbasis Android, khususnya dalam kasus pencemaran nama baik. | Penelitian menunjukkan bahwa alat forensik MOBILedit Forensic Express Pro memiliki tingkat akurasi yang lebih tinggi (85.71%) dibandingkan dengan Magnet Axiom Forensic (57.14%) dalam mendapatkan bukti digital dari aplikasi Facebook Lite. | Penelitian ini relevan dengan topik saya karena kedua penelitian menggunakan metode forensik yang terstandarisasi, yaitu NIST dan NIJ, untuk menganalisis data digital. Fokus pada platform media sosial menunjukkan relevansi dalam konteks penggunaan media sosial yang terus meningkat. |
| 74 | Novi Saputri, Rini Indrayani. (2022). Analisis Data Forensik Investigasi Kasus Peredaran Narkoba pada Smartphone Berbasis Android | Penelitian ini menggunakan metode National Institute of Justice (NIJ) dan membandingkan dua alat forensik, yaitu Magnet Axiom dan MobilEdit Forensic, dengan dua pendekatan: Tanpa Akses Root & Dengan Akses Root | Tujuan dari penelitian ini adalah untuk:  Menemukan bukti forensik terkait peredaran narkoba yang dilakukan melalui aplikasi WhatsApp di smartphone.  Membandingkan efektivitas dua alat forensik dalam mengekstraksi data dengan dan tanpa akses root. | Hasil penelitian menunjukkan bahwa Dengan akses root, Magnet Axiom memiliki tingkat ekstraksi data yang lebih tinggi (77,77%) dibandingkan MobilEdit Forensic (66,66%). Tanpa akses root, kedua alat memiliki efektivitas yang sama (33,33%).  Magnet Axiom direkomendasikan sebagai alat forensik yang lebih baik berdasarkan kinerjanya dalam penelitian ini. | Penelitian ini relevan dengan topik saya karena kedua studi ini fokus pada forensik digital meskipun dalam konteks yang berbeda, dengan tujuan menemukan bukti digital untuk penegakan hukum. Pemilihan alat forensik juga menjadi perhatian utama, di mana penelitian Anda menggunakan Tools Autopsy sementara penelitian sebelumnya menggunakan Magnet Axiom dan MobilEdit Forensic. |
| 75 | Hafiidh Akbar Sya’bani, Chaerul Umam, L. Budi Handoko. (2024). Forensic Analysis of Podman Container Towards Metasploit Backdoor Using Checkpointctl | Penelitian ini menggunakan metode forensik digital berdasarkan kerangka kerja NIST, yang mencakup empat tahap Pengumpulan,  Pemeriksaan,  Analisis, Pelaporan. | Tujuan penelitian ini adalah untuk melakukan analisis forensik pada kontainer Podman yang terinfeksi backdoor Metasploit dengan menggunakan alat checkpointctl, untuk mendapatkan bukti digital yang relevan terkait insiden siber. | Penelitian ini menyimpulkan bahwa proses analisis forensik pada kontainer Podman dapat dilakukan efektif dengan menggunakan file checkpoint. Hasil analisis menunjukkan bahwa kontainer tersebut menjalankan file PHP berbahaya yang berfungsi sebagai backdoor. | Penelitian ini relevan dengan topik saya karena keduanya menggunakan pendekatan forensik untuk mengidentifikasi dan menganalisis bukti digital. Penelitian pertama menggunakan metode NIST, sedangkan artikel Anda menggunakan metode NIJ. Baik analisis forensik kontainer maupun penyebaran informasi palsu melibatkan pengumpulan dan pemeriksaan bukti digital untuk memahami insiden yang terjadi. |
| 76 | Wisnu Pranoto, Imam Riadi, Yudi Prayudi. (2020). Perbandingan Tools Forensics pada Fitur TRIM SSD NVMe Menggunakan Metode Live Forensics | Penelitian ini menggunakan metode live forensics untuk mengakuisisi dan memulihkan data dari SSD NVMe dengan fitur TRIM. Metode ini diterapkan pada sistem operasi Windows 10 dengan file system NTFS, dan menggunakan tools seperti FTK Imager Portable, Autopsy, Belkasoft, dan Testdisk untuk analisis dan recovery data. | Tujuan penelitian adalah untuk membandingkan efektivitas fungsi TRIM dalam keadaan disable dan enable serta untuk mengevaluasi kemampuan berbagai tools forensics dalam mengembalikan bukti digital yang dihapus pada SSD NVMe. | Penelitian menunjukkan bahwa pada fungsi TRIM disable, tools seperti Autopsy dan Testdisk dapat memulihkan 100% data tanpa kerusakan, sedangkan pada fungsi TRIM enable, tidak ada data yang dapat dipulihkan dengan baik. | Penelitian ini relevan dengan topik saya karena bertujuan untuk mengumpulkan dan menganalisis bukti digital. Keduanya memanfaatkan tools forensik untuk mengidentifikasi dan menganalisis data. Dalam penelitian pertama, tools seperti Autopsy digunakan, yang juga relevan dengan penelitian Anda mengenai penyebaran informasi palsu di TikTok. |
| 77 | Riska Wulandari, Yulita Salim, Erick Irawadi Alwi. (2024). Analisis Kesamaan Nada Menggunakan Teknik Spektral Pada Metode Audio Forensik | Penelitian ini menggunakan metode audio forensik dengan teknik analisis spektral untuk mendeteksi kesamaan nada antara dua lagu. Metode ini mencakup pembuatan spektogram untuk membandingkan frekuensi audio dari lagu yang diuji. | Tujuan penelitian adalah untuk mendeteksi kesamaan nada melodi antara dua lagu yang diduga memiliki plagiarisme, serta memberikan kontribusi dalam perlindungan hak cipta dan integritas karya musik. | Hasil analisis menunjukkan adanya kesamaan nada yang signifikan antara kedua lagu dalam beberapa segmen frekuensi. Meskipun demikian, analisis spektral hanya satu dari banyak metode yang perlu dipertimbangkan dalam menilai plagiarisme musik secara komprehensif. | Penelitian ini relevan dengan topik saya karena Metode analisis yang digunakan dalam kedua studi memanfaatkan teknik yang sistematis dan berbasis data. Penelitian pertama menggunakan analisis spektral, sedangkan artikel Anda menggunakan metode National Institute of Justice (NIJ) dan tools Autopsy untuk menganalisis data digital. |
| 78 | Rakha Pangestu Raharja, Erick Irawadi Alwi, Andi Widya Mufila Gaffar. (2024). Analisis Digital Forensic pada Aplikasi WhatsApp Menggunakan Metode National Institute of Justice (NIJ) pada Smartphone Android | Metode yang digunakan adalah National Institute of Justice (NIJ), yang terdiri dari lima tahapan:  Identification,  Collection,  Examination,  Analysis Reporting. | Tujuan penelitian ini adalah untuk mengidentifikasi, mengumpulkan, menganalisis, dan melaporkan bukti digital terkait aktivitas prostitusi online melalui aplikasi WhatsApp menggunakan alat Magnet Axiom. | Metode NIJ terbukti efektif dalam memperoleh dan menganalisis bukti digital, yang dapat digunakan dalam proses hukum. Penelitian ini menunjukkan bahwa prostitusi online memiliki konsekuensi hukum dan analisis digital forensic dapat membantu aparat penegak hukum dalam mengungkap kasus serupa secara lebih efektif dan akurat. | Penelitian ini relevan dengan topik saya karena kedua penelitian bertujuan untuk mengidentifikasi dan menganalisis bukti digital. Penelitian pertama berfokus pada aktivitas ilegal, sedangkan artikel Anda berfokus pada penyebaran informasi palsu, yang juga merupakan isu penting di era digital. |
| 79 | Harno Supardin, Ramdan Satra, Muhammad Arfah Asis. (2022). Analisis Perbandingan Tools Forensik Digital pada Instagram Messenger menggunakan Metode National Institute of Standards and Technology (NIST) | Penelitian ini menggunakan metode National Institute of Standards and Technology (NIST) yang mencakup tahapan Collection, Examination, Analysis, dan Reporting untuk melakukan analisis forensik digital pada Instagram Messenger. | Tujuan penelitian adalah untuk membandingkan kinerja tools forensik digital (MOBILedit Forensic dan Magnet Axiom) dalam mengembalikan bukti digital yang dihapus pada Instagram Messenger, serta untuk mengevaluasi akurasi masing-masing tool. | Hasil penelitian menunjukkan bahwa Magnet Axiom Forensic memiliki akurasi lebih tinggi dalam mengembalikan data yang dihapus (76,92%) dibandingkan dengan MOBILedit Forensic (69,23%). Kedua tools tersebut efektif dalam mengembalikan pesan gambar dan video, tetapi kurang baik dalam mengembalikan pesan teks. | Penelitian ini relevan dengan topik saya karena bertujuan untuk mengidentifikasi dan menganalisis bukti digital yang relevan dengan kejahatan. Penelitian pertama berfokus pada pornografi, sementara penelitian Anda berfokus pada penyebaran informasi palsu, yang juga merupakan isu penting dalam konteks keamanan digital. |
| 80 | Abdul Isnan Fahrial Sinusi, Yulita Salim, Erick Irawadi Alwi. (2023). Analisis Bukti Digital Untuk Penanganan Kekerasan Berbasis Gender Online Pada Media Sosial Whatsapp Menggunakan Metode National Institute Of Justice (NIJ) | Penelitian ini menggunakan metode Forensik Digital dengan pendekatan National Institute of Justice (NIJ). Proses penelitian dibagi menjadi beberapa tahapan:  Persiapan,  Koleksi,  Pemeriksaan,  Analisis,  Pelaporan. | Tujuan penelitian ini adalah untuk melakukan akuisisi dan analisis bukti digital dari aplikasi WhatsApp pada smartphone berbasis Android, serta menyusun protokol yang dapat membantu pihak berwajib dalam menangani kasus Kekerasan Berbasis Gender Online (KBGO). | Penelitian ini menyimpulkan bahwa metode NIJ yang diterapkan dapat efektif dalam memperoleh dan menganalisis bukti digital dari WhatsApp. Hasil analisis menunjukkan bahwa pelaku menggunakan WhatsApp sebagai media untuk melakukan pelecehan seksual, dengan bukti digital yang berhasil diambil berupa teks percakapan, waktu percakapan, dan gambar yang terhapus. | Penelitian ini relevan dengan topik saya karena penelitian menggunakan metode National Institute of Justice (NIJ), yang menunjukkan pendekatan sistematis dalam analisis forensik digital. Ini menciptakan kesamaan dalam cara pengumpulan, pemeriksaan, dan analisis bukti digital. Penelitian mengenai Kekerasan Berbasis Gender Online (KBGO) di WhatsApp dan penyebaran informasi palsu di TikTok sama-sama melibatkan platform media sosial. |
| 81 | Irhash Ainur Rafiq, Imam Riadi, Herman. (2022). Perbandingan Forensic Tools pada Instagram Menggunakan Metode NIST | Penelitian ini menggunakan metode National Institute of Standards and Technology (NIST), yang terdiri dari empat tahap: collection, examination, analysis, dan reporting. | Tujuan penelitian ini adalah untuk mendapatkan bukti digital dari aplikasi Instagram dengan menggunakan dua alat forensik, yaitu Belkasoft Evidence dan Magnet Axiom. | Hasil penelitian menunjukkan bahwa Magnet Axiom memiliki akurasi yang lebih tinggi (83.3%) dibandingkan dengan Belkasoft Evidence (50%) dalam mengembalikan data yang dihapus pada aplikasi Instagram. | Penelitian ini relevan dengan topik saya karena keduanya menggunakan metode forensik digital, meskipun dengan pendekatan yang berbeda (NIST vs. NIJ). Fokus pada platform media sosial: penelitian pertama meneliti Instagram, sedangkan penelitian Anda berfokus pada TikTok, menyoroti isu penyebaran informasi palsu di kedua platform. |
| 82 | Muhammad Noor Fadillah, Rusydi Umar, Anton Yudhana. (2022). Analisis Forensik Aplikasi Dompet Digital Pada Smartphone Android Menggunakan Metode DFRWS | Penelitian ini menggunakan metode Digital Forensic Research Workshop (DFRWS), yang terdiri dari beberapa tahapan:  Identification, Preservation,  Collection, Examination,  Analysis, Presentation. | Tujuan penelitian ini adalah untuk memberikan gambaran proses forensik pada aplikasi dompet digital dengan fokus mencari informasi terkait aktivitas transaksi yang dilakukan, sehingga bukti digital yang diperoleh dapat digunakan sebagai alat bukti hukum berdasarkan UU ITE. | Penelitian ini berhasil melakukan proses forensik pada aplikasi dompet digital dengan mengikuti prosedur DFRWS. Hasil penelitian menunjukkan bahwa semua aktivitas transaksi yang pernah dilakukan pada aplikasi dapat ditemukan, dengan tingkat keberhasilan 100% dalam pengambilan data pengguna dan aktivitas transaksi. | Penelitian ini relevan dengan topik saya karena berfokus pada forensik digital, yaitu proses pengumpulan dan analisis bukti dari perangkat elektronik. Meskipun aplikasi yang dianalisis berbeda, keduanya menggunakan pendekatan metodologis yang terstruktur dalam analisis forensik. Penelitian pertama meneliti transaksi keuangan, sedangkan artikel Anda mengkaji penyebaran informasi palsu. |
| 83 | Adhitya Nugraha, Erick Irawadi Alwi, Andi Widya Mufila Gaffar. (2024). Penerapan Model Investigasi Forensik Komputer Umum dalam Analisis Forensik Video CCTV | Metode penelitian yang digunakan adalah kualitatif dengan penerapan model Generic Computer Forensic Investigation Model (GCFIM). Penelitian ini melibatkan tahapan analisis data yang terdiri dari: Pre-Process, Acquisition and Preservation, Analysis, Presentation, Post-Process. | Tujuan penelitian ini adalah untuk menganalisis bukti digital dari rekaman video CCTV dalam kasus pembegalan yang terjadi di Jl. Pahlawan Kelurahan Batangmata, serta menjadikannya sebagai barang bukti dalam proses persidangan. | Proses identifikasi bukti dalam rekaman CCTV berhasil dilakukan menggunakan alat AmpedFive. Bukti yang diperoleh, seperti plat kendaraan dan objek wajah pelaku, sangat membantu penyidik dalam mencari pelaku kejahatan. | Penelitian ini relevan dengan topik saya karena berfokus pada analisis forensik digital untuk mengidentifikasi bukti dari media digital, serta menggunakan metode terstruktur (GCFIM dan NIJ) untuk memastikan investigasi dilakukan secara sistematis. Tujuan utamanya adalah untuk mengidentifikasi dan menganalisis bukti yang dapat digunakan dalam proses hukum. |
| 84 | Aidil Wijaya Kusuma, Erick Irawadi Alwi, Ramdaniah Ramdaniah. (2024). Analisis Bukti Digital Pada Media Penyimpanan Flash Disk Menggunakan Metode National Institute Of Standards And Technology (NIST) | Penelitian ini menggunakan metode National Institute of Standards and Technology (NIST) untuk analisis bukti digital. Alat yang digunakan meliputi FTK Imager untuk akuisisi data, Autopsy untuk analisis dan pemulihan data, serta HashGenerator untuk memverifikasi hasil hash dari setiap file. | Tujuan dari penelitian ini adalah untuk memperoleh, mengambil, melestarikan, dan menyajikan data terkait aktivitas cybercrime yang terdapat pada media penyimpanan flash disk yang telah dihapus, serta mendukung penyelidikan terhadap pelaku kejahatan dengan menerapkan prinsip-prinsip forensik digital. | Penelitian menunjukkan bahwa bukti digital yang telah dihapus pada media penyimpanan flash disk dapat ditemukan dan dipulihkan menggunakan alat forensik FTK Imager dan Autopsy. Semua bukti digital yang dipulihkan cocok dengan data asli meskipun terdapat perubahan nama file pada perlakuan tertentu, dan nilai hash MD5 tidak menunjukkan adanya perubahan. | Penelitian ini relevan dengan topik saya karena penelitian menggunakan pendekatan metodologis yang sistematis dalam analisis forensik digital, meskipun berbeda dalam lembaga standar. Kedua, fokus pada forensik digital menjadi inti dari kedua studi, dengan tujuan mendukung penegakan hukum melalui pengumpulan dan analisis data digital. Ketiga, penggunaan alat forensik yang sama, yaitu Autopsy, menunjukkan konsistensi dalam penerapan teknologi untuk analisis data. |
| 85 | Michelle Mawar J. Sianipar, Setia Juli Irzal Ismail, Gandeva Bayu Satrya. (2021). Analisis Digital Forensik Aplikasi OVO Pada Android | Penelitian ini menggunakan metode analisis digital forensik untuk mengkaji cybercrime yang terjadi pada aplikasi OVO. Proses analisis meliputi pengumpulan, pemeriksaan, analisis, dan pelaporan sesuai dengan standar NIST SP 800-86. | Tujuan penelitian ini adalah untuk:  Mengungkap identitas pelaku kejahatan yang menggunakan aplikasi OVO.  Memulihkan dan menganalisis barang bukti digital yang berkaitan dengan cybercrime. | Digital forensik dapat digunakan untuk memulihkan barang bukti yang hilang dengan mencari artefak database pada aplikasi OVO. Metode NIST efektif untuk menganalisis barang bukti dengan bantuan alat seperti Notepad dan SQL DB Browser.  Algoritma hash digunakan untuk memastikan integritas dan keaslian barang bukti. | Penelitian ini relevan dengan topik saya karena fokus mereka pada cybercrime menunjukkan relevansi dalam konteks keamanan siber, di mana penelitian OVO menyoroti kejahatan dalam aplikasi pembayaran digital, sedangkan artikel Anda meneliti penyebaran informasi palsu. Penggunaan alat forensik seperti Autopsy dalam artikel Anda sejalan dengan penggunaan perangkat lunak analisis dalam penelitian OVO. |
| 86 | Khairunnisak Nur Isnaini, Hamid Ashari, Adam Prayogo Kuncoro. (2020). Analisis Forensik untuk Mendeteksi Keaslian Citra Digital Menggunakan Metode NIST | Penelitian ini menggunakan metode NIST (National Institute of Standards and Technology) yang terdiri dari tahapan: Collection,  Examination,  Analysis, Reporting. | Tujuan penelitian ini adalah untuk membuktikan keaslian bukti digital, terutama video, dan menunjukkan peran digital forensik dalam mendukung proses hukum di Indonesia dengan ilustrasi kasus nyata. | Penelitian menunjukkan bahwa alat yang digunakan dalam identifikasi forensik video efektif. Metode NIST dapat diterapkan sebagai standar untuk membuktikan keaslian file elektronik yang diduga sebagai bukti digital. | Penelitian ini relevan dengan topik saya karena menerapkan pendekatan forensik digital untuk menganalisis keaslian informasi. Sementara penelitian pertama fokus pada keaslian citra digital, artikel Anda menyoroti penyebaran informasi palsu di platform TikTok. penelitian menggunakan alat forensik yang berbeda—Exiftools dan Forevid dalam penelitian sebelumnya, serta Autopsy dalam artikel Anda—untuk mencapai tujuan yang sama. |
| 87 | Salma Azizah, Sri Ayu Ramadhona, Kenny Willy Gustitio. (2020). Analisis Bukti Digital pada Telegram Messenger Menggunakan Framework NIST | Metode penelitian yang digunakan adalah metode NIST (National Institute of Standard Technology). Penelitian ini melalui beberapa tahapan, yaitu:  Collection,  Examination,  Analysis,  Reporting. | Tujuan penelitian ini adalah untuk menemukan bukti digital pada kasus penipuan online shop, dengan menggunakan teknik live forensics untuk mengakuisisi data dari Random Access Memory (RAM) pada komputer yang menjalankan aplikasi Telegram. | Teknik live forensics dapat digunakan untuk mendapatkan bukti digital dari Telegram berbasis desktop dengan sistem operasi Windows 10 menggunakan FTK Imager. Meskipun data yang diperoleh tidak selalu sama persis dengan data asli di smartphone korban, metode ini efektif dalam mengungkap tindak kejahatan penipuan online shop. | Penelitian ini relevan dengan topik saya karena kedua penelitian menggunakan pendekatan forensik digital untuk mengidentifikasi dan menganalisis bukti dari platform media sosial yang berbeda. Kedua, meskipun menggunakan metode yang berbeda—NIST dan NIJ—tujuan utama keduanya adalah untuk menjaga integritas dan validitas data yang diperoleh. Masing-masing penelitian berfokus pada kejahatan siber yang berbeda: penipuan online dan penyebaran informasi palsu, mencerminkan tantangan yang dihadapi masyarakat modern. |
| 88 | Syifa Riski Ardiningtias, Sunardi, Herman. (2021). Forensik Digital Kasus Penyebaran Pornografi pada Aplikasi Facebook Messenger Berbasis Android Menggunakan Kerangka Kerja National Institute of Justice | Penelitian ini menggunakan kerangka kerja National Institute of Justice (NIJ) yang terdiri dari beberapa tahapan: Identification, Preservation, Collection, Examination, Analysis, Presentation. | Tujuan dari penelitian ini adalah untuk mendapatkan bukti forensik terkait penyebaran konten pornografi melalui aplikasi Facebook Messenger yang diakses menggunakan smartphone berbasis Android. | Penelitian menunjukkan bahwa menggunakan perangkat lunak Magnet Axiom menghasilkan akurasi 90,91% dalam menemukan bukti digital, jauh lebih baik dibandingkan dengan Belkasoft Evidence Center yang hanya mencapai 46,66%. Hasil ini menunjukkan efektivitas alat forensik dalam investigasi kejahatan digital. | Penelitian ini relevan dengan topik saya karena menggunakan metode National Institute of Justice (NIJ), yang menunjukkan pendekatan sistematis dalam analisis forensik digital. Fokus penelitian sama-sama berada pada platform media sosial, dengan Facebook Messenger dan TikTok sebagai contoh. Meskipun jenis konten yang ditangani berbeda pornografi dan informasi palsu. kedua penelitian menunjukkan bahwa kejahatan siber dapat muncul dalam berbagai bentuk di media sosial. |
| 89 | Imam Riadi, Rusydi Umar, Imam Mahfudl Nasrulloh. (2017). Analisis Forensik Bukti Digital Pada Frozen Solid State Drive Dengan Metode National Institute Of Standards And Technology (NIST) | Metode penelitian yang digunakan adalah metode akuisisi statis (static forensic) untuk pengambilan bukti digital serta tahapan analisis forensik berdasarkan metode dari National Institute of Standards and Technology (NIST) yang meliputi pengumpulan, pemeriksaan, analisis, dan pelaporan. | Tujuan penelitian ini adalah untuk menganalisis bukti digital yang tersimpan pada Frozen Solid State Drive (SSD) dan memberikan panduan bagi investigator forensik dalam menghadapi tantangan yang muncul akibat penggunaan software pembeku drive. | Kesimpulan dari penelitian ini adalah bahwa analisis bukti digital sangat penting dalam kasus kejahatan komputer, dan diperlukan prosedur penanganan yang tepat serta penggunaan metode NIST untuk mendapatkan bukti digital yang valid dan dapat dipertanggungjawabkan. Penelitian ini juga menekankan perlunya pemahaman yang mendalam mengenai teknologi penyimpanan terbaru seperti SSD dan pengaruh software pembeku terhadap analisis forensik. | Penelitian ini relevan dengan topik saya karena kedua penelitian menggunakan metode analisis forensik yang terstruktur, meskipun dengan pendekatan yang berbeda (NIST vs. NIJ). Fokus pada pengumpulan dan analisis bukti digital menjadi inti dari kedua studi, baik itu dari media penyimpanan SSD atau platform media sosial seperti TikTok. Ketiga, tantangan dalam analisis bukti digital yang dihadapi dalam masing-masing konteks menunjukkan perlunya metode dan alat yang tepat. |
| 90 | Galih Fanani, Imam Riadi, Anton Yudhana. (2022). Analisis Forensik Aplikasi Michat Menggunakan Metode Digital Forensics Research Workshop | Penelitian ini menggunakan kerangka kerja Digital Forensics Research Workshop (DFRWS) yang terdiri dari enam tahapan:  Identification (Identifikasi),  Preservation (Pemeliharaan),  Collection (Pengumpulan),  Examination (Pemeriksaan),  Analysis (Analisis),  Presentation (Presentasi). | Tujuan penelitian ini adalah untuk melakukan analisis forensik terhadap aplikasi MiChat guna memperoleh bukti digital yang dapat digunakan dalam kasus perdagangan narkoba (drug trafficking) dan untuk memberikan pemahaman yang lebih baik tentang proses forensik digital. | Penelitian menunjukkan bahwa investigasi forensik pada aplikasi MiChat menggunakan alat-alat seperti Mobiledit Forensic Express, DB Browser For SQLite, dan Oxygen Forensic Detective dapat berhasil memulihkan bukti digital dengan tingkat keberhasilan 100%. Alat Oxygen Forensic Detective memiliki kemampuan tertinggi dalam menemukan bukti. | Penelitian ini relevan dengan topik saya karena berfokus pada identifikasi dan pengumpulan bukti dari aplikasi digital, meskipun menggunakan metode yang berbeda: DFRWS untuk MiChat dan NIJ untuk TikTok. Alat forensik yang digunakan juga berbeda, dengan MiChat menggunakan beberapa tools dan Anda menggunakan Autopsy. Tujuan utama dari kedua penelitian adalah untuk memperoleh bukti yang dapat digunakan dalam proses hukum, baik untuk kasus narkoba maupun informasi palsu. |
| 91 | Meyti Eka Apriyani, Rahmad Alfian Maskuri, M. Hasyim Ratsanjani, Agung Pramudhita, Rawansyah. (2023). Forensic Digital Analysis of Telegram Applications Using the National Institute of Justice and Naïve Bayes Methods | Metode National Institute of Justice (NIJ): Digunakan untuk melakukan analisis forensik dan mengidentifikasi tahapan dalam proses pengambilan bukti digital.  Metode Naïve Bayes: Digunakan untuk mengklasifikasikan percakapan yang ditemukan, khususnya untuk mendeteksi percakapan yang mengandung pelecehan seksual. | Tujuan dari penelitian ini adalah untuk:  Menganalisis bukti digital dari aplikasi Telegram dalam konteks pelecehan seksual.  Menggunakan metode NIJ untuk mengidentifikasi dan mengumpulkan bukti.  Menggunakan metode Naïve Bayes untuk mengklasifikasikan percakapan sebagai positif (mengandung pelecehan) atau negatif (tidak mengandung pelecehan). | Smartphone yang di-root memiliki akses data yang lebih luas dibandingkan yang tidak di-root. Aplikasi MOBILedit Forensic Express tidak efektif dalam menemukan bukti digital, sedangkan FTK Imager sangat efektif. Algoritma Naïve Bayes berhasil mengklasifikasikan percakapan dengan akurasi yang baik, menghasilkan nilai akurasi 85%, presisi 85.7%, dan recall 85.7%. | Penelitian ini relevan dengan topik saya karena Keduanya menggunakan metode National Institute of Justice (NIJ) untuk sistematis dalam mengidentifikasi dan mengumpulkan bukti digital. Fokus utama kedua penelitian adalah pada platform digital yang berbeda—Telegram untuk pelecehan seksual dan TikTok untuk informasi palsu—menyoroti tantangan dalam menangani kejahatan digital. |
| 92 | Nur Dwi Putri dan Dahliyusmanto. (2024). Analisis Keamanan Menggunakan Metode Live Forensic pada Web | Metode penelitian yang digunakan adalah Live Forensic, yang mengikuti kerangka kerja National Institute of Justice. Penelitian ini meliputi lima tahap: Identifikasi, Pengumpulan, Pemeriksaan, Analisis, Pelaporan. | Tujuan penelitian adalah untuk menunjukkan bagaimana metode live forensic pada RAM komputer dapat digunakan untuk mendapatkan data yang tersimpan di RAM, khususnya dalam konteks keamanan e-commerce. | Penelitian menunjukkan bahwa dalam dua simulasi yang dilakukan, email pengguna dapat terdeteksi, tetapi password tidak dapat ditemukan. Hal ini mengindikasikan bahwa website e-commerce yang diuji relatif aman untuk diakses oleh pengguna. | Penelitian ini relevan dengan topik saya karena menggunakan metode NIJ sebagai kerangka kerja untuk analisis forensik. Kedua, fokus utama dari kedua penelitian adalah pada keamanan digital, di mana penelitian pertama menilai risiko data pengguna dan artikel Anda mengkaji dampak informasi palsu pada masyarakat. |
| 93 | M Alfalogika Kholifatulloh, Ari Kusyanti. (2024). Analisis Investigasi Forensik Smartphone Android Terhadap Tindakan Cybercrime Menggunakan Framework Digital Forensic Model Based In Malaysian Investigation Process | Metode penelitian yang digunakan dalam studi ini mencakup pendekatan kualitatif dan kuantitatif. Penelitian ini melibatkan pengumpulan data melalui survei, wawancara, dan analisis dokumen untuk mendapatkan pemahaman yang mendalam tentang topik yang diteliti. | Tujuan penelitian ini adalah untuk mengeksplorasi dan menganalisis fenomena yang berkaitan dengan tema yang diangkat. Penelitian ini bertujuan untuk memberikan kontribusi pada pengembangan ilmu pengetahuan dan praktik di bidang terkait, serta untuk mengidentifikasi masalah dan solusi yang relevan. | Kesimpulan dari penelitian ini menegaskan pentingnya hasil yang diperoleh dalam konteks aplikasi praktis dan teori. Penelitian ini menunjukkan bahwa terdapat hubungan signifikan antara variabel yang diteliti dan memberikan rekomendasi untuk penelitian lebih lanjut serta implementasi di lapangan. | Penelitian ini relevan dengan topik saya karena metode penelitian yang sistematis, seperti yang diterapkan dalam penelitian di atas, sejalan dengan penggunaan metode NIJ dalam analisis penyebaran informasi palsu. Tujuan penelitian Anda untuk mengeksplorasi dampak informasi palsu di TikTok mencerminkan tujuan penelitian yang lebih umum dalam mengidentifikasi masalah sosial. |
| 94 | Andria dan Saifulloh. (2022). Forensik Metadata Foto Sebagai Alat Bukti Digital | Penelitian ini menggunakan metode forensik digital berdasarkan pedoman National Institute of Justice (NIJ). Lima tahapan yang diadopsi dari metode NIJ adalah Policy and Procedure Development, Evidence Assessment, Evidence Acquisition, Evidence Examination, Documenting and Reporting. | Penelitian ini bertujuan untuk melakukan analisis forensik metadata foto menggunakan alat Exiftool yang dijalankan di aplikasi Termux pada smartphone Android, guna memperoleh informasi dari metadata yang dapat digunakan sebagai alat bukti digital dalam suatu persidangan. | Penelitian menunjukkan bahwa metadata pada file foto mengandung berbagai informasi penting seperti Nama file, ukuran, dimensi (panjang & lebar), Tanggal dan waktu pengambilan, Lokasi pengambilan foto (pada foto asli), Aplikasi editing yang digunakan (pada foto hasil edit) | Penelitian ini relevan dengan topik saya karena terletak pada penggunaan metode NIJ dalam konteks forensik digital untuk menangani penyebaran informasi palsu. Anda hanya berbeda dalam konteks media (TikTok vs. Foto), tapi prinsip dasar, tujuan, dan proses forensik digital tetap serupa. |
| 95 | Reben Yulandra Agustian, Tata Sutabri. (2024). Analisis Keamanan Data pada Aplikasi Chatting Menggunakan Metode Network Forensics | Metode yang digunakan dalam penelitian ini adalah network forensics, yang mencakup langkah-langkah berikut: Identifikasi, Pengumpulan Data, Pemeriksaan, Analisis, Pelaporan. | Tujuan dari penelitian ini adalah untuk menganalisis keamanan data pada aplikasi chatting populer dengan menggunakan metode network forensics, serta mengidentifikasi langkah-langkah yang diperlukan untuk meningkatkan keamanan data. | Kesimpulan dari penelitian ini menyatakan bahwa analisis keamanan data pada aplikasi chatting menunjukkan bahwa meskipun enkripsi digunakan untuk melindungi komunikasi, masih terdapat kerentanan yang harus diwaspadai, seperti pencurian metadata dan serangan man-in-the-middle (MitM). | Penelitian ini relevan dengan topik saya karena menekankan pentingnya keamanan dan integritas informasi, dengan fokus pada identifikasi ancaman—penelitian pertama mengidentifikasi kerentanan dalam aplikasi chatting, sedangkan artikel Anda menganalisis penyebaran informasi palsu di TikTok. |
| 96 | Zikri Sulthoni Daulay, Rini Indrayani. (2022). Analisis Keamanan Browser Dalam Bersosial Media Menggunakan Metode Institute Of Justice (NIJ) | Penelitian ini menggunakan metodologi National Institute of Justice (NIJ) dengan teknik live forensic. Proses pengujian dilakukan dengan dua browser (Google Chrome dan Mozilla Firefox) dalam mode publik dan mode incognito, serta menggunakan aplikasi FTK Imager untuk menangkap data. | Tujuan dari penelitian ini adalah untuk mengenal tingkat keamanan browser dalam menggunakan media sosial dan untuk mengidentifikasi data yang masih dapat diakses oleh alat forensic pada saat menggunakan browser. | Kesimpulan dari penelitian menunjukkan bahwa mengakses media sosial (Facebook, Instagram, Twitter) menggunakan Google Chrome dan Mozilla Firefox, baik dalam mode publik maupun mode incognito, tidak aman. Data seperti user\_id, email, dan beberapa password masih terdeteksi. | Penelitian ini relevan dengan topik saya karena menggunakan metode National Institute of Justice (NIJ) untuk analisis data digital, menekankan pendekatan sistematis dalam pengumpulan dan analisis. Meskipun fokus pada platform yang berbeda, yaitu media sosial, keduanya menyoroti isu keamanan data pengguna dan dampak informasi yang tidak akurat. Penggunaan alat forensik yang berbeda, FTK Imager dan Autopsy. |
| 97 | Wahyu Aji Purnama, Yustian Servanda, Djumhadi, Agus Wijayanto. (2024). Analisis Kasus Kehilangan Data Akibat Format dan Pemulihan Data Menggunakan Aplikasi Wondershare Recoverit | Penelitian ini menggunakan pendekatan studi kasus dengan simulasi skenario di mana sebuah flash disk terformat secara tidak sengaja. Peneliti melakukan evaluasi terhadap efektivitas aplikasi Wondershare Recoverit dalam memulihkan data yang hilang akibat pemformatan. | Tujuan utama dari penelitian ini adalah untuk menganalisis efektivitas Wondershare Recoverit dalam memulihkan data yang hilang akibat format yang tidak disengaja pada perangkat penyimpanan, khususnya flash disk. | Penelitian menunjukkan bahwa Wondershare Recoverit efektif dalam memulihkan data yang hilang akibat pemformatan. Aplikasi ini memiliki antarmuka yang intuitif dan mampu memulihkan berbagai jenis file, serta mendukung pemulihan dari berbagai perangkat penyimpanan. Pencegahan kehilangan data juga lebih diutamakan dibandingkan pemulihan. | Penelitian ini relevan dengan topik saya karena menekankan pentingnya analisis data yang hilang atau terhapus, dengan fokus pada keakuratan dalam memproses informasi. Metodologi yang digunakan, termasuk perangkat lunak untuk analisis dan pemulihan data, menunjukkan kesamaan dalam pendekatan teknis. Selain itu, kedua penelitian menyoroti pentingnya pencegahan. |
| 98 | I Putu Agus Eka Pratama. (2021). Computer Forensic Using Photorec for Secure Data Recovery Between Storage Media: a Proof of Concept | Penelitian ini menggunakan metode eksperimental. Langkah-langkah penelitian meliputi:  Identifikasi kasus masalah data.  Identifikasi ekstensi data.  Proses pemulihan data berdasarkan kondisi. | Tujuan dari penelitian ini adalah untuk:  Menguji keandalan alat Photorec dalam melakukan pemulihan data secara aman dari media penyimpanan USB Flashdisk ke hard disk komputer. | Penelitian menyimpulkan bahwa Photorec adalah alat forensik digital yang dapat diandalkan untuk pemulihan data, mampu mengembalikan 100% file yang hilang, Proses pemulihan data yang aman dilakukan dengan memberikan akses root pada semua file yang dipulihkan, sehingga hanya pengguna dengan akses root yang dapat mengakses file tersebut. | Penelitian ini relevan dengan topik saya karena menekankan pentingnya pengumpulan dan analisis bukti digital. Penelitian Anda menggunakan metode NIJ, sementara penelitian sebelumnya memanfaatkan Photorec untuk pemulihan data, menunjukkan relevansi penggunaan alat dan metode yang diakui. Selain itu, kedua penelitian menyoroti isu keamanan data. |
| 99 | Muhammad Fahmi Abdillah, Yudi Prayudi. (2022). Data Recovery Comparative Analysis using Open-based Forensic Tools Source on Linux | Penelitian ini menggunakan pendekatan perbandingan alat forensik, khususnya Foremost Recover dan Testdisk Recover, dengan fokus pada penggunaan Command Line Interface (CLI) di sistem operasi Linux untuk memulihkan data yang hilang atau rusak. | Tujuan penelitian ini adalah untuk menentukan alat forensik yang efektif untuk pemulihan data, serta untuk memberikan solusi terhadap masalah kehilangan data dengan menggunakan alat pemulihan berbasis open source. | Dari hasil penelitian, ditemukan bahwa alat pemulihan Foremost dan Testdisk dapat melakukan pemulihan data secara penuh. Meskipun beberapa alat seperti TSK recover dan FTK imager tidak selalu berhasil memulihkan data sepenuhnya, penelitian ini menunjukkan bahwa ada opsi alat yang dapat membantu dalam proses investigasi forensik digital. | Penelitian ini relevan dengan topik saya karena penelitian pertama menggunakan pendekatan perbandingan alat dan artikel Anda mengikuti metode National Institute Of Justice (NIJ). Selain itu, kedua penelitian bertujuan untuk memberikan solusi terhadap masalah yang dihadapi dalam konteks digital, dengan fokus pada pemulihan data dan identifikasi informasi palsu. Keduanya relevan dalam menghadapi isu-isu yang muncul akibat perkembangan teknologi digital. |
| 100 | Ageng Restu Triyanto dan Fahmi Fachri. (2024). Analisis Forensik Bukti Digital Pada Kejahatan Pembunuhan Berencana Menggunakan Metode National Institute of Justice | Penelitian ini menggunakan metode National Institute of Justice (NIJ), yang mencakup lima langkah: identifikasi, pengumpulan, pemeriksaan, analisis, dan pelaporan. Metode ini diterapkan untuk memulihkan data yang dihapus secara permanen dari media penyimpanan seperti SSD dan flashdisk. | Tujuan dari penelitian ini adalah untuk mengembalikan data yang telah dihapus dari media penyimpanan dan menganalisis keaslian serta validitas barang bukti menggunakan metode NIJ. | Penelitian menunjukkan bahwa penghapusan data secara permanen memungkinkan pemulihan data dengan tingkat keberhasilan 100% menggunakan tools FTK Imager dan Autopsy. Sebaliknya, penghapusan dengan cara format menghasilkan 0% pemulihan. Metode NIJ terbukti efisien dalam menganalisis dan menentukan keaslian barang bukti digital. | Penelitian ini relevan dengan topik saya karena menggunakan metode National Institute of Justice (NIJ) untuk analisis forensik digital, menunjukkan pendekatan yang terstruktur dalam mengidentifikasi dan menganalisis bukti. Kedua penelitian menggunakan tools Autopsy, yang menunjukkan efektivitas alat yang sama dalam memulihkan dan menganalisis data. Kedua penelitian bertujuan untuk mendapatkan bukti yang sah dan menganalisis keaslian data. |
| 101 | Muhammad Ali Diko Putra, Arif Wirawan Muhammad, Bita Parga Zen, Rianti Yunita Kisworini, dan Tuti Rohayati (2024) dalam jurnal berjudul "Analisis Forensik Pada Instagram dan Tik Tok Dalam Mendapatkan Bukti Digital Dengan Menggunakan Metode NIST 800-86" menggunakan metode National Institute of Standards and Technology (NIST) 800-86. | Metode ini terdiri dari empat tahapan, yaitu Collection, Examination, Analysis, dan Reporting. Penelitian ini memanfaatkan alat forensik seperti MOBILedit Forensic Express, Autopsy, dan FTK Imager untuk mengumpulkan dan menganalisis bukti digital dari aplikasi Instagram dan TikTok. | Tujuan dari penelitian ini adalah untuk menentukan proses menemukan bukti digital pada aplikasi Instagram dan TikTok yang diakses melalui smartphone, serta untuk mengidentifikasi dan membandingkan kinerja berbagai alat forensik dalam memperoleh bukti digital. | Hasil penelitian menunjukkan bahwa FTK Imager lebih unggul dalam akuisisi bukti digital dibandingkan dengan MOBILedit Forensic Express dan Autopsy, dengan FTK Imager berhasil mendapatkan 57% dari total data awal di Instagram dan 71% di TikTok | Penelitian ini relevan dengan topik saya karena kedua studi berfokus pada aplikasi TikTok sebagai platform yang dapat menjadi sarana peredaran informasi, termasuk informasi palsu atau hoaks. Meskipun menggunakan metode yang berbeda, keduanya bertujuan untuk mengidentifikasi dan memperoleh bukti digital yang relevan dari aktivitas pengguna di TikTok. |
| 102 | Nasirudin, Sunardi, dan Imam Riadi (2020) dalam jurnal "Analisis Forensik Smartphone Android Menggunakan Metode NIST dan Tool MOBILedit Forensic Express" | Penelitian ini menggunakan alat forensik MOBILedit Forensic Express untuk menganalisis bukti digital dari smartphone Android, khususnya Samsung Galaxy A8. | Tujuan dari penelitian ini adalah untuk menganalisis bukti digital yang dapat diperoleh dari smartphone Android | Hasil penelitian menunjukkan bahwa data backup, ekstraksi, dan analisis yang relevan untuk penyelidikan berhasil ditemukan. | Penelitian ini relevan dengan topik saya karena.Penelitian ini memberikan dasar untuk memahami proses forensik digital pada smartphone yang juga relevan dengan aplikasi media sosial. |
| 103 | Anton Yudhana, Imam Riadi, dan Ikhwan Anshori (2018) dalam jurnal "Identification of Digital Evidence Facebook Messenger on Mobile Phone with National Institute of Standards Technology (NIST) Method" menggunakan | Penelitian ini menggunakan metode NIST dengan alat forensik Magnet AXIOM dan Oxygen Forensics Suite. | Tujuan dari penelitian ini adalah untuk mengumpulkan bukti digital dari Facebook Messenger untuk keperluan penyelidikan. | Hasil penelitian menunjukkan bahwa bukti yang ditemukan berupa akun, teks percakapan, dan gambar. | Penelitian ini relevan dengan topik saya karena penelitian ini relevan dalam konteks penggunaan aplikasi media sosial untuk kejahatan digital. |
| 104 | Rizdqi Akbar Ramadhan, Panji Rachmat Setiawan, dan Dedy Hariyadi (2022) dalam jurnal "Digital Forensic Investigation for Non-Volatile Memory Architecture by Hybrid Evaluation Based on ISO/IEC 27037:2012 and NIST SP800-86 Framework" | Penelitian ini menggunakan menggabungkan metode NIST SP 800-86 dan ISO/IEC 27037:2012 untuk investigasi forensik. | Tujuan dari penelitian ini adalah untuk mendesain kerangka kerja untuk investigasi bukti digital non-volatil. | Hasil penelitian menunjukkan bahwa kerangka kerja yang dihasilkan lebih komprehensif untuk penanganan bukti digital. | Penelitian ini relevan dengan topik saya karena Penelitian ini memberikan panduan untuk penanganan bukti digital yang relevan dengan penelitian forensik. |
| 105 | Muhammad Adam, Erick Irawadi Alwi, Ihwana As’ad, 2022, "Analisis Forensik Terhadap Serangan DDoS Ping of Death pada Server". | Tujuan dari penelitian ini adalah untuk menganalisis serangan DDoS dengan jenis Ping of Death terhadap web server, serta untuk mengumpulkan dan menganalisis bukti digital yang dihasilkan dari serangan tersebut menggunakan metode forensik yang sesuai. | Metode penelitian yang digunakan dalam studi ini meliputi simulasi serangan DDoS Ping of Death pada web server dan analisis forensik menggunakan metode National Institute of Standards and Technology (NIST). Proses ini mencakup tahapan pengumpulan data, pemeriksaan, analisis, dan pelaporan hasil yang diperoleh dari software Snorby. | Hasil penelitian menunjukkan bahwa serangan DDoS Ping of Death berhasil dilakukan dengan alamat IP penyerang 192.168.177.2 terhadap web server dengan alamat IP 103.229.73.105, yang mengakibatkan penurunan kinerja server. Kesimpulan dari penelitian ini adalah bahwa analisis forensik dapat memberikan bukti yang kuat terkait serangan siber dan membantu dalam proses investigasi. Saran yang diberikan adalah perlunya peningkatan sistem keamanan dan penggunaan alat forensik yang lebih canggih untuk mendeteksi dan mencegah serangan di masa mendatang. | Penelitian Muhammad Adam dkk. (2022) tentang analisis forensik terhadap serangan DDoS dengan jenis Ping of Death pada server relevan dengan analisis forensik digital dalam konteks penyusupan dalam Tiktok. Meskipun fokus penelitian ini adalah pada serangan DDoS terhadap web server, metodologi yang digunakan dapat diterapkan untuk menganalisis potensi penyusupan atau serangan yang dapat mempengaruhi sistem komunikasi seperti Tiktok. |
| 106 | Leonardo Bagas Pradana, Agri Chairunisa Isradjuningtias, Anyelir Puspa Kemala, 2023, "Pemanfaatan Digital Forensik dalam Usaha Preventif Penumpasan Penyebaran Berita Bohong (Hoax)". | Tujuan dari penelitian ini adalah untuk menganalisis pemanfaatan digital forensik dalam upaya pencegahan penyebaran berita bohong (hoax) dan untuk mengevaluasi efektivitas metode digital forensik dalam mengatasi masalah penyebaran informasi yang tidak benar di masyarakat | Metode penelitian yang digunakan adalah penelitian asosiatif dengan teknik penelusuran bahan hukum melalui studi kepustakaan dan analisis kualitatif. Penelitian ini mengkaji berbagai spesialisasi dalam digital forensik, termasuk Computer Forensic, Mobile Forensic, dan Cyber Forensic, untuk memahami bagaimana masing-masing dapat berkontribusi dalam penanganan berita bohong. | Hasil penelitian menunjukkan bahwa pemanfaatan digital forensik sangat berpengaruh dalam usaha preventif penumpasan penyebaran berita bohong, dengan ketiga spesialisasi forensik tersebut memberikan bukti yang kuat dalam investigasi. Kesimpulan dari penelitian ini adalah bahwa digital forensik merupakan alat yang fundamental dalam mengatasi penyebaran hoax. | Penelitian Leonardo Bagas Pradana dkk. (2023) tentang pemanfaatan digital forensik dalam usaha preventif penumpasan penyebaran berita bohong (hoax) relevan dengan analisis forensik digital dalam konteks penyusupan dalam Tiktok. Meskipun fokus penelitian ini adalah pada penyebaran informasi yang tidak benar, metodologi dan pendekatan yang digunakan dapat diterapkan untuk mengidentifikasi dan menganalisis potensi penyusupan atau perilaku tidak etis yang mungkin terjadi selama . |
| 107 | M. Syaiful Huda Mubarok, Rahmat Novrianda Dasmen, Ardiansyah, Viren Pranata, M. Ary Januarta, 2024, "Analisis Digital Forensik Data: Digital Analysis of Forensic Data Recovery on Flash Drive Using National Institute Of Justice (NIJ) Method".. | Tujuan dari penelitian ini adalah untuk menganalisis efektivitas teknik forensik komputer dalam proses pemulihan data dari media penyimpanan digital, khususnya flash drive, dengan menggunakan metode National Institute of Justice (NIJ). | Metode penelitian yang digunakan adalah pendekatan forensik digital dengan menerapkan metode NIJ yang terdiri dari lima fase: persiapan, pengumpulan, pemeriksaan, analisis, dan pelaporan. Penelitian ini juga menggunakan alat TestDisk untuk memulihkan data yang hilang dari flash drive. | Hasil penelitian menunjukkan bahwa alat TestDisk sangat efektif dalam memulihkan data yang hilang dari flash drive, dengan tingkat keberhasilan yang tinggi dalam mengembalikan berbagai jenis file. Kesimpulan dari penelitian ini adalah bahwa penggunaan metode NIJ dan alat TestDisk dapat meningkatkan efektivitas pemulihan data dalam konteks forensik digital. Saran yang diberikan adalah untuk terus mengembangkan dan memperbarui teknik dan alat forensik guna menghadapi tantangan baru dalam pemulihan data di era digital. | Penelitian M. Syaiful Huda Mubarok dkk. (2024) tentang analisis digital forensik data pada flash drive menggunakan metode National Institute of Justice (NIJ) relevan dengan analisis forensik digital dalam konteks penyusupan dalam Tiktok. Meskipun fokus penelitian ini adalah pada pemulihan data dari media penyimpanan digital, metodologi yang digunakan dapat diterapkan untuk mengidentifikasi dan menganalisis bukti digital yang mungkin terkait dengan penyusupan atau aktivitas mencurigakan selama . |
| 108 | Galih Fanani, Imam Riadi, Anton Yudhana, 2022, "Analisis Forensik Aplikasi Michat Menggunakan Metode Digital Forensics Research Workshop" | Tujuan dari penelitian ini adalah untuk menganalisis aplikasi Michat dalam konteks forensik digital, dengan fokus pada pengumpulan dan analisis bukti digital yang terkait dengan kejahatan siber, seperti perdagangan narkoba, menggunakan kerangka kerja Digital Forensics Research Workshop (DFRWS). | Metode penelitian yang digunakan adalah kerangka kerja DFRWS, yang terdiri dari enam tahapan: identifikasi, pemeliharaan, pengumpulan, pemeriksaan, analisis, dan presentasi. Penelitian ini juga menggunakan beberapa alat forensik, seperti MOBILedit Forensic Express Pro, DB Browser For SQLite, dan Oxygen Forensic Detective untuk mengumpulkan dan menganalisis bukti. | Hasil penelitian menunjukkan bahwa alat forensik yang digunakan memiliki tingkat keberhasilan 100% dalam menemukan bukti digital, dengan perbandingan efektivitas alat yang berbeda. Kesimpulan dari penelitian ini adalah bahwa digital forensik dapat secara efektif digunakan untuk mengumpulkan bukti dari aplikasi Michat dalam kasus kejahatan siber. Saran yang diberikan adalah perlunya peningkatan keamanan aplikasi pesan instan untuk mencegah penyalahgunaan dan kejahatan siber lebih lanjut. | Penelitian ini memiliki kesamaan metodologis dengan studi Galih Fanani dkk. (2022) yang menganalisis bukti digital pada aplikasi MiChat menggunakan kerangka Digital Forensics Research Workshop (DFRWS). Namun, penelitian ini berfokus pada kasus *penyusupan Tiktok* dengan menerapkan metode NIST SP 800-86 untuk mengeksplorasi keunikan bukti digital (seperti log meeting, rekaman, dan metadata) yang tidak tercakup dalam studi sebelumnya. Temuan Fanani dkk. tentang efektivitas alat forensik juga mendorong penggunaan tools seperti FTK Imager atau Autopsy dalam penelitian ini untuk memastikan integritas bukti |
| 109 | Moh. Badri Tamam, Hoiriyah, Anwari, Yuri Efenie, 2023, "Analisis Forensik Originalitas Gambar Menggunakan Autopsy dan OpenCV". | Tujuan dari penelitian ini adalah untuk menganalisis keaslian gambar dengan menggunakan teknik forensik digital, khususnya melalui aplikasi Autopsy dan OpenCV, untuk mendeteksi manipulasi gambar yang dapat mengubah informasi visual yang disampaikan. | Metode penelitian yang digunakan meliputi analisis forensik digital dengan menggunakan Autopsy untuk menganalisis metadata dan keaslian gambar, serta OpenCV untuk memproses dan mengevaluasi gambar. Penelitian ini membandingkan gambar asli dan gambar yang telah diedit untuk mengidentifikasi perbedaan yang menunjukkan manipulasi. | Hasil penelitian menunjukkan bahwa terdapat perbedaan signifikan antara gambar asli dan gambar yang telah diedit, dengan nilai Ray yang menunjukkan penurunan pada gambar yang dimanipulasi. Kesimpulan dari penelitian ini adalah bahwa penggunaan Autopsy dan OpenCV efektif dalam mendeteksi manipulasi gambar. Saran yang diberikan adalah untuk melakukan penelitian lebih lanjut dengan menggunakan gambar yang beredar di media sosial untuk meningkatkan akurasi deteksi keaslian gambar. | tudi Moh. Badri Tamam dkk. (2023) membuktikan efektivitas Autopsy dan OpenCV dalam mendeteksi manipulasi gambar melalui analisis metadata dan pemrosesan visual. Penelitian ini memperkuat relevansi penggunaan alat forensik seperti Autopsy dalam investigasi digital, yang dapat diadaptasi untuk menganalisis bukti pada kasus *penyusupan Tiktok* (misalnya: rekaman meeting yang dimanipulasi). Namun, penelitian Anda mengkhususkan pada kerangka NIST SP 800-86 untuk menelusuri jejak penyusup (log, IP, timestamp) yang tidak tercakup dalam studi Tamam dkk. Temuan mereka tentang integritas data mendorong pentingnya validasi bukti digital dalam forensik Tiktok. |
| 110 | Mia Nuur Aini, Carudin, Dadang Yusup, 2021, "Analisis Tingkat Kemiripan Suara Sebagai Bukti Digital Dengan Menggunakan Teknik Audio Forensik". | Tujuan dari penelitian ini adalah untuk menganalisis tingkat kemiripan suara sebagai bukti digital dalam kasus penipuan melalui panggilan telepon, dengan menggunakan teknik audio forensik untuk membantu mengidentifikasi pelaku kejahatan. | Metode penelitian yang digunakan meliputi empat tahapan dalam audio forensik: acquisition, audio enhancement, decoding, dan voice recognition. Penelitian ini melibatkan pengambilan suara dari tiga subyek yang berbeda dan membandingkannya dengan rekaman suara bukti menggunakan analisis pitch dan formant untuk menentukan tingkat kemiripan suara. | Hasil penelitian menunjukkan bahwa subyek kedua memiliki tingkat kemiripan suara yang lebih tinggi dibandingkan dengan subyek lainnya, dengan analisis formant menunjukkan kemiripan suara sebanyak 2 kata untuk subyek 1, 2 kata untuk subyek 2, dan 3 kata untuk subyek 3. Kesimpulan dari penelitian ini adalah bahwa teknik audio forensik dapat digunakan secara efektif untuk menganalisis kemiripan suara dalam kasus penipuan. | Penelitian Aini dkk. (2021) membuktikan keefektifan analisis suara forensik, yang dapat diadaptasi untuk mengidentifikasi suara penyusup Tiktok. Namun, penelitian Anda melangkah lebih jauh dengan kerangka NIST SP 800-86 untuk mengintegrasikan bukti audio dengan log meeting dan metadata, menciptakan pendekatan forensik yang lebih holistik terhadap kasus Tiktok |
| 111 | Ilham Faisal, Arief Budiman, Elsya Indah Fitiria, 2023, "Penerapan Digital Forensics Research Workshop Dalam Akuisisi Evidence Forensik Aplikasi Snack Video". | Tujuan dari penelitian ini adalah untuk menerapkan metode Digital Forensics Research Workshop (DFRWS) dalam akuisisi bukti forensik dari aplikasi Snack Video, guna membantu pihak berwajib dalam mengungkap kejahatan siber yang terjadi di platform tersebut. | Metode penelitian yang digunakan mengikuti kerangka kerja DFRWS, yang mencakup tahapan identifikasi, preservasi, koleksi, pemeriksaan, analisis, dan presentasi. Penelitian ini menggunakan dua alat forensik, yaitu Oxygen Forensic dan Magnet Axiom, untuk mengumpulkan dan menganalisis bukti digital dari aplikasi Snack Video | Hasil penelitian menunjukkan bahwa penerapan metode DFRWS berhasil dalam mengidentifikasi dan mengumpulkan bukti digital, termasuk file text chat, video, gambar, dan metadata. Kesimpulan dari penelitian ini adalah bahwa bukti digital yang diperoleh dapat digunakan sebagai alat bukti yang sah dalam proses hukum. Saran yang diberikan adalah perlunya peningkatan penggunaan alat forensik yang lebih canggih dan pelatihan bagi penyidik untuk meningkatkan efektivitas dalam menangani kasus kejahatan siber. | Studi Faisal dkk. (2023) menegaskan pentingnya kerangka forensik terstruktur (DFRWS) dan alat seperti Magnet Axiom untuk akuisisi bukti digital. Penelitian ini mengadopsi prinsip serupa tetapi menerapkan NIST SP 800-86 guna menangani kompleksitas bukti pada platform Tiktok (log, IP, rekaman), sekaligus mengisi gap literatur dalam investigasi penyusupan daring (\*tiktok-bombing*).* |
| 112 | Dedy Hariyadi, Muhammad Agung Nugroho, Chanief Budi Setiawan, Arief Ikhwan Wicaksono, 2023, "Hybrid Acquisition pada Forensik Digital Berbasis ISO/IEC 27037:2012 Menggunakan Port Mirroring dan Single Board Computer" | Tujuan dari penelitian ini adalah untuk mengusulkan metode akuisisi hybrid dalam forensik digital yang menggabungkan akuisisi parsial dari perangkat router dan akuisisi fisik dari kartu memori Raspberry Pi, untuk menyelidiki kejahatan dunia maya, khususnya yang berkaitan dengan anomali lalu lintas jaringan. | Metode penelitian yang digunakan adalah akuisisi hybrid, yang terdiri dari akuisisi live menggunakan teknik port mirroring pada router Mikrotik dan akuisisi fisik pada kartu memori Raspberry Pi. Penelitian ini mengikuti standar ISO/IEC 27037:2012 dalam proses identifikasi, koleksi, akuisisi, dan preservasi bukti digital. | Hasil penelitian menunjukkan bahwa metode akuisisi hybrid efektif dalam mengumpulkan bukti digital dari lalu lintas jaringan dan perangkat penyimpanan. Kesimpulan dari penelitian ini adalah bahwa kombinasi teknik akuisisi ini dapat meningkatkan efektivitas penyelidikan kejahatan siber. Saran yang diberikan adalah untuk menerapkan metode ini dalam berbagai sistem dan jaringan untuk investigasi yang lebih komprehensif terhadap kejahatan dunia maya. | Penelitian Hariyadi dkk. (2023) tentang akuisisi hybrid berbasis ISO/IEC 27037 relevan untuk pengumpulan bukti jaringan dalam studi Anda (misal: pelacakan IP penyusup Tiktok). Namun, penelitian Anda menggunakan NIST SP 800-86 guna analisis lebih komprehensif, mencakup bukti cloud (rekaman, log) yang tidak dibahas dalam jurnal tersebut. Keduanya saling melengkapi dalam konteks forensik digital. |
| 113 | Deanna Durbin Hutagalung, Cholis Hanifurohman, Debby Rahadian Baskhara, 2023, "Analisa Forensik Memori pada Aplikasi E-Commerce Berbasis Web Menggunakan Metode National Institute of Justice (NIJ)". | Tujuan dari penelitian ini adalah untuk melakukan analisis forensik terhadap data memori browser pada aplikasi e-commerce berbasis web untuk meningkatkan keamanan data dan melindungi informasi sensitif pengguna. | Metode penelitian yang digunakan adalah analisis forensik berdasarkan pedoman National Institute of Justice (NIJ), yang terdiri dari lima tahap: Identifikasi, Pengumpulan, Pemeriksaan, Analisis, dan Pelaporan. Penelitian ini juga melibatkan studi literatur dan analisis hasil forensik memori pada lima aplikasi e-commerce, yaitu Tokopedia, Shopee, Lazada, Bukalapak, dan Orami. | Hasil penelitian menunjukkan bahwa dari lima aplikasi e-commerce yang dianalisis, ditemukan item barang dan nominal, tetapi username dan password tidak ditemukan, kecuali pada Lazada dan Bukalapak yang ditemukan username. Kesimpulan dari penelitian ini adalah bahwa meskipun data sensitif tidak selalu dapat diakses, penting untuk terus meningkatkan keamanan data dalam aplikasi e-commerce. Saran yang diberikan adalah untuk menerapkan langkah-langkah keamanan tambahan dan melakukan audit secara berkala untuk melindungi data pengguna. | Penelitian Hutagalung dkk. (2023) mengaplikasikan metode National Institute of Justice (NIJ) untuk analisis forensik memori pada aplikasi e-commerce berbasis web, dengan fokus pada identifikasi data sensitif seperti *username* dan transaksi. Studi ini relevan dengan penelitian Anda dalam hal metodologi forensik terstruktur (tahap identifikasi hingga pelaporan), yang sejalan dengan kerangka NIST SP 800-86 yang Anda gunakan. Namun, penelitian Anda berfokus pada platform Tiktok dengan bukti digital yang lebih beragam (log meeting, rekaman, metadata), bukan memori browser. Temuan Hutagalung dkk. tentang keterbatasan akses data sensitif (misalnya: *password*) menguatkan pentingnya analisis multi-sumber dalam forensik digital, termasuk pendekatan NIST untuk mengintegrasikan bukti dari berbagai aspek (jaringan, cloud, dan aktivitas *real-time*) guna mengungkap penyusupan Tiktok secara komprehensif. |
| 114 | Mutierly Sulastri, Tiwa Cindy Claudia Sinaga, Wulan Chorry Shafira, 2023, "Optimalisasi Metode Digital Forensik Sebagai Upaya Pengembalian Aset Negara Hasil Tindak Pidana Korupsi Dalam Bentuk Bitcoin." | Tujuan dari penelitian ini adalah untuk menganalisis dan mengoptimalkan metode digital forensik dalam upaya pemulihan aset negara yang dihasilkan dari tindak pidana korupsi, khususnya yang disembunyikan dalam bentuk Bitcoin. Penelitian ini bertujuan untuk memberikan solusi terhadap kesulitan yang dihadapi penegak hukum dalam mengidentifikasi dan mengembalikan aset yang telah dicuci melalui cryptocurrency. | Metode penelitian yang digunakan adalah kualitatif dengan pendekatan yuridis normatif. Penelitian ini melibatkan analisis literatur dan data virtual untuk mengevaluasi efektivitas metode digital forensik dalam mengidentifikasi dan mengembalikan aset negara yang disembunyikan dalam Bitcoin. Penelitian ini juga menekankan pentingnya kerjasama antar lembaga dalam proses pemulihan aset. | Hasil penelitian menunjukkan bahwa optimalisasi digital forensik dapat dilakukan melalui penguatan regulasi, peningkatan keterampilan akuntan forensik, dan kerjasama antara lembaga seperti PPATK, KPK, dan Kejaksaan. Kesimpulan dari penelitian ini adalah bahwa meskipun ada tantangan dalam mengungkap kejahatan yang melibatkan Bitcoin, langkah-langkah yang diusulkan dapat meningkatkan efektivitas pemulihan aset. Penelitian ini menyarankan agar pemerintah segera membentuk regulasi yang mengatur penggunaan Bitcoin dan memperkuat upaya digital forensik untuk menanggulangi pencucian uang. | Studi Sulastri dkk. (2023) tentang forensik Bitcoin menguatkan pentingnya metode terstandarisasi (seperti NIST SP 800-86 dalam penelitian Anda) untuk analisis bukti digital kompleks. Meski berbeda objek (kripto vs. Tiktok), keduanya menyoroti kebutuhan kolaborasi multidisiplin dan regulasi proaktif. Penelitian Anda melengkapi dengan fokus spesifik pada bukti *tiktok-bombing* (log, rekaman) yang belum tercakup dalam literatur forensik kripto. |
| 115 | Hasan Bisri, Marza Ihsan Marzuki, 2023, "Forensik Citra Digital Menggunakan Metode Error Level Analysis, Clone Detection dan Exif Untuk Deteksi Keaslian Gambar." | tujuan dari penelitian ini adalah untuk menganalisis keaslian citra digital dengan menggunakan tiga metode forensik, yaitu Error Level Analysis (ELA), Clone Detection (CD), dan Exif Metadata. Penelitian ini bertujuan untuk memberikan alternatif dalam pembuktian keaslian citra digital yang telah mengalami proses editing. | Metode penelitian yang digunakan adalah simulasi dengan menggunakan sampel citra digital asli dan citra yang telah diedit. Peneliti menerapkan ketiga metode forensik (ELA, CD, dan Exif) untuk menganalisis citra digital dari berbagai sumber pengambilan, serta menguji keandalan dan efektivitas masing-masing metode | Hasil penelitian menunjukkan bahwa ketiga metode forensik dapat digunakan secara efektif untuk mendeteksi keaslian citra digital yang telah dimanipulasi. Kesimpulan dari penelitian ini adalah bahwa kombinasi dari ELA, CD, dan Exif dapat memberikan hasil yang lebih akurat dalam analisis citra digital. Saran yang diberikan adalah perlunya pengembangan lebih lanjut dalam metode forensik untuk meningkatkan efektivitas dan kecepatan dalam mendeteksi pemalsuan citra digital. | Seperti studi Bisri & Marzuki (2023) yang membuktikan efektivitas kombinasi ELA, CD, dan Exif untuk deteksi manipulasi gambar, penelitian ini menerapkan NIST SP 800-86 untuk mengintegrasikan bukti forensik Tiktok (log, metadata, rekaman) guna mengungkap penyusupan. Temuan mereka tentang pentingnya multi-metode memperkuat perlunya pendekatan holistik dalam analisis insiden keamanan digital |
| 116 | Imam Riadi, Sunardi, Yana Safitri, 2023, "Analisis Forensik Cyberbullying pada Aplikasi IMO Messenger Menggunakan Metode Association of Chief Police Officers." | Tujuan dari penelitian ini adalah untuk menginvestigasi kejahatan cyberbullying yang terjadi melalui aplikasi IMO Messenger dengan mengumpulkan dan menganalisis bukti digital yang relevan. Penelitian ini bertujuan untuk memberikan pemahaman yang lebih baik tentang bagaimana cyberbullying dapat diidentifikasi dan ditangani secara forensik. | Metode penelitian yang digunakan adalah Association of Chief Police Officers (ACPO), yang terdiri dari empat tahapan: Plan, Capture, Analysis, dan Present. Penelitian ini melibatkan pengumpulan data digital dari aplikasi IMO Messenger, termasuk teks percakapan, user ID, dan grup, serta menggunakan alat MOBILEdit Forensic Express untuk analisis. | Hasil penelitian menunjukkan bahwa metode ACPO berhasil memperoleh 100% data digital untuk teks percakapan, user ID, dan grup, sementara data yang dihapus tidak dapat diperoleh. Kesimpulan dari penelitian ini adalah bahwa metode ACPO efektif dalam membantu penyelidikan kasus cyberbullying di aplikasi IMO Messenger. Saran yang diberikan adalah agar pengembang aplikasi lebih memperhatikan aspek keamanan data untuk mencegah penyalahgunaan. | Riadi dkk. (2023) tentang cyberbullying di IMO Messenger menggunakan metode ACPO relevan dengan penelitian Anda dalam hal pendekatan forensik terstruktur dan pengumpulan bukti digital. Meski berbeda platform (chat vs. video conference), keduanya menekankan pentingnya prosedur standar (ACPO/NIST) dan alat forensik yang tepat. Penelitian Anda memperluas cakupan dengan analisis bukti real-time Tiktok (log, rekaman) untuk investigasi *tiktok-bombing* yang lebih kompleks. |
| 117 | Ageng Restu Triyanto, Fahmi Fachri, 2024, "Analisis Forensik Bukti Digital Pada Kejahatan Berencana Menggunakan Metode National Institute of Justice." | Aplikasi Pencarian Jasa Tukang Berbasis Android bertujuan untuk membantu masyarakat dalam pemesanan atau pencarian jasa tukang yang terpercaya dan berkualitas. | Metode pengumpulan data yang digunakan adalah studi Pustaka. | tukang berfungsi dengan baik dan sesuai dengan spesifikasi yang diharapkan, menampilkan data dan informasi jasa tukang yang dibutuhkan oleh pengguna. | Penelitian Triyanto & Fachri (2024) tentang forensik digital dengan metode NIJ memperkuat dasar metodologis penelitian Anda. Meski berbeda konteks, keduanya menekankan pentingnya standar forensik (NIJ/NIST) dalam investigasi bukti digital. Penelitian Anda memberikan kontribusi spesifik dengan menerapkan NIST SP 800-86 untuk kasus tiktok-bombing yang belum banyak diteliti. |
| 118 | Ahmad Subki, Muh Nasirudin Karim, Bahtiar Imran, 2023, "Analisis Rekaman Suara pada Aplikasi Magic Call dengan Metode Forensik Audio untuk Mendapatkan Bukti Digital." | Tujuan dari penelitian ini adalah untuk menganalisis rekaman suara yang dihasilkan oleh aplikasi Magic Call menggunakan metode forensik audio. Penelitian ini bertujuan untuk menentukan keaslian suara yang diubah oleh aplikasi tersebut dan untuk mengidentifikasi karakteristik suara asli yang masih melekat pada rekaman yang dimanipulasi. | Metode penelitian yang digunakan adalah analisis forensik audio, yang meliputi pengumpulan rekaman suara asli dan rekaman suara yang dihasilkan oleh aplikasi Magic Call. Proses analisis dilakukan dengan menggunakan alat analisis seperti Praat untuk mendapatkan nilai pitch, formant, dan spektrogram dari kedua jenis rekaman tersebut. | Hasil penelitian menunjukkan bahwa analisis rekaman suara Magic Call dapat dilakukan dengan menggunakan analisis formant dan spektrogram, meskipun analisis pitch tidak dapat digunakan karena perbedaan yang signifikan antara rekaman asli dan rekaman yang dimodifikasi. Kesimpulan dari penelitian ini adalah bahwa meskipun suara dapat dimanipulasi, karakteristik tertentu dari suara asli masih dapat diidentifikasi. Saran yang diberikan adalah perlunya penelitian lebih lanjut untuk mengeksplorasi teknik analisis lain yang dapat meningkatkan akurasi dalam identifikasi suara yang dimodifikasi. | Penelitian Subki dkk. (2023) tentang forensik audio di *Magic Call* relevan dengan studi Anda dalam hal analisis bukti suara digital. Meski berbeda platform, teknik spektrogram dan formant analysis-nya dapat diadaptasi untuk memverifikasi rekaman Tiktok yang dicurigai palsu. Penelitian Anda melengkapi dengan pendekatan NIST SP 800-86 yang lebih holistik, mencakup log, metadata, dan aktivitas real-time untuk investigasi *tiktok-bombing*. |
| 119 | Steven Marcellino, Henki Bayu Seta, Wayan Widi, 2023, Analisis Forensik Digital Recovery Data Smartphone pada Kasus Penghapusan Berkas Menggunakan Metode National Institute Of Justice (NIJ) | Penelitian ini bertujuan untuk menganalisis proses pemulihan data digital dari smartphone Android yang telah dihapus, menggunakan metode National Institute of Justice (NIJ). Penelitian ini juga bertujuan untuk memberikan referensi bagi penyelidikan digital dan membantu penyidik dalam memperoleh bukti yang relevan. | Penelitian ini menggunakan metode NIJ yang terdiri dari lima tahap: identifikasi, pengumpulan, pemeriksaan, analisis, dan pelaporan. Data yang digunakan dalam penelitian ini meliputi file Excel, gambar, audio, video, dan file ZIP dari smartphone Android. Dua alat pemulihan data yang digunakan adalah Wondershare Dr Fone dan EaseUS Data Recovery. | Hasil penelitian menunjukkan bahwa EaseUS Data Recovery mampu mengembalikan 100% data yang dihapus, sementara Wondershare Dr Fone hanya berhasil mengembalikan 63% dari total data. EaseUS lebih efektif dalam memulihkan berbagai jenis file, termasuk file Excel dan ZIP, yang tidak dapat dipulihkan oleh Wondershare. Penelitian ini menyimpulkan bahwa metode NIJ efektif untuk menganalisis dan memulihkan data digital dari smartphone Android. Alat EaseUS Data Recovery terbukti lebih unggul dibandingkan Wondershare Dr Fone dalam pemulihan data yang terhapus. | Penelitian oleh Steven Marcellino dkk. (2023) yang mengaplikasikan metode National Institute of Justice (NIJ) dalam pemulihan data smartphone memberikan kontribusi penting terhadap penguatan proses investigasi digital, terutama dalam tahap identifikasi hingga pelaporan. Relevansi penelitian ini terhadap analisis forensik digital pada kasus penyusupan Tiktok terletak pada penerapan sistematis metode NIJ dalam menangani bukti digital, yang juga dapat diadaptasi dalam mengurai jejak digital penyusup, termasuk artefak komunikasi, file log, dan data cache yang mungkin telah dihapus dari perangkat pengguna atau pelaku. |
| 120 | Didik Sudyana, Irwan Hadi, Fietyata Yudha, 2023, Analisis Investigasi Forensik Digital pada Layanan Private Cloud Computing Menggunakan SNI 27037:2014 | Penelitian ini bertujuan untuk menganalisis proses investigasi forensik digital pada layanan private cloud computing, dengan menggunakan standar SNI 27037:2014. Fokus penelitian adalah untuk menemukan dan menganalisis barang bukti digital dari sisi pengguna yang terhubung dengan layanan private cloud. | Metode penelitian yang digunakan terdiri dari empat tahapan utama berdasarkan SNI 27037:2014, yaitu: persiapan sistem, studi kasus dan simulasi, penerapan standar SNI, serta analisis barang bukti. Penelitian ini melibatkan simulasi kasus pembocoran informasi oleh pengguna layanan cloud. | Hasil penelitian menunjukkan bahwa metode SNI 27037:2014 berhasil dalam menangani investigasi forensik digital. Beberapa barang bukti yang ditemukan meliputi data yang dihapus, riwayat akses cloud, dan log sistem yang menunjukkan aktivitas pengguna.Kesimpulan dari penelitian ini adalah bahwa investigasi forensik digital pada layanan private cloud dapat dilakukan secara efektif. Penggunaan SNI 27037:2014 memberikan panduan yang terstandar dan terstruktur untuk proses pencarian barang bukti. | Penelitian oleh Didik Sudyana dkk. (2023) menunjukkan pentingnya penerapan standar forensik digital seperti SNI 27037:2014 dalam menangani investigasi pada lingkungan cloud. Meskipun menggunakan standar berbeda, pendekatan sistematis yang mencakup persiapan sistem, analisis bukti digital, dan dokumentasi temuan memberikan wawasan penting bagi penerapan metode NIST dalam konteks penyusupan Tiktok, yang juga bergantung pada lingkungan digital terhubung. Temuan terkait data yang dihapus dan log akses sistem memperkuat kebutuhan akan proses forensik yang teliti, yang juga krusial dalam mengidentifikasi aktivitas penyusup dalam platform konferensi daring. |
| 121 | Nur Iman, Aris Susanto, Rahmat Inggi, 2019, "Analisa Perkembangan Digital Forensik dalam Penyelidikan Cybercrime di Indonesia (Systematic Review)." | Tujuan dari penelitian ini adalah untuk mengidentifikasi sub-sub digital forensik dan menganalisis perkembangan digital forensik dalam penyelidikan kasus kejahatan siber di Indonesia. Penelitian ini bertujuan untuk memberikan gambaran yang jelas mengenai tren dan efektivitas metode forensik digital yang digunakan dalam menangani kejahatan dunia maya. | Metode penelitian yang digunakan adalah kajian sistematis (systematic review) dengan proses pemilihan sumber data dari tiga database, yaitu Garba Rujukan Digital, Science and Technology Index, dan RAMA Repository. Penelitian ini melibatkan pencarian dan analisis jurnal yang relevan dengan topik digital forensik menggunakan kata kunci tertentu. | Hasil penelitian menunjukkan bahwa kejahatan yang paling banyak ditangani dalam konteks digital forensik adalah live forensic, network forensic, dan mobile forensic, dengan jumlah publikasi yang lebih tinggi dibandingkan dengan computer forensic dan database forensic. Kesimpulan dari penelitian ini adalah bahwa perkembangan digital forensik di Indonesia lebih banyak digunakan pada jenis forensik yang berkaitan dengan perangkat yang lebih dinamis dan terkoneksi. | Penelitian oleh Nur Iman dkk. (2019) relevan karena membahas tren *live* dan *network forensic* yang berkaitan langsung dengan penyusupan Tiktok. Meski tidak menggunakan metode NIST, hasilnya mendukung pentingnya forensik digital pada perangkat dan jaringan dinamis area yang jadi fokus dalam penelitian kamu. |
| 122 | Muhammad Rizki Setyawan, Hermansa, Muh Fadli Hasa, 2022, "Analisis Forensik Digital pada Skype Berbasis Windows 10 Menggunakan Framework ACPO." | Tujuan dari penelitian ini adalah untuk membandingkan hasil analisis forensik pada aplikasi Skype berbasis Windows 10 dengan menggunakan metode static forensic dan framework Association of Chief Police Officers (ACPO). Penelitian ini bertujuan untuk menemukan bukti digital yang relevan dalam konteks kejahatan siber yang menggunakan aplikasi Skype. | Metode penelitian yang digunakan adalah analisis forensik digital dengan pendekatan static forensic dan penerapan framework ACPO. Penelitian ini melibatkan pengumpulan data dari aplikasi Skype dan analisis menggunakan dua alat forensik, yaitu Autopsy dan Belkasoft Evidence Center, untuk mengevaluasi kinerja masing-masing alat dalam menemukan bukti digital. | Hasil penelitian menunjukkan bahwa Autopsy berhasil menemukan 15 kontak, 1 pesan teks, dan 9 file gambar dengan persentase kinerja sebesar 48%. Sementara itu, Belkasoft Evidence Center berhasil menemukan 15 kontak, 2 pesan teks, tetapi tidak dapat menemukan file gambar, dengan persentase kinerja sebesar 32%. Kesimpulan dari penelitian ini adalah bahwa Autopsy memiliki kinerja yang lebih baik dibandingkan Belkasoft dalam menemukan bukti digital yang telah terhapus. Saran yang diberikan adalah untuk menggunakan Autopsy sebagai alat utama dalam analisis forensik digital pada aplikasi Skype. | Penelitian oleh Muhammad Rizki Setyawan dkk. (2022) kurang relevan secara langsung dengan topik kamu karena menggunakan framework ACPO, bukan NIST. Namun, penelitian ini tetap memberikan referensi penting terkait proses analisis aplikasi komunikasi digital, yang mirip dengan Tiktok. Temuan tentang efektivitas alat forensik seperti Autopsy juga bisa jadi pertimbangan dalam analisis bukti digital dari platform serupa. |
| 123 | Ivan Adinata dan Yustian Servanda, 2024, Kajian Literatur: Metode Analisis dan Tools Live Forensics Pada Random Access Memory (RAM) | Tujuan dari kajian ini adalah untuk melakukan pengkajian terhadap mafdaetode analisis dan alat yang digunakan dalam live forensics pada RAM. Jurnal ini bertujuan memberikan wawasan mendalam dan panduan bagi peneliti serta praktisi dalam bidang forensik digital untuk mengaplikasikan metode dan alat yang tepat dalam pengumpulan serta analisis data dari memori aktif. | Metode penelitian yang digunakan adalah systematic literature review. Penulis mengidentifikasi, menilai, dan menginterpretasi topik penelitian berdasarkan literatur yang relevan. Pengumpulan literatur dilakukan melalui pencarian artikel di Google Cendekia dengan kata kunci terkait live forensics pada RAM. | Hasil penelitian menunjukkan bahwa metode NIST paling sering digunakan dalam analisis live forensics pada RAM. Terdapat beberapa tools yang diidentifikasi dalam literatur, seperti FTK Imager, RamCapturer, dan lain-lain, yang digunakan dalam berbagai tahapan analisis, yaitu collection, examination, analysis, dan reporting. Kesimpulan dari kajian ini adalah bahwa metode NIST lebih dominan dalam penggunaan live forensics untuk analisis RAM. Semua literatur yang ditelaah menunjukkan kesamaan dalam urutan tahapan analisis, yaitu collection, examination, analysis, dan reporting. Jurnal ini menekankan pentingnya penggunaan metode dan alat yang sesuai untuk mendapatkan hasil yang valid dalam investigasi digital. | Penelitian oleh Ivan Adinata dan Yustian Servanda (2024) sangat relevan dengan topik kamu karena secara langsung membahas penerapan metode NIST dalam *live forensics*, khususnya pada RAM—komponen penting dalam insiden penyusupan Tiktok. Kajian ini mendukung pendekatan kamu dengan menegaskan bahwa metode NIST efektif dan dominan digunakan dalam analisis memori aktif, serta memperkenalkan tools yang relevan untuk tahap-tahap forensik seperti collection hingga reporting. |
| 124 | Rivan Hikmawan , 2016, Forensik Digital Random Access Memory pada Sistem Operasi Linux Menggunakan Metode Dumpmemory | Tujuan dari proyek akhir ini adalah untuk memahami tahapan forensik memori dalam pengumpulan data dari memori volatile RAM sebagai bukti digital yang sah, serta untuk memperoleh hasil data forensik yang mencakup riwayat dan log aktivitas yang dilakukan oleh penyerang, menggunakan metode dumpmemory. | Metode yang digunakan dalam penelitian ini adalah SDLC (Systems Development Life Cycle), yang mencakup tahap perencanaan, analisis, desain, pengembangan, implementasi, dan perawatan sistem. Penelitian ini juga mengaplikasikan metode dumpmemory untuk mendapatkan snapshot dari RAM, yang kemudian dianalisis untuk menemukan bukti digital.. | Hasil penelitian menunjukkan bahwa metode dumpmemory efektif dalam mengumpulkan data dari RAM pada sistem operasi Linux. Data yang diperoleh berupa log aktivitas yang dapat digunakan untuk mengidentifikasi tindakan penyerang. Penelitian ini juga berhasil mengidentifikasi beberapa skenario serangan seperti session hijacking dan FTP attack. Kesimpulan dari penelitian ini adalah bahwa forensik RAM menggunakan metode dumpmemory dapat memberikan wawasan yang penting dalam investigasi digital. Data yang diperoleh dari RAM dapat dipertanggungjawabkan dan digunakan sebagai bukti dalam proses hukum. Penelitian ini menunjukkan bahwa pemahaman mendalam tentang metode dan alat yang digunakan dalam forensik digital sangat penting | Penelitian oleh Rivan Hikmawan (2016) cukup relevan dengan topik kamu karena membahas analisis forensik RAM, yang merupakan sumber penting untuk mendeteksi aktivitas penyusupan, seperti pada Tiktok. Meskipun tidak menggunakan metode NIST, pendekatan *dumpmemory* menunjukkan proses pengumpulan dan analisis data volatile yang sejalan dengan prinsip NIST. Hasilnya mendukung pentingnya RAM sebagai media kunci dalam mengungkap jejak digital pelaku. |
| 125 | Anton Yudhana, Imam Riadi, Riski Yudhi Prasongko, 2022, Forensik WhatsApp Menggunakan Metode Digital Forensic Research Workshop (DFRWS) | Tujuan penelitian ini adalah untuk mengumpulkan bukti forensik dari aplikasi WhatsApp, yang sering digunakan dalam kegiatan kriminal, dengan menerapkan metodologi DFRWS untuk memastikan keaslian dan integritas data digital. | Metode penelitian yang digunakan adalah Digital Forensic Research Workshop (DFRWS), yang mencakup tahapan identifikasi, preservasi, pengumpulan, pemeriksaan, analisis, dan presentasi bukti digital. Penggunaan perangkat lunak MOBILedit Forensic Express dan HashMyFiles juga menjadi bagian dari metodologi yang diterapkan. | Hasil penelitian menunjukkan bahwa perangkat lunak MOBILedit Forensic Express dapat mendeteksi bukti digital dengan tingkat akurasi 84,6%, sedangkan HashMyFiles dapat memastikan keaslian bukti dengan tingkat akurasi 100%. Penelitian ini mengidentifikasi 13 parameter sebagai fokus pencarian bukti. Kesimpulan dari penelitian ini adalah bahwa metode DFRWS efektif untuk mendeteksi dan mengumpulkan bukti digital dari aplikasi WhatsApp. Kedua alat yang digunakan menunjukkan kemampuan dalam mendeteksi dan memvalidasi barang bukti yang relevan untuk keperluan hukum. | Penelitian oleh Anton Yudhana dkk. (2022) kurang relevan langsung dengan topik penyusupan Tiktok karena fokus pada aplikasi WhatsApp. Namun, metodologi DFRWS yang diterapkan, dengan tahapan-tahapan forensik yang sistematis, memberikan gambaran yang berguna tentang bagaimana proses serupa dapat diterapkan pada platform lain, seperti Tiktok. Temuan terkait alat seperti MOBILedit Forensic Express dan HashMyFiles juga memberikan wawasan mengenai teknologi yang dapat mendeteksi dan memvalidasi bukti digital, yang relevan untuk analisis forensik pada aplikasi komunikasi digital lainnya |
| 126 | Pradipta Mahardika Sulaksono, Banu Santoso , 2022, Static Forensic Pada USB Mass Storage Menggunakan Forensics Toolkit Imager | Untuk mengevaluasi efektivitas metode static forensic berbasis NIST framework dalam proses recovery data digital yang dihapus secara permanen dari berbagai jenis perangkat penyimpanan USB, serta memastikan integritas data tetap terjaga selama proses forensic. | Penelitian ini menggunakan metode static forensic dengan menerapkan framework NIST SP 800-86, yang meliputi empat tahapan: *Collection, Examination, Analysis*, dan *Reporting*. Eksperimen dilakukan pada tiga jenis perangkat USB mass storage (USB Flash Drive, USB Hard Disk Drive, dan Micro Memory Card) dengan bantuan tools FTK Imager, HashTab, dan Microsoft Office. File dihapus permanen dari perangkat dan dilakukan proses recovery melalui imaging dan validasi nilai hash. | Penelitian membuktikan bahwa metode static forensic dengan FTK Imager dan framework NIST mampu melakukan recovery 100% data dari ketiga perangkat yang diuji. Validasi dilakukan dengan pengecekan nilai hash dan metadata. Hasil ini menunjukkan bahwa prosedur forensic yang ketat dan penggunaan tools yang tepat dapat menghasilkan bukti digital yang valid dan forensik. | Penelitian ini cukup relevan secara metodologis, karena menggunakan framework NIST SP 800-86, sama seperti yang kamu gunakan untuk analisis forensik penyusupan Tiktok. Namun, fokus penelitian ini adalah forensik perangkat penyimpanan USB dengan pendekatan static (post-incident), bukan pada data volatile di aplikasi komunikasi daring seperti Tiktok. Meski begitu, teknik imaging, validasi hash, dan sistematika pelaporan dapat menjadi referensi penting untuk mendukung integritas bukti dalam riset kamu lainnya |
| 127 | Ikhsan Zuhriyanto, Anton Yudhana, dan Imam Riadi, 2018, "Perancangan Digital Forensik pada Aplikasi Twitter Menggunakan Metode Live Forensics." | Tujuan dari penelitian ini adalah untuk mendapatkan bukti digital dari aplikasi Twitter dengan menerapkan metode live forensics. Penelitian ini bertujuan untuk memberikan pemahaman tentang bagaimana bukti digital dapat diperoleh dan digunakan dalam penanganan tindak kejahatan di dunia maya, khususnya yang terjadi di platform media sosial. | Metode penelitian yang digunakan adalah metode live forensics yang diadaptasi dari National Institute of Justice (NIJ). Penelitian ini melibatkan tahapan persiapan, pengumpulan, pemeriksaan, analisis, dan pelaporan untuk mendapatkan bukti digital dari aplikasi Twitter. Alat yang digunakan dalam penelitian ini termasuk FTK Imager untuk mengelola dan menganalisis data. | Hasil penelitian menunjukkan bahwa metode live forensics efektif dalam mengumpulkan bukti digital dari aplikasi Twitter, termasuk informasi seperti nama akun, data lokasi, dan konten tweet. Kesimpulan dari penelitian ini adalah bahwa bukti digital yang diperoleh dapat digunakan sebagai barang bukti yang valid dalam penanganan kasus kejahatan siber. Saran yang diberikan adalah perlunya pengembangan lebih lanjut dalam teknik forensik digital untuk meningkatkan efektivitas pengumpulan bukti di media sosial. | Penelitian oleh Ikhsan Zuhriyanto dkk. (2018) relevan dengan topik kamu karena menerapkan metode *live forensics* yang juga diadaptasi dari metode NIST, yang penting untuk menganalisis aktivitas real-time pada platform seperti Tiktok. Proses pengumpulan dan analisis bukti digital dalam aplikasi Twitter dapat diterapkan pada analisis jejak digital penyusupan daring, mengingat kedua platform sama-sama berbasis komunikasi daring. Penggunaan alat seperti FTK Imager juga relevan untuk mendalami bukti yang mungkin tersembunyi dalam aktivitas pengguna. |
| 128 | Rahmat Novrianda Dasmen, Ferry Kurniawan, 2021, Digital Forensik Deleted Cyber Crime Evidence pada Pesan Instan Media Sosial | Tujuan penelitian ini adalah untuk mengungkap bukti digital dari tindakan cyberbullying yang terjadi di platform media sosial, khususnya melalui aplikasi Facebook Messenger dan WhatsApp, meskipun bukti tersebut telah terhapus atau sengaja dihapus oleh pelaku. | Metode yang digunakan dalam penelitian ini adalah Action Research, yang mencakup tahapan diagnosis, perencanaan tindakan, pelaksanaan, evaluasi, dan pembelajaran. Penelitian ini melibatkan penggunaan teknik digital forensik untuk mengidentifikasi dan mengumpulkan bukti dari perangkat mobile yang digunakan dalam tindakan cyberbullying. | Hasil penelitian menunjukkan bahwa teknik digital forensik dapat berhasil mengidentifikasi dan mengungkap bukti cyberbullying dalam bentuk teks, gambar, dan video, meskipun data tersebut telah dihapus. Peneliti menggunakan alat seperti DumpIt dan WinHex untuk mengakses dan menganalisis data yang tersimpan dalam RAM perangkat. Kesimpulan dari penelitian ini adalah bahwa digital forensik merupakan metode yang efektif untuk mengungkap bukti-bukti digital yang telah dihapus, dengan catatan bahwa perangkat mobile yang digunakan masih dapat diakses. Proses dump pada RAM dapat memfasilitasi pemulihan informasi yang relevan untuk penyelidikan. | Penelitian oleh Rahmat Novrianda Dasmen dkk. (2021) relevan dengan topik kamu karena membahas teknik digital forensik untuk mengungkap bukti yang telah dihapus, terutama dalam konteks aplikasi komunikasi seperti WhatsApp, yang mirip dengan Tiktok. Metode *dump RAM* yang digunakan dalam penelitian ini, serta alat seperti DumpIt dan WinHex, dapat diterapkan untuk mengakses data dari Tiktok yang mungkin terhapus atau tersembunyi, mendukung analisis forensik dalam penyusupan daring. |
| 129 | Bayu Tapa Brata, Abrar Hiswara, 2020, Optimalisasi Validitas Pengujian Otentisitas dan Kredibilitas pada Forensik Foto Digital dengan Metode ACE-V | Tujuan penelitian ini adalah untuk menguji kinerja tiga teknik pengujian otentisitas dan kredibilitas foto dalam forensik digital, yaitu jpeg-ghost, histogram equalization-gamma correction, dan error level analysis (ELA). Penelitian ini bertujuan untuk meningkatkan validitas hasil pengujian dengan menerapkan prosedur verifikasi dari metode ACE-V. | Metode yang digunakan dalam penelitian ini adalah ACE-V, yang terdiri dari empat tahap: Analysis, Comparison, Evaluation, dan Verification. Dalam penelitian ini, penulis menguji tiga teknik pengujian otentisitas foto terhadap beberapa kategori manipulasi foto, seperti splicing-duplicate, splicing-erase, dan copy-move. | Hasil penelitian menunjukkan bahwa ketiga teknik pengujian dapat mendeteksi berbagai jenis manipulasi foto dengan tingkat akurasi yang berbeda. Teknik jpeg-ghost efektif dalam mendeteksi splicing-duplicate dan splicing-erase, sedangkan teknik ELA memberikan hasil yang baik dalam mendeteksi copy-move. Kesimpulan dari penelitian ini adalah bahwa kombinasi dari berbagai teknik pengujian dapat meningkatkan validitas hasil pengujian otentisitas foto digital. Penggunaan metode ACE-V memungkinkan peneliti untuk mendapatkan temuan yang lebih relevan dan akurat. | Penelitian oleh Bayu Tapa Brata dkk. (2020) kurang relevan langsung dengan topik kamu karena fokus pada forensik foto digital, sedangkan penelitian kamu berkaitan dengan penyusupan dalam Tiktok. Namun, metode ACE-V yang diterapkan dalam pengujian otentisitas dapat memberi wawasan tentang bagaimana proses analisis yang sistematis dan terverifikasi diterapkan dalam forensik digital, yang bisa diterapkan untuk memastikan keabsahan bukti digital yang ditemukan dalam penyusupan daring. |
| 130 | Halimah Septya Mikayla, Ari Kusyanti, Primantara Hari Trisnawan, 2024, Analisis Forensik Digital untuk Investigasi Kasus Cyberbullying pada Media Sosial TikTok | Jurnal ini bertujuan untuk mengumpulkan dan menganalisis bukti digital terkait kasus cyberbullying di TikTok, dengan menerapkan model investigasi forensik digital yang berfokus pada jejaring sosial. Penelitian ini diharapkan dapat membantu akademisi, praktisi forensik digital, dan pihak berwenang dalam memahami dan menangani kasus cyberbullying. | Metode penelitian dilakukan dengan studi literatur untuk merancang skenario kasus cyberbullying, serta menerapkan investigasi forensik digital. Fase penelitian mencakup perencanaan, pengumpulan data, dan analisis bukti digital menggunakan alat forensik yang sesuai untuk kedua platform TikTok, yaitu Android dan web. | Penelitian ini berhasil mengumpulkan bukti digital yang substansial, dengan 68,8% kesesuaian antara data awal skenario dan data yang ditemukan melalui analisis forensik. Hasil menunjukkan perbedaan signifikan dalam bukti digital yang diperoleh dari TikTok Android dan TikTok web. Jurnal menyimpulkan bahwa investigasi forensik digital efektif dalam mengidentifikasi dan mengumpulkan bukti terkait kasus cyberbullying di TikTok. Penelitian ini menegaskan perlunya penerapan metode forensik yang sistematis untuk mengatasi masalah cyberbullying secara hukum. | Penelitian oleh Halimah Septya Mikayla dkk. (2024) cukup relevan dengan topik kamu, meskipun fokus pada kasus cyberbullying di TikTok. Metode yang diterapkan dalam pengumpulan dan analisis bukti digital, serta penggunaan alat forensik pada platform media sosial, dapat diadaptasi untuk penelitian kamu mengenai penyusupan dalam Tiktok. Pendekatan sistematis dalam mengidentifikasi dan menganalisis bukti digital, serta penggunaan metode forensik yang tepat, sangat relevan untuk menganalisis jejak digital yang mungkin ada dalam penyusupan daring. |
| 131 | Ayubi Wirara, Bangkit Hardiawan, Muhammad Salman, 2020, Identifikasi Bukti Digital pada Akuisisi Perangkat Mobile dari Aplikasi Pesan Instan “WhatsApp” | Tujuan penelitian ini adalah untuk menganalisis dan mengidentifikasi bukti digital yang dapat diperoleh dari aplikasi WhatsApp pada perangkat smartphone, baik berbasis Android maupun iOS, dalam konteks forensik digital. | Metode penelitian yang digunakan meliputi instalasi aplikasi WhatsApp pada perangkat mobile yang tidak di-root/jailbreak, diikuti dengan skenario percakapan yang telah ditentukan. Proses akuisisi dan ekstraksi data dilakukan dengan menggunakan tools digital forensik yang umum digunakan oleh para ahli. | Hasil penelitian menunjukkan bahwa artefak penting dari aplikasi WhatsApp dapat diakses, termasuk database SQLite yang menyimpan informasi percakapan, kontak, dan media. Penelitian ini berhasil mengekstrak data dari perangkat Android dan iOS tanpa perlu melakukan root atau jailbreak pada perangkat. Penelitian ini menyimpulkan bahwa bukti digital dari aplikasi WhatsApp masih dapat diperoleh dengan metode akuisisi yang tepat. Tools forensik yang ada saat ini dapat digunakan untuk mengekstrak data WhatsApp meskipun perangkat tidak dimodifikasi. Penelitian ini juga menyarankan untuk mengembangkan metode forensik lebih lanjut terkait fitur-fitur baru WhatsApp. | Penelitian oleh Ayubi Wirara dkk. (2020) relevan dengan topik kamu dalam konteks penerapan metode forensik digital untuk mengidentifikasi bukti dari aplikasi komunikasi, meskipun penelitian ini fokus pada WhatsApp. Teknik akuisisi data dan ekstraksi bukti digital tanpa memodifikasi perangkat, seperti yang dilakukan dalam penelitian ini, dapat diterapkan untuk mengidentifikasi bukti digital dari Tiktok, terutama terkait percakapan dan data yang disembunyikan atau dihapus. Pendekatan ini mendukung pengumpulan bukti dari platform komunikasi yang digunakan dalam penyusupan daring. |
| 132 | Deska Widodo, 2019, Analisis Forensik Digital Aplikasi WhatsApp dan Facebook Messenger pada Android sebagai Barang Bukti Digital dalam Penanganan Kasus Prostitusi Online | Tujuan penelitian ini adalah untuk menganalisis bukti digital yang dapat diperoleh dari aplikasi WhatsApp dan Facebook Messenger pada perangkat Android, khususnya dalam konteks penanganan kasus prostitusi online. Penelitian ini bertujuan untuk menunjukkan bagaimana data dari aplikasi tersebut dapat digunakan sebagai barang bukti dalam proses hukum. | Metode penelitian yang digunakan meliputi eksperimen dengan skenario percakapan pada aplikasi yang diteliti. Data dikumpulkan melalui proses akuisisi menggunakan tools forensik seperti Oxygen Forensic dan Mobiledit Forensic Express Pro. Penelitian dilakukan dengan menganalisis data yang diambil dari kedua aplikasi untuk menentukan nilai bukti digital yang relevan. | Hasil penelitian menunjukkan bahwa data percakapan dari WhatsApp dan Facebook Messenger dapat diakses dan dianalisis meskipun ada penghapusan. Penelitian ini berhasil mengekstrak dan membuktikan bahwa informasi yang diperoleh dari kedua aplikasi tersebut dapat digunakan sebagai bukti dalam kasus prostitusi online. Penelitian ini menyimpulkan bahwa aplikasi WhatsApp dan Facebook Messenger menyimpan informasi yang sangat berharga sebagai bukti digital dalam kasus-kasus kriminal. Bukti digital yang dihasilkan dari kedua aplikasi ini dapat dipertanggungjawabkan dalam proses hukum, dan analisis forensik dapat dilakukan tanpa memerlukan akses root pada perangkat. | Penelitian Deska Widodo (2019) relevan dengan topik kamu karena berfokus pada analisis forensik aplikasi komunikasi, yakni WhatsApp dan Facebook Messenger, dalam konteks pengumpulan bukti digital yang dapat digunakan dalam proses hukum. Meskipun penelitian ini lebih berfokus pada kasus prostitusi online, teknik yang digunakan untuk mengakses data percakapan yang telah dihapus melalui forensik digital dapat diterapkan dalam kasus penyusupan Tiktok. Metode akuisisi data dan penggunaan alat forensik tanpa perlu mengakses root perangkat dapat diterapkan untuk mengidentifikasi dan memverifikasi bukti dalam investigasi penyusupan Tiktok. |
| 133 | Tayomi Dwi Larasati, 2017, Analisis Live Forensics untuk Perbandingan Aplikasi Instant Messenger (LINE, Facebook, dan Telegram) pada Sistem Operasi Windows 10. | Tujuan dari penelitian ini adalah untuk mengimplementasikan teknik live forensics dalam menginvestigasi bukti digital dari aktivitas penggunaan aplikasi instant messenger, yaitu LINE, Facebook, dan Telegram. Penelitian ini bertujuan untuk mengetahui karakteristik dan perbandingan bukti digital yang dihasilkan dari ketiga aplikasi tersebut. | Metode penelitian yang digunakan adalah eksperimen dengan skenario percakapan yang umum terjadi pada aplikasi instant messenger. Penelitian ini melibatkan pengambilan data digital menggunakan alat seperti DumpIt dan Belkasoft RamCapturer, serta analisis data menggunakan WinHex dan Belkasoft Evidence Center. | Kesimpulan dari penelitian ini adalah bahwa live forensics dapat digunakan untuk mengevaluasi keamanan aplikasi instant messenger. Perbedaan dalam struktur dan pengelolaan data di masing-masing aplikasi mempengaruhi jumlah dan kualitas bukti digital yang dapat diperoleh. | Penelitian Tayomi Dwi Larasati (2017) relevan dengan topik kamu karena mengimplementasikan teknik live forensics untuk menginvestigasi aplikasi instant messenger (LINE, Facebook, dan Telegram) pada sistem operasi Windows 10. Teknik yang digunakan untuk mengumpulkan dan menganalisis bukti digital dapat diterapkan dalam konteks penyusupan Tiktok, terutama dalam mengidentifikasi dan memperoleh bukti digital yang terhubung dengan aktivitas percakapan. Pendekatan live forensics yang digunakan di penelitian ini, seperti penggunaan alat forensik dan analisis data, dapat diadaptasi untuk menganalisis bukti dari aplikasi Tiktok terkait penyusupan atau kegiatan mencurigakan lainnya selama virtual. |
| 134 | Vipkas Al Hadid Firdaus, Dodit Suprianto, Rini Agustina, 2021, Analisis Forensik Digital Memori Volatile untuk Mendapatkan Kunci Enkripsi Aplikasi Dm-Crypt. | Tujuan dari penelitian ini adalah untuk mengidentifikasi dan mendapatkan kunci enkripsi dari aplikasi dm-crypt melalui analisis forensik pada memori volatile. Penelitian ini bertujuan untuk membantu penyidik cybercrime dalam mengakses informasi penting yang terakses dalam memori saat investigasi, khususnya pada sistem operasi Linux. | Metode penelitian yang digunakan adalah analisis forensik memori dengan melakukan live memory dump menggunakan alat LiME (Linux Memory Extractor). Penelitian ini juga melibatkan proses akuisisi data dari memori komputer dalam kondisi aktif untuk menemukan kunci enkripsi yang digunakan oleh dm-crypt. | Kesimpulan dari penelitian ini adalah bahwa analisis forensik pada memori volatile dapat menjadi metode efektif untuk menemukan kunci enkripsi dalam kasus disk yang terenkripsi menggunakan dm-crypt. Teknik ini sangat bermanfaat bagi penyidik untuk mengakses informasi yang sebelumnya tersembunyi. | Penelitian Vipkas Al Hadid Firdaus, Dodit Suprianto, dan Rini Agustina (2021) relevan dengan topik kamu karena mengaplikasikan teknik analisis forensik memori volatile untuk mendapatkan kunci enkripsi dari aplikasi dm-crypt. Meskipun fokus penelitian ini pada Linux dan dm-crypt, teknik yang digunakan, seperti live memory dump dengan alat LiME, dapat diterapkan dalam konteks penyusupan Tiktok untuk memperoleh bukti digital dari memori yang sedang aktif selama . Pendekatan ini menawarkan wawasan tentang bagaimana analisis memori volatile dapat digunakan untuk mendapatkan informasi penting yang mungkin tersembunyi dalam sistem yang terenkripsi atau aktif, yang relevan untuk investigasi forensik digital dalam kasus penyusupan atau kebocoran informasi selama virtual. |
| 135 | Arum Hidayah, Fahmi Fachri, 2024, Analisis Bukti Digital Terhadap Kasus Prostitusi Online Pada Aplikasi MiChat Menggunakan Metode ACPO | Penelitian ini bertujuan untuk menganalisis barang bukti digital dari kasus prostitusi online yang terjadi pada aplikasi MiChat, serta membandingkan efektivitas dua alat forensik dalam pengambilan bukti. | Metode yang digunakan dalam penelitian ini adalah Association of Chief Police Officers (ACPO), dengan alat bantu FTK Imager dan MOBILedit Forensic. | Hasil penelitian menunjukkan bahwa FTK Imager mampu memperoleh lebih banyak barang bukti digital (75%) dibandingkan MOBILedit Forensic (68,75%). Bukti yang berhasil diperoleh mencakup pesan gambar, video, dan audio, tetapi tidak ada pesan teks yang dapat dipulihkan. | Penelitian ini relevan dengan topik Anda mengenai analisis forensik digital pada penyusupan dalam Tiktok menggunakan metode NIST, karena keduanya melibatkan teknik forensik digital untuk mengungkap kejahatan siber. Penekanan pada pengumpulan dan analisis bukti digital sangat penting dalam kedua konteks tersebut. |
| 136 | Achmad Iqbal Yuladi, Rini Indrayani, 2023, Analisis dan Perbandingan Tools Forensik Menggunakan Metode NIST dalam Penanganan Kasus Kejahatan Siber | Penelitian ini bertujuan untuk menganalisis dan membandingkan efektivitas dua tools forensik dalam menangani kasus cyberbullying pada aplikasi WhatsApp. | Metode yang digunakan adalah National Institute of Standards and Technology (NIST), dengan analisis menggunakan tools MOBILedit Forensic Express dan Magnet Axiom. | Hasil penelitian menunjukkan bahwa Magnet Axiom memiliki akurasi lebih tinggi (81,8%) dibandingkan MOBILedit Forensic Express (72,7%) dalam ekstraksi barang bukti digital. Kedua tools tidak berhasil mengembalikan pesan yang telah dihapus karena objek dalam kondisi un-rooted. | Penelitian ini relevan dengan topik Anda tentang analisis forensik digital, khususnya dalam penggunaan metode NIST. Kedua penelitian fokus pada pengumpulan dan analisis bukti digital untuk mengungkap kejahatan siber, yang penting dalam konteks forensik digital secara umum. |
| 137 | Aditya Primukti, Putri Kartika Sari, Didit Suhartono, Khairunnisak Nur Isnaini, 2025, Analisis Memori Forensik pada Aplikasi TikTok Berbasis Web Menggunakan Metode National Institute of Justice (NIJ) | Penelitian ini bertujuan untuk menganalisis memori forensik pada aplikasi TikTok berbasis web dan mengidentifikasi informasi penting yang tersimpan selama sesi penggunaan. | Metode yang digunakan adalah National Institute of Justice (NIJ), dengan perangkat lunak FTK Imager 4.7.1 dan HxD untuk analisis memori. | Hasil analisis menunjukkan bahwa informasi yang berhasil diidentifikasi mencakup nomor telepon untuk login, riwayat pencarian, dan nama pengguna aktif. Namun, data sensitif seperti kode OTP tidak ditemukan, menandakan adanya langkah keamanan yang diterapkan oleh TikTok. | Penelitian ini relevan dengan analisis forensik digital yang Anda lakukan, terutama dalam konteks penggunaan metode NIJ. Keduanya menekankan pentingnya pengumpulan dan analisis bukti digital untuk mengungkap aktivitas pengguna pada platform online. |
| 138 | Ageng Restu Triyanto, Fahmi Fachri, 2024, Analisis Forensik Bukti Digital Pada Kejahatan Pembunuhan Berencana Menggunakan Metode National Institute of Justice | Penelitian ini bertujuan untuk menganalisis bukti digital yang terkait dengan kejahatan pembunuhan berencana, termasuk pemulihan data yang dihapus dari SSD dan flashdisk. | Metode yang digunakan adalah National Institute of Justice (NIJ), dengan alat bantu FTK Imager dan Autopsy untuk analisis data. | Hasil penelitian menunjukkan bahwa penggunaan metode NIJ efektif dalam mengidentifikasi dan mengembalikan data yang dihapus secara permanen, dengan presentase keberhasilan 100% untuk penghapusan permanen, sedangkan untuk penghapusan format, tidak ada data yang berhasil dipulihkan. | Penelitian ini relevan dengan topik Anda tentang analisis forensik digital, terutama dalam konteks penggunaan metode NIJ dan pemulihan data. Keduanya menekankan pentingnya bukti digital dalam pengungkapan kejahatan. |
| 139 | Anton Yudhana, Rusydi Umar, Ahwan Ahmadi, 2018, Akuisisi Data Forensik Google Drive Pada Android Dengan Metode National Institute of Justice (NIJ) | Penelitian ini bertujuan untuk menganalisis dan mengakuisisi data forensik dari Google Drive pada perangkat Android, serta memeriksa keamanan data yang tersimpan di media penyimpanan cloud. | Metode yang digunakan adalah National Institute of Justice (NIJ), dengan alat bantu Oxygen Forensic dan MOBILedit Forensic. | Hasil akuisisi menunjukkan bahwa metode NIJ efektif dalam menemukan dan memulihkan data yang dihapus dari Google Drive. Oxygen Forensic mampu mengidentifikasi lebih banyak data dibandingkan dengan MOBILedit Forensic. | Penelitian ini relevan dengan topik Anda tentang analisis forensik digital, terutama dalam konteks penggunaan metode NIJ untuk mengungkap data yang dapat dijadikan bukti dalam kasus kejahatan siber. |
| 140 | Akhsan Tofik, Ghufron Zaida Muflih, 2024, Akuisisi Barang Bukti Digital Pada Aplikasi Discord Menggunakan Metode ACPO | Penelitian ini bertujuan untuk melakukan akuisisi dan analisis bukti digital dari aplikasi Discord, khususnya terkait kasus cyberbullying, menggunakan metode ACPO. | Metode yang digunakan adalah ACPO (Association of Chief Police Officers), dengan alat bantu FTK Imager dan Autopsy untuk analisis bukti digital. | Hasil penelitian menunjukkan bahwa metode ACPO efektif dalam mengidentifikasi dan mengamankan bukti digital terkait cyberbullying. Penelitian berhasil menemukan 80 pesan teks, 6 gambar, dan 17 data yang dihapus. | Penelitian ini sangat relevan dengan topik Anda tentang analisis forensik digital, karena keduanya menggunakan metode sistematis (NIJ vs. ACPO) untuk mengungkap bukti digital dari platform komunikasi. Kedua penelitian menyoroti pentingnya pemulihan data yang dapat digunakan dalam proses hukum, serta tantangan yang dihadapi dalam menangani kejahatan siber. |
| 141 | Arjun Zakari Yahya, Dirman, Dadang Juwoto Buru, 2022, Analisis Bukti Digital Pada Random Access Memory Android Menggunakan Metode Live Forensic Kasus Penjualan Senjata Illegal | Penelitian ini bertujuan untuk mengidentifikasi dan mengakuisisi bukti digital dari Random Access Memory (RAM) pada smartphone pelaku dan korban dalam kasus penjualan senjata illegal. | Metode yang digunakan adalah Live Forensic, dengan analisis mengikuti langkah-langkah dari NIST (National Institute of Standards Technology) dan menggunakan perangkat FTK (Forensic Tool Kit). | Hasil penelitian menunjukkan bahwa metode Live Forensic efektif dalam mengidentifikasi dan memulihkan bukti digital, termasuk log panggilan, SMS, dan data WhatsApp. Penelitian berhasil menemukan bukti yang dihapus, yang mengindikasikan aktivitas ilegal. | Penelitian ini sangat relevan dengan topik Anda mengenai analisis forensik digital, terutama dalam konteks penggunaan metode Live Forensic untuk mengungkap bukti dalam kasus kejahatan. Keduanya menekankan pentingnya pengambilan dan analisis data yang valid untuk mendukung proses hukum. |
| 142 | Azis Fahrudin, Gufron Zaida Muflih, 2024, Analisis Forensik Digital Pada Pesan WhatsApp Yang Terenkripsi Dengan Pretty Good Privacy (PGP) Menggunakan Framework DFRWS | Penelitian ini bertujuan untuk menganalisis dan memulihkan pesan WhatsApp yang terenkripsi menggunakan PGP dalam konteks kasus pengedaran narkoba. | Metode yang digunakan adalah framework DFRWS (Digital Forensics Research Workshop) dengan analisis menggunakan perangkat lunak MOBILedit Forensic Express dan Kleopatra. | Hasil penelitian menunjukkan bahwa framework DFRWS efektif dalam memulihkan dan menganalisis bukti digital, termasuk pesan terenkripsi dan private key. Penelitian berhasil mengungkap detail transaksi narkoba, memberikan kontribusi signifikan bagi penegakan hukum. | Penelitian ini sangat relevan dengan topik Anda mengenai analisis forensik digital, terutama dalam konteks penggunaan metode DFRWS untuk mengatasi tantangan enkripsi dalam penyelidikan kejahatan. Keduanya menyoroti pentingnya pemulihan data yang aman dan valid untuk mendukung proses hukum. |
| 143 | Desti Mualfah, Afdel Viransa, Hasanatul Fu’adah Amran, 2021, Akuisisi Bukti Digital Pada Aplikasi TamTam Messenger Menggunakan Metode National Institute of Justice | Penelitian ini bertujuan untuk menganalisis dan mengembalikan bukti digital yang dihapus dari aplikasi TamTam Messenger pada smartphone, dalam konteks kasus cyberbullying. | Metode yang digunakan adalah National Institute of Justice (NIJ), dengan analisis menggunakan perangkat lunak MobileEdit Forensic. | Hasil penelitian menunjukkan bahwa metode NIJ efektif dalam mengidentifikasi dan memulihkan bukti digital, termasuk pesan yang dihapus. Penelitian berhasil mengembalikan bukti berupa pesan teks dan gambar. | Penelitian ini sangat relevan dengan topik Anda mengenai analisis forensik digital, karena keduanya menggunakan metode sistematis (NIJ) untuk mengungkap bukti digital dari platform komunikasi. Keduanya menekankan pentingnya pengumpulan dan pemulihan data yang valid untuk mendukung proses hukum, terutama dalam konteks kejahatan siber. |
| 144 | Desti Mualfah, Rizdqi Akbar Ramadhan, 2020, Analisis Forensik Metadata Kamera CCTV Sebagai Alat Bukti Digital | Penelitian ini bertujuan untuk menganalisis metadata dari rekaman kamera CCTV sebagai alat bukti digital dalam proses hukum, serta memastikan integritas dan keaslian bukti digital. | Metode yang digunakan adalah live forensik dengan pendekatan berdasarkan SNI 27037:2014 dan kerangka kerja Common Phases of Computer Forensics Investigation Models. | Hasil penelitian menunjukkan bahwa metode live forensik efektif dalam mengidentifikasi dan mengamankan bukti digital dari kamera CCTV. Metadata yang berhasil diekstrak memberikan informasi penting untuk mendukung proses hukum. | Penelitian ini sangat relevan dengan topik Anda mengenai analisis forensik digital, terutama dalam konteks pengumpulan dan analisis bukti digital dari perangkat perekam. Keduanya menegaskan pentingnya penerapan metode yang tepat untuk memastikan integritas bukti dalam investigasi. |
| 145 | Desti Mualfah, Muhammad Iqbal Syam, Baidarus, 2023, Analisis Perbandingan Tools Mobile Forensic Menggunakan Metode National Institute of Justice (NIJ) | Penelitian ini bertujuan untuk membandingkan kinerja dua tools forensik dalam mengembalikan data yang dihapus pada aplikasi Signal Messenger dalam konteks kasus transaksi narkoba. | Metode yang digunakan adalah National Institute of Justice (NIJ), dengan perbandingan dua tools forensik: Oxygen Forensic Detective dan Belkasoft Evidence Center. | Hasil penelitian menunjukkan bahwa Oxygen Forensic Detective lebih unggul, berhasil mendapatkan 5 dari 6 total bukti digital dengan tingkat akurasi 83,33%, sedangkan Belkasoft Evidence Center hanya berhasil mendapatkan 4 dari 6 bukti digital dengan akurasi 66,67%. | Penelitian ini sangat relevan dengan topik Anda tentang analisis forensik digital, terutama dalam konteks perbandingan alat forensik. Keduanya menekankan pentingnya pemilihan tools yang tepat untuk mengungkap bukti digital dalam investigasi kejahatan siber, serta penerapan metode NIJ yang sistematis. |
| 146 | Desti Mualfah, Afdel Viransa, Hasanatul Fu’adah Amran, 2024, Investigasi dan Analisis Pengembalian Pesan Whatsapp yang Sudah Terhapus Menggunakan Metode National Institute of Justice (NIJ) | Penelitian ini bertujuan untuk menganalisis dan mengembalikan bukti digital yang dihapus dari aplikasi TamTam Messenger dalam konteks kasus cyberbullying. | Metode yang digunakan adalah National Institute of Justice (NIJ), dengan analisis menggunakan perangkat lunak MobileEdit Forensic. | Hasil penelitian menunjukkan bahwa metode NIJ efektif dalam mengidentifikasi dan memulihkan bukti digital, termasuk pesan yang dihapus. Penelitian berhasil mengembalikan bukti berupa pesan teks dan gambar. | Penelitian ini relevan dengan topik Anda mengenai analisis forensik digital, meskipun menggunakan metode yang berbeda (NIJ vs. NIST). Keduanya menekankan pada pentingnya pengumpulan dan pemulihan data yang valid untuk mendukung proses hukum. Namun, pendekatan Anda dengan metode NIST mungkin menawarkan kerangka kerja yang lebih sistematis dalam konteks penyusupan dalam aplikasi seperti Tiktok, dibandingkan dengan pendekatan NIJ yang digunakan dalam penelitian ini. |
| 147 | Ilham Faisal, Arief Budiman, Elsya Indah Fitiria, 2023, Penerapan Digital Forensics Research Workshop Dalam Akuisisi Evidence Forensik Snack Video | Penelitian ini bertujuan untuk menerapkan metode DFRWS dalam mengakuisisi bukti digital dari aplikasi Snack Video, dengan fokus pada kasus kejahatan cybercrime. | Metode yang digunakan adalah Digital Forensics Research Workshop (DFRWS), yang meliputi tahapan identifikasi, pemeliharaan, koleksi, pemeriksaan, analisis, dan presentasi. | Hasil penelitian menunjukkan bahwa kedua tools forensik, yaitu Oxygen Forensic dan Magnet Axiom, berhasil menemukan berbagai bukti digital. Oxygen Forensic mencapai tingkat akurasi 100%, sedangkan Magnet Axiom mencapai 83,3%. | Penelitian ini relevan dengan topik Anda mengenai analisis forensik digital, meskipun menggunakan metode yang berbeda (DFRWS vs. NIST). Sementara Anda berfokus pada penyusupan dalam Tiktok menggunakan metode NIST, penelitian ini menunjukkan aplikasi DFRWS dalam konteks media sosial dan cybercrime. Keduanya menekankan pentingnya metodologi yang sistematis dalam pengumpulan dan analisis bukti digital. |
| 148 | Erly Dwi Ariyanti, Carudin, Dadang Yusup, 2022, IDENTIFIKASI BUKTI DIGITAL INSTAGRAM WEB DENGAN LIVE FORENSIC PADA KASUS PENIPUAN ONLINE SHOP | Penelitian ini bertujuan untuk mengidentifikasi bukti digital dari kasus penipuan online di Instagram, menggunakan metode live forensic untuk menemukan percakapan yang dihapus oleh pelaku. | Metode yang digunakan adalah NIST (National Institute of Standards and Technology), dengan pendekatan live forensic untuk mengidentifikasi bukti digital. | Hasil penelitian menunjukkan bahwa penggunaan tools FTK Imager dan Browser History Viewer berhasil mengidentifikasi 39 percakapan yang dihapus, yang dapat digunakan sebagai bukti dalam kasus penipuan online. | Penelitian ini sangat relevan dengan topik Anda mengenai analisis forensik digital menggunakan metode NIST. Keduanya menekankan pentingnya metodologi yang sistematis dalam pengumpulan dan analisis bukti digital. Anda sama-sama menggunakan pendekatan NIST untuk mengidentifikasi dan memulihkan bukti dalam konteks kejahatan siber, meskipun fokus Anda mungkin berbeda. |
| 149 | Faul Isnaeni, Fahmi Fachri, 2025, ANALISIS FORENSIK SMARPHONE ANDROID PADA APLIKASI TIKTOK MENGGUNAKAN METODE NIST | Penelitian ini bertujuan untuk menginvestigasi kasus pencemaran nama baik di TikTok dengan memulihkan video, hashtag, dan pesan teks yang telah dihapus dari perangkat smartphone Android. | Metode yang digunakan adalah NIST (National Institute of Standards and Technology), dengan fokus pada tahapan Collection, Examination, Analysis, dan Reporting | Hasil penelitian menunjukkan bahwa penggunaan tools Mobiledit dan FTK Imager berhasil mengidentifikasi bukti digital, dengan tingkat keberhasilan 100% untuk Mobiledit dan 74,4% untuk FTK Imager dalam mengembalikan data yang dihapus. | Penelitian ini memiliki relevansi dengan topik Anda yang juga menggunakan metode NIST untuk analisis forensik digital. Meski fokus Anda pada penyusupan dalam Tiktok berbeda dari konteks pencemaran nama baik di TikTok, keduanya menekankan pentingnya metodologi yang sistematis dalam pengumpulan dan analisis bukti digital. Namun, jika Anda merasa topik ini kurang relevan dengan fokus spesifik Anda, hal tersebut bisa dicatat. |
| 150 | Febe Dwi Intan Permatasari, 2023, ANALISIS AKTIVITAS CYBER BULLYING PENGGUNA FACEBOOK MELALUI BROWSER CHROME DENGAN PENDEKATAN LIVE FORENSICS | Penelitian ini bertujuan untuk menganalisis aktivitas cyber bullying di Facebook melalui browser Chrome dan mengumpulkan bukti digital menggunakan metode forensik. | Metode yang digunakan adalah NIST (National Institute of Standards and Technology) dengan pendekatan live forensic. | Hasil penelitian menunjukkan bahwa metode live forensic efektif dalam mengidentifikasi bukti digital, dengan hasil yang mencakup riwayat percakapan, gambar, dan data relevan lainnya. | Penelitian ini relevan dengan topik Anda mengenai analisis forensik digital, karena keduanya menggunakan metode NIST untuk pengumpulan dan analisis bukti digital. Meskipun fokus Anda adalah pada penyusupan dalam Tiktok, prinsip-prinsip yang diterapkan dalam penelitian ini dapat memberikan wawasan tambahan tentang bagaimana metode NIST dapat diterapkan dalam konteks yang berbeda, seperti dalam kasus cyber bullying di media sosial. |
| 151 | Febriand Gysberth Pariela Zamsari, Teguh Wahyono, 2024, Forensic Investigation of Digital Evidence on Flash Disk with Forensic Process Method Based on NIST | Penelitian ini bertujuan untuk menyelidiki bukti digital yang terdapat pada flash disk dengan menggunakan metode NIST untuk menentukan validitas bukti digital. | Metode yang digunakan adalah NIST (National Institute of Standards and Technology) untuk proses investigasi forensik. | Hasil penelitian menunjukkan bahwa evidence pada skenario 1 dan 4 dianggap valid untuk diajukan ke pengadilan, sedangkan evidence pada skenario 2 dan 3 tidak valid. | Penelitian ini relevan dengan topik Anda mengenai analisis forensik digital menggunakan metode NIST. Keduanya menekankan pentingnya metodologi yang sistematis dalam pengumpulan dan analisis bukti digital. Meskipun fokus Anda berbeda, yaitu pada penyusupan dalam Tiktok, prinsip-prinsip NIST yang diterapkan dalam kedua penelitian ini menunjukkan konsistensi dalam penerapan metode forensik yang tepat. |
| 152 | Firmansyah Yasin, Abdul Fadlil, Rusydi Umar, 2021, Identifikasi Bukti Forensik Jaringan Virtual Router Menggunakan Metode NIST | Tujuan penelitian ini adalah untuk mengidentifikasi bukti forensik dari lalu lintas jaringan virtual router dengan memanfaatkan metode NIST untuk meningkatkan efektivitas dalam investigasi forensik. | Penelitian ini menggunakan metode National Institute of Standards and Technology (NIST), yang mencakup tahapan koleksi, pemeriksaan, analisis, dan pelaporan. Alat yang digunakan termasuk Windump untuk merekam lalu lintas, serta Network Miner dan Wireshark untuk analisis bukti. | Penelitian ini menyimpulkan bahwa penggunaan metode NIST efektif dalam mengidentifikasi bukti digital dalam skenario serangan siber. Hasil percobaan menunjukkan bahwa sistem berhasil merekam 220494 paket, dan bukti-bukti tersebut telah diverifikasi menggunakan alat analisis yang berbeda. | Penelitian ini sangat relevan dengan topik analisis forensik digital terhadap penyusupan dalam Tiktok menggunakan metode NIST. Metode yang sama digunakan dalam konteks yang berbeda (virtual router) menegaskan fleksibilitas dan efektivitas NIST dalam situasi forensik digital. Selain itu, tantangan yang dihadapi dalam investigasi forensik di lingkungan virtual juga dapat memberikan wawasan untuk penanganan kasus penyusupan dalam platform seperti Tiktok. |
| 153 | Fitri Anggraini et al., 2023, Akuisisi Bukti Digital Tiktok Berbasis Android Menggunakan Metode National Institute of Justice | Tujuan penelitian ini adalah untuk melakukan proses forensik dalam mendapatkan bukti pencemaran nama baik dan ancaman melalui aplikasi TikTok di perangkat Android. | Penelitian ini menggunakan metode National Institute of Justice (NIJ) dengan tahapan identifikasi, koleksi, pemeriksaan, analisis, dan pelaporan. Alat yang digunakan adalah MOBILedit Forensic Express. | Penelitian ini menyimpulkan bahwa proses forensik yang dilakukan pada smartphone yang sudah di-root berhasil mendapatkan lebih banyak data (85,7% keberhasilan) dibandingkan yang belum di-root (42,8% keberhasilan). Bukti yang dapat diambil mencakup informasi akun, pesan, dan gambar, tetapi beberapa data seperti video dan hashtag tidak dapat diakses pada smartphone yang belum di-root | Penelitian ini relevan dengan topik analisis forensik digital terhadap penyusupan dalam Tiktok, karena keduanya menggunakan metode NIJ untuk mengumpulkan dan menganalisis bukti digital. Temuan dalam penelitian ini dapat memberikan wawasan mengenai teknik yang efektif dalam akuisisi bukti digital dari aplikasi media sosial, yang dapat diterapkan dalam konteks penyelidikan forensik pada platform Tiktok. |
| 154 | Muh. Hajar Akbar et al., 2024, INVESTIGASI STEGO FILE MENGGUNAKAN FRAMEWORK NATIONAL INSTITUTE OF JUSTICE | Tujuan penelitian ini adalah untuk menganalisis dan mengekstraksi bukti digital yang mengandung pesan steganografi, serta untuk menunjukkan bahwa file hasil ekstraksi dapat dijadikan bukti digital yang sah secara hukum. | Penelitian ini menggunakan metode static forensics dengan menerapkan lima tahapan dari framework National Institute of Justice (NIJ), yaitu identifikasi, pengumpulan, pemeriksaan, analisis, dan pelaporan. Alat yang digunakan mencakup FTK Imager, Autopsy, WinHex, Hiderman, dan StegSpy. | Hasil penelitian menunjukkan bahwa dari 10 file yang diskenariokan, 9 file terdeteksi mengandung pesan steganografi. Proses ekstraksi menggunakan Hiderman menunjukkan tingkat keberhasilan 90%, dengan file yang berhasil diekstraksi dapat digunakan sebagai bukti yang sah. | Penelitian ini relevan dengan topik analisis forensik digital terhadap penyusupan dalam Tiktok, terutama dalam hal penggunaan teknik forensik yang sistematis dan terstandarisasi seperti NIJ. Teknik steganografi yang dibahas juga dapat memberikan wawasan tambahan tentang bagaimana informasi dapat disembunyikan dalam konteks komunikasi digital, yang bisa diterapkan dalam investigasi penyusupan di platform seperti Tiktok. |
| 155 | Harno Supardin et al., 2022, Analisis Perbandingan Tools Forensik Digital pada Instagram Messenger menggunakan Metode National Institute of Standards and Technology (NIST) | Tujuan penelitian ini adalah untuk membandingkan kinerja dua tools forensik digital dalam mengembalikan data yang telah terhapus pada Instagram Messenger, khususnya dalam konteks kasus kejahatan cyber. | Penelitian ini menggunakan metode NIST yang mencakup tahapan Collection, Examination, Analysis, dan Reporting. Alat yang digunakan adalah MOBILedit Forensic dan Magnet Axiom Forensic untuk mendapatkan bukti digital dari Instagram Messenger. | Hasil penelitian menunjukkan bahwa Magnet Axiom Forensic memiliki akurasi lebih tinggi (76,92%) dibandingkan MOBILedit Forensic (69,23%) dalam mengembalikan data yang telah dihapus. Penelitian ini menegaskan pentingnya penggunaan metode NIST dalam proses penyidikan forensik digital. | Penelitian ini relevan dengan topik analisis forensik digital terhadap penyusupan dalam Tiktok. Metode NIST yang digunakan untuk mengumpulkan dan menganalisis bukti digital memberikan dasar yang kuat untuk investigasi yang sistematis. Temuan mengenai efektivitas tools forensik juga dapat diaplikasikan dalam konteks penyelidikan penyusupan di platform lain, termasuk Tiktok. |
| 156 | Hendra et al., 2021, Teknik Audio Forensik untuk Analisis Rekaman Suara sebagai Barang Bukti Digital | Tujuan penelitian ini adalah untuk menganalisis dan membuktikan kepemilikan suara dalam rekaman suara yang dijadikan barang bukti digital, serta untuk menunjukkan efektivitas teknik audio forensik dalam mengidentifikasi rekaman suara. | Penelitian ini menggunakan teknik audio forensik untuk menganalisis rekaman suara sebagai barang bukti digital. Metode yang diterapkan meliputi tahapan akuisisi, perbaikan audio, dekoding, dan pengenalan suara. Analisis dilakukan menggunakan parameter pitch, formant, dan spectrogram. | Hasil penelitian menunjukkan bahwa sampel A memiliki jumlah kata yang identik dengan rekaman suara barang bukti di semua analisis yang dilakukan. Teknik audio forensik terbukti efektif dalam menunjukkan kepemilikan rekaman suara, meskipun analisis formant dianggap paling lemah dibandingkan dengan analisis lain. | Penelitian ini relevan dengan topik analisis forensik digital terhadap penyusupan dalam Tiktok, karena keduanya mengandalkan teknik forensik untuk menganalisis bukti digital. Teknik yang digunakan dalam analisis suara dapat memberikan wawasan tambahan dalam menangani bukti audio yang mungkin muncul dalam kasus penyusupan, seperti rekaman percakapan yang relevan. |
| 157 | Imam Mahfudl Nasrulloh et al., 2019, Analisis Forensik Solid State Drive (SSD) Menggunakan Framework GRR Rapid Response | Tujuan penelitian ini adalah untuk mengimplementasikan framework GRR Rapid Response dalam akuisisi dan analisis data dari SSD, serta mengevaluasi efektivitas metode ini dalam mengembalikan bukti digital. | Penelitian ini menggunakan metode live forensik dengan framework GRR Rapid Response untuk menganalisis Solid State Drive (SSD) dalam konteks kehilangan data. Tahapan forensik mengikuti standar dari National Institute of Standards Technology (NIST), mencakup pengumpulan, pemeriksaan, analisis, dan pelaporan. | Hasil penelitian menunjukkan bahwa framework GRR Rapid Response efektif dalam mengembalikan bukti digital dari SSD. Validasi menunjukkan bahwa nilai hash dari bukti digital yang dikembalikan identik dengan nilai hash dari file asli, menggunakan algoritma MD5 dan SHA-1. | Penelitian ini relevan dengan topik analisis forensik digital terhadap penyusupan dalam Tiktok, karena keduanya mengandalkan metode forensik yang sistematis untuk mengumpulkan dan menganalisis bukti digital. Penggunaan metode live forensik dan framework GRR dapat memberikan wawasan tambahan untuk investigasi dalam konteks keamanan digital yang lebih luas. |
| 158 | Imam Riadi et al., 2018, Forensic Tools Performance Analysis on Android-based Blackberry Messenger using NIST Measurements | Tujuan dari penelitian ini adalah untuk membandingkan efektivitas masing-masing alat forensik dalam mendapatkan dan menganalisis bukti digital terkait kejahatan siber yang terjadi melalui aplikasi Blackberry Messenger. | Penelitian ini menggunakan metode NIST untuk mengevaluasi kinerja tiga alat forensik: Andriller, Oxygen Forensic Suite, dan Autopsy 4.1.1 dalam mengakuisisi bukti digital dari Blackberry Messenger pada smartphone Android. Proses analisis mencakup tahap pengumpulan, pemeriksaan, analisis, dan pelaporan. | Hasil penelitian menunjukkan bahwa Oxygen Forensic Suite memiliki kinerja terbaik dengan nilai indeks kinerja 100%, diikuti oleh Andriller dengan 25%. Autopsy 4.1.1 tidak berhasil mengembalikan artefak apapun. Oxygen Forensic Suite berhasil memenuhi hampir semua kriteria NIST, sementara Andriller dan Autopsy memiliki kelemahan tertentu dalam akuisisi data. | Penelitian ini relevan dengan topik analisis forensik digital terhadap penyusupan dalam Tiktok, karena keduanya menggunakan metode forensik yang terstruktur untuk mengumpulkan dan menganalisis bukti digital. Temuan tentang efektivitas alat forensik dalam menangani aplikasi komunikasi dapat memberikan wawasan berharga untuk investigasi penyusupan di platform lain. |
| 159 | Imam Riadi et al. 2019, Analisis Forensik Recovery pada Smartphone Android Menggunakan Metode National Institute Of Justice (NIJ) | Tujuan utama dari penelitian ini adalah untuk mengevaluasi efektivitas berbagai alat forensik dalam mengembalikan data yang dihapus, seperti pesan, log panggilan, dan kontak, dari smartphone Android. | Penelitian ini menggunakan metode National Institute of Justice (NIJ) untuk menganalisis forensik recovery data pada smartphone Android. Alat yang digunakan dalam penelitian ini adalah MOBILedit Forensic, Wondershare dr. Fone for Android, dan Belkasoft Evidence Center untuk mengembalikan data yang telah dihapus. | Hasil penelitian menunjukkan bahwa Wondershare dan Belkasoft berhasil mengembalikan data yang telah dihapus, sementara MOBILedit hanya dapat menampilkan data yang belum dihapus. Wondershare berhasil mengembalikan data kontak, log panggilan, dan pesan, sedangkan Belkasoft dapat mengembalikan log panggilan dan kontak. | Penelitian ini relevan dengan topik analisis forensik digital terhadap penyusupan dalam Tiktok, karena keduanya menggunakan metode forensik terstruktur untuk mengumpulkan dan menganalisis bukti digital. Temuan tentang efektivitas alat forensik dalam konteks komunikasi digital dapat memberikan wawasan tambahan untuk investigasi penyusupan yang melibatkan data yang dihapus atau disembunyikan. |
| 160 | Abdul Isnan Fahrial Sinusi et al., 2023, Analisis Bukti Digital Untuk Penanganan Kekerasan Berbasis Gender Online Pada Media Sosial Whatsapp Menggunakan Metode National Institute Of Justice (NIJ) | Tujuan utama penelitian ini adalah untuk mengakuisisi dan menganalisis bukti digital dari aplikasi WhatsApp yang digunakan dalam tindakan pelecehan seksual, serta memberikan panduan bagi penegak hukum dalam menangani kasus-kasus KBGO. | Penelitian ini menggunakan metode National Institute of Justice (NIJ) untuk melakukan analisis forensik terhadap bukti digital yang terkait dengan Kekerasan Berbasis Gender Online (KBGO) melalui aplikasi WhatsApp. Proses investigasi meliputi tahapan persiapan, koleksi, pemeriksaan, analisis, dan pelaporan. | Hasil penelitian menunjukkan bahwa dengan menggunakan alat forensik seperti Magnet Axiom dan MOBILedit Forensic Express, peneliti berhasil mengidentifikasi dan mengembalikan bukti digital, termasuk pesan dan gambar yang terkait dengan tindakan pelecehan. Proses akuisisi dan analisis menggunakan metode NIJ terbukti efektif dalam menangani kasus KBGO. | Penelitian ini relevan dengan topik analisis forensik digital terhadap penyusupan dalam Tiktok, karena keduanya menggunakan pendekatan sistematis untuk mengumpulkan dan menganalisis bukti digital. Temuan tentang penggunaan alat forensik dalam konteks kekerasan berbasis gender di media sosial dapat memberikan wawasan tambahan untuk investigasi keamanan digital yang lebih luas. |
| 161 | Jusia Amanda Ginting et al., 2024, REKONSTRUKSI DAN INVESTIGASI DIGITAL FORENSIK PADA APLIKASI WHATSAPP DENGAN METODE NIST : KASUS PELECEHAN SEKSUAL | Tujuan penelitian ini adalah untuk mengevaluasi efektivitas metode forensik dalam mengungkap dan menganalisis bukti digital dari WhatsApp, serta untuk mengidentifikasi tantangan dalam mengatasi pelecehan seksual melalui platform tersebut. | Penelitian ini menggunakan metode National Institute of Standards Technology (NIST) untuk melakukan investigasi forensik terhadap bukti digital terkait kasus pelecehan seksual yang terjadi melalui aplikasi WhatsApp. Proses investigasi terdiri dari empat tahap: pengumpulan data, pemeriksaan, analisis, dan pelaporan. | Hasil penelitian menunjukkan bahwa sebagian besar pesan yang dihapus dapat dipulihkan menggunakan alat forensik seperti FTK Imager dan WhatsApp Viewer, meskipun pesan yang dihapus dengan fitur "unsent" tidak dapat dipulihkan. Dari total 11 pesan yang diteliti, 55% berhasil dipulihkan, sementara 45% tidak dapat diakses. | Penelitian ini relevan dengan topik analisis forensik digital terhadap penyusupan dalam Tiktok, karena keduanya menggunakan pendekatan sistematis untuk mengumpulkan dan menganalisis bukti digital. Temuan tentang efektivitas metode dan alat forensik dalam konteks kekerasan berbasis gender di media sosial dapat memberikan wawasan tambahan untuk investigasi keamanan digital yang lebih luas. |
| 162 | Jeki Kuswanto et al., 2023, AKUISISI GOOGLE DRIVE ANDROID MENGGUNAKAN OXYGEN DAN MOBILedit DENGAN METODE NATIONAL INSTITUTE OF JUSTICE | Tujuan utama penelitian ini adalah untuk mengevaluasi efektivitas dua alat forensik dalam mengakses dan mengembalikan data dari Google Drive di smartphone, serta mengidentifikasi informasi penting yang dapat digunakan sebagai bukti digital. | Penelitian ini menggunakan metode National Institute of Justice (NIJ) untuk mengakuisisi data dari Google Drive pada perangkat Android. Proses penelitian dibagi menjadi beberapa tahapan: identifikasi, koleksi, pemeriksaan, analisis, dan pelaporan, dengan menggunakan alat forensik seperti Oxygen dan MOBILedit. | Hasil penelitian menunjukkan bahwa Oxygen Forensic berhasil mengembalikan 100% data yang diujikan, termasuk alamat akun, kata sandi, dan file-file penting. Sebaliknya, MOBILedit hanya berhasil mengembalikan 20% dari data yang diakuisisi, terbatas pada informasi dasar seperti gambar dan lokasi GPS. | Penelitian ini relevan dengan topik analisis forensik digital karena sama-sama memanfaatkan metode sistematis untuk mengumpulkan dan menganalisis bukti digital. Temuan mengenai efektivitas alat forensik dalam konteks penyimpanan cloud dapat memberikan wawasan untuk investigasi yang melibatkan data digital dalam kejahatan siber lainnya. |
| 163 | Karolina Eka Purnama et al., 2023, ANALISIS FORENSIC CITRA DIGITAL MENGGUNAKAN TEKNIK ERROR LEVEL ANALYSIS DAN METADATA BERDASARKAN METODE NIST | Tujuan utama penelitian ini adalah untuk membuktikan keaslian bukti digital melalui analisis citra yang telah dimanipulasi, serta untuk mengidentifikasi tanda-tanda pemalsuan menggunakan alat forensik. | Penelitian ini menggunakan metode National Institute of Standards Technology (NIST) untuk menganalisis keaslian citra digital. Proses penelitian mencakup tahap identifikasi, pengumpulan data, pemeriksaan, analisis, dan pelaporan, dengan menerapkan teknik Error Level Analysis (ELA) dan analisis metadata. | Hasil penelitian menunjukkan bahwa foto yang dimanipulasi dapat teridentifikasi melalui analisis metadata dan ELA. Foto asli terdeteksi sebagai gambar yang tidak dimanipulasi, sedangkan foto yang telah diedit menggunakan perangkat lunak seperti Adobe Photoshop menunjukkan tanda-tanda manipulasi. Penelitian ini menegaskan pentingnya teknik forensik dalam mengidentifikasi dan menganalisis citra digital. | Penelitian ini relevan dengan topik analisis forensik digital, terutama dalam konteks pengumpulan dan analisis bukti digital. Temuan tentang penggunaan ELA dan analisis metadata dapat memberikan wawasan tambahan untuk investigasi yang melibatkan bukti visual dalam kasus-kasus digital, termasuk penyusupan atau pemalsuan informasi. |
| 164 | Mustofa Julianto dan Yustian Servanda, 2024, Kajian Literatur: Analisis Perbandingan Efektivitas Tools Forensik Recovery Data Pada Smartphone Android | Tujuan utama penelitian ini adalah untuk membandingkan efektivitas berbagai tools forensik dalam mengatasi masalah kejahatan digital yang melibatkan data yang dihapus pada smartphone, serta memberikan wawasan mengenai proses forensik yang dapat digunakan oleh penegak hukum. | Penelitian ini menggunakan pendekatan studi literatur untuk menganalisis efektivitas berbagai alat forensik dalam pemulihan data pada smartphone Android. Fokusnya adalah pada metode National Institute of Justice (NIJ) dan National Institute of Standards and Technology (NIST). | Hasil kajian menunjukkan bahwa penggunaan metode NIJ dan NIST efektif dalam pemulihan data pada smartphone Android. Alat Oxygen Forensic menunjukkan tingkat keberhasilan 100% dalam mengidentifikasi data, sementara MOBILedit hanya 20%. Penelitian ini menegaskan pentingnya alat forensik yang tepat untuk investigasi digital. | Penelitian ini relevan dengan topik analisis forensik digital karena membahas pemulihan dan analisis bukti digital, yang sama pentingnya dalam konteks penyelidikan kejahatan. Temuan mengenai efektivitas alat forensik dapat memberikan panduan untuk penelitian lebih lanjut dalam bidang digital forensik. |
| 165 | Marcel Afandi et al., 2024, Analisis Forensik Pemalsuan Dokumen PDF Menggunakan Metode National Institute of Justice (NIJ) | Tujuan utama penelitian ini adalah untuk membuktikan keaslian dokumen PDF melalui analisis forensik, serta untuk mengidentifikasi tanda-tanda manipulasi dan pemalsuan. | Penelitian ini menggunakan metode National Institute of Justice (NIJ) untuk menganalisis keaslian dokumen PDF yang diduga dipalsukan. Proses penelitian meliputi identifikasi, pengumpulan, pemeriksaan, analisis, dan pelaporan, dengan menggunakan alat seperti Exiftools, Jpegsnoop, dan Adobe Acrobat Reader. | Hasil penelitian menunjukkan bahwa metode NIJ dan analisis menggunakan Principal Component Analysis (PCA) efektif dalam mendeteksi manipulasi dokumen PDF. Temuan menunjukkan adanya perbedaan signifikan antara metadata dokumen asli dan yang telah dimanipulasi, serta kemampuan untuk mengidentifikasi perubahan yang dilakukan. | Penelitian ini relevan dengan topik analisis forensik digital, khususnya dalam konteks pemalsuan dokumen. Temuan mengenai penggunaan metode forensik untuk mendeteksi manipulasi dalam dokumen dapat memberikan wawasan tambahan untuk studi lebih lanjut dalam bidang keamanan informasi dan investigasi digital. |
| 166 | Muhammad Marzuki dan Tata Sutabri,2023, ANALISIS FORENSIK MEDIA SOSIAL MICHAT METODE DIGITAL FORENSIK INTEGRATED INVESTIGATION FRAMEWORK (IDFIF) | Tujuan utama penelitian ini adalah untuk menyelidiki kejahatan yang terjadi melalui aplikasi Michat, termasuk penipuan dan cybercrime, dengan menggunakan alat forensik untuk mendapatkan bukti digital yang valid. | Penelitian ini menggunakan metode Digital Forensic Integrated Investigation Framework (IDFIF) untuk menganalisis dokumen dan bukti dari aplikasi Michat. Proses penelitian meliputi tahapan identifikasi, pengumpulan, pemeriksaan, analisis, dan pelaporan. | Hasil penelitian menunjukkan bahwa metode IDFIF efektif dalam mengidentifikasi dan memulihkan bukti digital dari aplikasi Michat. Alat forensik yang digunakan berhasil mencapai tingkat keberhasilan 100% dalam menemukan bukti yang diperlukan untuk investigasi. | Penelitian ini relevan dengan analisis forensik digital, terutama dalam konteks penggunaan aplikasi pesan untuk kejahatan. Temuan yang berkaitan dengan pengumpulan dan analisis bukti digital dapat memberikan wawasan tambahan untuk penelitian lebih lanjut dalam bidang keamanan informasi dan investigasi kriminal. |
| 167 | Mohammad Yan Fikri Hendrawan, Subektiningsih, Arifiyanto Hadinegoro, 2023, Analisis Bukti Digital Pada Discord Browser Menggunakan Teknik Live Forensic Dengan Metode NIST SP 800-86 | Menelusuri dan memulihkan bukti digital (pesan teks dan gambar yang telah dihapus) dari platform Discord browser menggunakan teknik *live forensic* berdasarkan metodologi NIST SP 800-86, serta mengevaluasi efektivitas berbagai tools forensik terhadap ketiga browser yang digunakan. | Penelitian ini menggunakan *live forensic* dengan pendekatan metodologi NIST SP 800-86 yang terdiri dari empat tahap utama: *Collection*, *Examination*, *Analysis*, dan *Reporting*. Eksperimen dilakukan dengan mensimulasikan kasus cybercrime (body shaming dan sexual harassment) di platform Discord yang diakses melalui tiga jenis browser (Google Chrome, Mozilla Firefox, dan Microsoft Edge). Tools forensik yang digunakan meliputi: FTK Imager, Autopsy, ChromeCacheView, dan MZCacheView. | Penelitian berhasil menemukan bukti digital berupa teks, gambar, username, dan waktu dari pesan yang telah dihapus. Autopsy dan ChromeCacheView menunjukkan akurasi terbaik (75%), diikuti FTK Imager (50%) dan MZCacheView (25%). Kombinasi tools terbukti efektif dalam mendukung pembuktian digital, terutama pada kondisi *live system* (komputer masih menyala). | Penelitian ini **sangat relevan** dengan topik kamu, yaitu analisis forensik digital terhadap penyusupan dalam Tiktok menggunakan metode NIST. Keduanya mengimplementasikan metode NIST SP 800-86 dalam skenario komunikasi daring dan kondisi *live forensic*. Temuan dari penelitian ini memberikan wawasan tentang pemanfaatan berbagai tools dan pendekatan teknis yang bisa diadaptasi untuk konteks penyusupan Tiktok, terutama dalam menangani data yang bersifat volatile serta penggunaan browser-based platform. |
| 168 | Muhammad Syahrizal Darwis, Erick Irawadi Alwi, Huzain Azis ,2023, Investigasi Aplikasi Facebook Messenger Pada Smartphone Berbasis iOS Menggunakan Metode DFRWS | Tujuannya adalah untuk menganalisis dan mengidentifikasi bukti digital berupa percakapan teks dan gambar dari aplikasi Facebook Messenger di smartphone berbasis iOS, lalu mendokumentasikannya untuk kepentingan persidangan. | Penelitian ini menggunakan metode Digital Forensic Research Workshop (DFRWS) untuk melakukan investigasi forensik digital terhadap aplikasi Facebook Messenger pada smartphone berbasis iOS. Tahapannya meliputi *Identification, Preservation, Collection, Examination, Analysis,* dan *Presentation*. Tools yang digunakan antara lain MOBILedit Forensic Express dan FTK Imager | Penelitian berhasil menemukan bukti digital berupa teks percakapan dan gambar dari aplikasi Facebook Messenger, namun hanya data yang belum dihapus yang berhasil diperoleh. Tools MOBILedit Forensic Express mampu membuat backup data dan mengekstraksi bukti, sedangkan analisis dilakukan lebih lanjut dengan FTK Imager. Penelitian juga menekankan pentingnya metode DFRWS dalam menjaga keaslian dan keutuhan bukti. | Penelitian ini kurang relevan secara langsung dengan topik kamu tentang analisis forensik penyusupan Tiktok menggunakan metode NIST. Perbedaan utamanya ada pada metode yang digunakan (DFRWS vs NIST SP 800-86) serta konteks aplikasi yang dianalisis (Facebook Messenger berbasis mobile vs Tiktok berbasis desktop/meeting platform). Namun, tetap ada manfaat dari sisi pendekatan umum investigasi mobile forensics dan teknik pengamanan bukti yang bisa jadi referensi tambahan. |
| 169 | Muhammad Rizki Setyawan , 2023, Perbandingan Tools Forensik Dalam Analisis Bukti Digital Pada Aplikasi Skype Menggunakan Framework NIST | Untuk mengevaluasi efektivitas tiga tools forensik dalam menemukan bukti digital berupa akun, percakapan, gambar, video, dan kontak pada aplikasi Skype yang digunakan dalam simulasi kasus perdagangan narkoba berbentuk vape dan liquid vape. | Penelitian ini menggunakan framework NIST (National Institute of Standards and Technology) yang terdiri dari empat tahapan: *Collection, Examination, Analysis,* dan *Reporting*. Penelitian dilakukan dengan membandingkan performa tiga tools forensik: Oxygen Forensic Suite, Belkasoft Evidence Center, dan MOBILedit Forensic Express dalam mengidentifikasi bukti digital pada aplikasi Skype berbasis Android. | Semua tools berhasil menemukan bukti digital dengan hasil paling tinggi ditunjukkan oleh Oxygen Forensic Suite (98%), diikuti Belkasoft Evidence Center (88%), dan MOBILedit Forensic Express (84%). Tools digunakan untuk memulihkan bukti digital dari backup image perangkat yang telah di-*root*, dan proses analisis membuktikan bahwa framework NIST mampu memandu tahapan forensik secara sistematis. | Penelitian ini relevan dengan topik kamu karena menggunakan framework NIST dalam konteks analisis bukti digital dari platform komunikasi, meskipun platform yang dianalisis adalah Skype dan bukan Tiktok. Penekanan pada perbandingan tools juga dapat menjadi insight tambahan untuk menentukan tools terbaik yang bisa dipakai dalam forensik terhadap penyusupan Tiktok, terutama jika aktivitasnya melibatkan komunikasi atau pertukaran file. |
| 170 | Mulia Fitriana, Khairan AR, Jiwa Malem Marsya , 2020, PENERAPANA METODE NATIONAL INSTITUTE OF STANDARS AND TECHNOLOGY (NIST) DALAM ANALISIS FORENSIK DIGITAL UNTUK PENANGANAN CYBER CRIME | Menemukan kembali bukti digital yang telah dihapus dari aplikasi WhatsApp pada perangkat Android, dalam konteks simulasi kasus cyber pornography, serta menyusun prosedur forensik digital yang sesuai dengan metode NIST untuk keperluan penyidikan. | Penelitian ini menggunakan metode NIST dengan empat tahapan utama: *Collection, Examination, Analysis*, dan *Reporting*. Peneliti menjalankan skenario kasus kejahatan pornografi melalui WhatsApp, kemudian menghapus data untuk disimulasikan sebagai barang bukti yang hilang. Tools yang digunakan antara lain WhatsApp Viewer, AccessData FTK Imager, DB Browser for SQLite, serta proses rooting dengan KingRoot dan CWM Recovery. | Penelitian berhasil mendapatkan kembali bukti digital berupa percakapan WhatsApp yang dihapus, kontak, tanggal dan waktu, serta profil pengguna. Prosedur NIST terbukti membantu menyusun langkah investigasi yang sistematis. Selain aspek teknis, penelitian ini juga melibatkan validasi hukum dari aparat kepolisian dan ahli hukum untuk memastikan kesesuaian prosedur dan pasal yang dikenakan terhadap simulasi kasus. | Penelitian ini **sangat relevan** karena menggunakan metode NIST untuk menganalisis kasus forensik digital berbasis komunikasi daring, dalam hal ini WhatsApp. Walau berbeda platform (WhatsApp vs Tiktok), pendekatan yang digunakan dalam hal *data recovery, digital evidence handling,* dan penggunaan tools forensik dapat diadaptasi untuk kasus penyusupan Tiktok. Penelitian ini juga memberikan contoh nyata bagaimana metode NIST diterapkan dari awal hingga pelaporan, yang bisa jadi acuan kuat dalam struktur riset kamu. |
| 171 | Nabilla Fatmah, Rini Indrayani , 2022, Analisis Forensik Digital pada Solid State Drive Fungsi TRIM Menggunakan Tools Autopsy dan OSForensics | Untuk menganalisis dan membandingkan efektivitas dua tools forensik dalam melakukan recovery data dari SSD NVMe M.2 dengan kondisi TRIM enable dan disable. Penelitian juga bertujuan menilai pengaruh fitur TRIM terhadap keberhasilan pemulihan bukti digital. | Penelitian ini menggunakan metode static forensic dan standar SNI Acquisition 27037:2014 sebagai panduan akuisisi data digital pada perangkat mati (SSD NVMe). Tools yang digunakan untuk proses akuisisi dan recovery adalah Autopsy dan OSForensics. Eksperimen dilakukan dengan skenario penghapusan data pada SSD fungsi TRIM enable dan disable, lalu dilakukan pemulihan data untuk mengevaluasi efektivitas tools tersebut. | Tools Autopsy dan OSForensics sama-sama tidak mampu memulihkan data dari SSD dengan fungsi TRIM aktif (0% recovery), namun berhasil 100% ketika TRIM dinonaktifkan. Dari sisi durasi, OSForensics lebih efisien (228–231 menit) dibanding Autopsy (323–334 menit) dalam proses akuisisi. Kedua tools menunjukkan hasil identik dalam validasi hash, menunjukkan integritas data selama proses berlangsung. | Penelitian ini cukup relevan secara teknis, meskipun konteksnya bukan aplikasi komunikasi seperti Tiktok. Fokus utama pada pemulihan bukti digital dari perangkat penyimpanan dengan fitur TRIM dapat memberi pemahaman penting mengenai keterbatasan forensik pada perangkat modern, yang juga bisa terjadi pada perangkat yang digunakan dalam penyusupan Tiktok. |
| 172 | Nur Halimah, Fahmi Fachri , 2024, ANALISIS BUKTI DIGITAL TWITTER WEB MENGGUNAKAN LIVE FORENSIC PADA KASUS CYBERBULLYING | Menganalisis bukti digital berupa percakapan cyberbullying di Twitter Web yang telah dihapus oleh pelaku, serta membuktikan efektivitas metode live forensic berbasis NIST dalam mengungkap kejahatan siber dengan cepat dan akurat. | Penelitian ini menggunakan metode live forensic dengan pendekatan NIST SP 800-86 yang mencakup empat tahapan: *Collection, Examination, Analysis,* dan *Reporting*. Tools utama yang digunakan adalah FTK Imager dan HxD Editor. Data diambil dari RAM laptop pelaku saat masih dalam kondisi hidup (active state), memungkinkan penyidik mengakses data volatile (seperti isi chat yang telah dihapus di Twitter web). | Penelitian berhasil memulihkan 100% bukti digital berupa percakapan teks antara pelaku dan korban, meskipun data sudah dihapus dari browser. Tools FTK Imager dan HxD Editor mampu mengidentifikasi pesan kasar, ujaran kebencian, serta akun Twitter pelaku. Hasil ini menunjukkan bahwa pendekatan live forensic sangat efektif untuk menangani kasus kejahatan yang melibatkan platform media sosial berbasis web. | Penelitian ini sangat relevan dengan topik kamu. Selain sama-sama menggunakan metode NIST SP 800-86, pendekatan live forensic terhadap aplikasi komunikasi (dalam hal ini Twitter Web) mencerminkan praktik serupa dengan kasus penyusupan dalam Tiktok. Teknik *memory capture*, analisis data volatile, serta penggunaan FTK Imager dapat dijadikan referensi teknis yang langsung bisa diadaptasi dalam riset kamu. |
| 173 | Nur Rochmah Dyah Puji Astuti, Fiftin Noviyanto, Dewi Soyusiawati , 2018, Forensik Digital Metode RegEx (Regular Expression) dari Grab Google Search Api dalam Proses Pelacakan Terhadap Kejahatan Online | Membangun sistem pelacakan otomatis terhadap situs penipuan online dengan menggabungkan metode RegEx dan Google Search API untuk memudahkan aparat penegak hukum (khususnya POLDA DIY) dalam mengidentifikasi jejak digital penipu secara cepat dan akurat. | Penelitian ini menggunakan pendekatan forensik digital berbasis pencocokan pola teks (RegEx) dari hasil grab Google Search API. Metode ini memungkinkan pelacakan situs dan blog penipuan secara otomatis dari data laporan masyarakat. Prosesnya mencakup: input laporan penipuan (misal: URL, email, atau nomor telepon), ekstraksi data menggunakan RegEx, lalu pengambilan data (grabbing) melalui Google Search API untuk pelacakan situs terkait. | Penggunaan metode RegEx dari Grab Google Search API terbukti mempercepat proses pelacakan situs penipuan dibanding metode manual. Sistem ini dapat menampilkan daftar situs berdasarkan keyword dari laporan (seperti nomor HP atau URL penipuan), membantu proses penyelidikan, dan memudahkan masyarakat mengenali situs palsu. | Penelitian ini kurang relevan secara langsung dengan topik kamu yang fokus menggunakan metode NIST. Perbedaan mendasar terletak pada pendekatan (RegEx dan web crawling vs. digital forensic framework NIST SP 800-86), jenis kasus (penipuan website vs penyusupan daring), dan jenis bukti (pola data publik vs artefak digital volatile). Namun, secara konsep, pendekatan identifikasi jejak digital dari data laporan masyarakat tetap dapat menginspirasi tahap awal investigasi atau *information gathering* dalam kasus |
| 174 | Rahmat Novrianda Dasmen, Ferry Kurniawan , 2021, Digital Forensik Deleted Cyber Crime Evidence pada Pesan Instan Media SosialDigital Forensik Deleted Cyber Crime Evidence pada Pesan Instan Media Sosial | Untuk membuktikan bahwa bukti digital berupa pesan, gambar, dan video dari media sosial yang telah dihapus (deleted evidence) masih bisa dipulihkan dan dianalisis menggunakan teknik digital forensik, khususnya pada kasus cyberbullying di media sosial. | Penelitian ini menggunakan Metode Action Research yang terdiri dari lima tahapan: *Diagnosing, Action Planning, Action Taking, Evaluating*, dan *Learning*. Proses investigasi difokuskan pada pesan instan yang telah dihapus dari Facebook Messenger dan WhatsApp. Tools yang digunakan dalam proses forensik adalah DumpIt untuk melakukan *memory dump* (RAM) dari perangkat smartphone, serta WinHex untuk analisis data hexadesimal guna menemukan kembali data pesan yang dihapus. | Pesan teks, gambar, dan video dari Facebook Messenger berhasil ditemukan kembali. Dari WhatsApp, hanya pesan teks dan video yang berhasil ditemukan, sedangkan gambar tidak berhasil dipulihkan — kemungkinan karena keterbatasan RAM atau proses dump yang tidak sempurna. Teknik forensik ini efektif untuk mengungkap bukti digital terhapus, selama perangkat (RAM) masih tersedia. | Penelitian ini sangat relevan dengan topik kamu karena sama-sama menyasar pemulihan bukti digital yang dihapus, serta menggunakan teknik live memory forensics, yang juga kamu perlukan dalam kasus penyusupan Tiktok meeting. Walaupun tidak menggunakan framework NIST secara eksplisit, tahapan investigasi dan teknik yang digunakan bisa dikaitkan dengan prinsip-prinsip dalam NIST SP 800-86, khususnya pada tahap *Collection* dan *Analysis*. Penggunaan DumpIt dan WinHex juga bisa dijadikan referensi alat bantu dalam proses investigasi Tiktok. |
| 175 | Ahmad Qayyum Ibnu Hidayat, Erick Irawadi Alwi, Andi Widya Mufila Gaffar. (2024). Studi Forensik Digital: Analisis Bukti Video TikTok dengan Metode DFRWS | Digital Forensic Research Workshop (DFRWS) yang terdiri dari enam tahapan:  Identification: Menentukan dan mengumpulkan barang bukti digital.  Preservation: Melindungi barang bukti dari kerusakan.  Collection: Mengumpulkan data dari bukti digital.  Examination: Memeriksa data untuk memastikan keasliannya.  Analysis: Menganalisis data untuk menentukan siapa, apa, dan bagaimana data dihasilkan.  Presentation: Menyajikan hasil analisis dalam bentuk yang dapat dipahami. | Tujuan penelitian ini adalah untuk menganalisis penyebaran konten video hoax di platform TikTok dan merekonstruksi bukti digital yang dihapus dari smartphone pelaku untuk digunakan sebagai barang bukti dalam proses hukum. | Penelitian ini berhasil menemukan bukti digital yang telah dihapus, termasuk video konten, pesan langsung, dan komentar, menggunakan alat forensik seperti Wondershare dr.fone dan Oxygen Forensic. Hasilnya menegaskan pentingnya bukti digital dalam penegakan hukum terkait penyebaran hoax melalui media sosial. | Kedua penelitian memiliki hubungan yang erat dalam konteks analisis forensik digital terkait penyebaran informasi palsu di TikTok. Pertama, keduanya fokus pada platform yang sama, yaitu TikTok, sebagai media penyebaran hoax. Selain itu, meskipun menggunakan metodologi yang berbeda. penelitian pertama menggunakan DFRWS dan artikel Anda menggunakan NIJ. keduanya bertujuan untuk mengidentifikasi dan menganalisis bukti digital yang berkaitan dengan tindakan penyebaran informasi palsu. |
| 176 | Muhammad Ali Diko Putra, Arif Wirawan Muhammad, Bita Parga Zen, Rianti Yunita Kisworini, Tuti Rohayati. (2024). Analisis Forensik Pada Instagram dan Tik Tok Dalam Mendapatkan Bukti Digital Dengan Menggunakan Metode NIST 800-86 | Metode yang digunakan dalam penelitian ini adalah National Institute of Standards and Technology (NIST) 800-86. Metode ini meliputi empat tahapan: Collection, Examination, Analysis, dan Reporting. Penelitian ini menggunakan alat forensik seperti MOBILedit Forensic Express, Autopsy, dan FTK Imager untuk mengumpulkan dan menganalisis bukti digital dari aplikasi Instagram dan TikTok. | Tujuan penelitian adalah untuk menentukan proses menemukan bukti digital pada aplikasi Instagram dan TikTok yang diakses melalui smartphone, menggunakan metode NIST. Penelitian ini bertujuan untuk mengidentifikasi dan membandingkan kinerja berbagai alat forensik dalam memperoleh bukti digital. | Penelitian menunjukkan bahwa alat FTK Imager lebih unggul dalam akuisisi bukti digital dibandingkan dengan MOBILedit Forensic Express dan Autopsy. Pada aplikasi Instagram, FTK Imager berhasil mendapatkan 57% dari total data awal, sementara di TikTok, alat ini berhasil mendapatkan 71%. | Penelitian ini relevan dengan topik saya karena Kedua studi berfokus pada aplikasi TikTok sebagai platform yang dapat menjadi sarana peredaran informasi, termasuk informasi palsu atau hoaks. Metode yang digunakan dalam kedua penelitian, meskipun berbeda (NIST dan NIJ), sama-sama bertujuan untuk mengidentifikasi dan memperoleh bukti digital yang relevan dari aktivitas pengguna di TikTok. |
| 177 | Aditya Primukti, Putri Kartika Sari, Didit Suhartono, Khairunnisak Nur Isnaini. (2025). Analisis Memori Forensik Pada Aplikasi Tiktok Berbasis Web Menggunakan Metode National Institute Of Justice (NIJ) | Penelitian ini menggunakan Metode National Institute of Justice (NIJ), yang mencakup tahapan:  Identifikasi: Menentukan perangkat yang digunakan untuk mengakses TikTok.  Pengumpulan: Menggunakan FTK Imager untuk mengambil snapshot memori (RAM) dari perangkat.  Pemeriksaan: Menganalisis data menggunakan HxD untuk menemukan pola dan artefak terkait.  Analisis: Mengkategorikan data berdasarkan relevansi terhadap tujuan penelitian.  Pelaporan: Menyusun laporan hasil penelitian. | Tujuan penelitian ini adalah untuk:  Menganalisis memori forensik pada aplikasi TikTok berbasis web.  Mengidentifikasi informasi penting yang tersimpan dalam memori aplikasi selama sesi penggunaan. | Penelitian ini menyimpulkan bahwa:  Analisis berhasil mengidentifikasi sejumlah informasi penting seperti nomor telepon yang digunakan untuk login, riwayat pencarian pengguna, dan nama pengguna (username) aktif. Data sensitif seperti kode OTP tidak ditemukan, menunjukkan langkah-langkah keamanan yang diterapkan oleh TikTok. Pengguna disarankan untuk menggunakan browser yang aman dan terkini, serta pengembang aplikasi perlu memperkuat keamanan data untuk mencegah penyimpanan informasi sensitif. | Penelitian ini relevan dengan topik saya karena penggunaan Metode National Institute of Justice (NIJ) yang sama, memberikan kerangka kerja sistematis untuk analisis forensik digital. Kedua penelitian berfokus pada platform TikTok, yang banyak digunakan, dengan yang pertama menganalisis memori forensik untuk mendapatkan data pengguna dan yang kedua mengungkap peredaran informasi palsu. Keduanya bertujuan untuk meningkatkan keamanan dan keabsahan data, serta memberikan rekomendasi bagi pengguna dan pengembang aplikasi. |
| 178 | Fauzan Natsir. (2021). Analisis Forensik Konten dan Timestamp pada Aplikasi TikTok | Penelitian ini menggunakan metodologi Open-Source Intelligence (OSINT) dan pendekatan National Institute of Standards Technology (NIST). Metode ini melibatkan pengumpulan, analisis, dan pelaporan data yang dapat diakses dari aplikasi TikTok menggunakan berbagai tools forensik seperti Browser History Capture/Viewer, Video Cache Viewer, Unfurl, dan Urlebird. | Tujuan dari penelitian ini adalah untuk mengungkap dan menganalisis timestamp yang diperoleh dari konten TikTok, serta merekonstruksi konten dan mencari kata kunci dari timestamp tersebut. Penelitian ini juga bertujuan untuk menyoroti potensi masalah privasi dan risiko yang dihadapi pengguna TikTok. | Kesimpulan dari penelitian ini menunjukkan bahwa aplikasi TikTok merupakan sumber data yang potensial untuk forensik digital. Proses analisis yang dilakukan dapat membantu dalam menemukan timestamp dan mengidentifikasi informasi penting dari pengguna. Hasil penelitian diharapkan dapat memberikan rekomendasi untuk meningkatkan kebijakan dan prosedur penggunaan aplikasi TikTok. | Penelitian ini relevan dengan topik saya karena keduanya berfokus pada TikTok sebagai platform media sosial yang relevan untuk analisis forensik. Metodologi yang digunakan berbeda. NIST dalam penelitian pertama dan NIJ dalam artikel Anda. namun keduanya bertujuan untuk menyediakan kerangka kerja sistematis dalam analisis data digital. Pengumpulan data dari TikTok menjadi fokus utama, dengan penelitian pertama menganalisis timestamp dan konten, sementara artikel Anda meneliti informasi palsu. |
| 179 | Herman, Anton Yudhana, Fitri Anggraini. (2023). Akuisisi Bukti Digital Tiktok Berbasis Androidmenggunakan Metode National Institute Of Justice | Penelitian ini menggunakan framework National Institute of Justice (NIJ) yang terdiri dari lima tahap:  Identification: Persiapan alat dan bahan untuk penyidikan.  Collection: Pengumpulan bukti fisik dan data.  Examination: Pengujian dan pengambilan barang bukti elektronik.  Analysis: Proses analisis data untuk menentukan signifikansi dan probabilitas.  Reporting: Pembuatan laporan hasil pemeriksaan. | Tujuan penelitian ini adalah untuk melakukan proses forensik untuk mendapatkan bukti-bukti terkait pencemaran nama baik dan ancaman di media sosial TikTok. | Penelitian menunjukkan bahwa metode forensik menggunakan NIJ dan alat MOBILedit Forensic Express efektif untuk ekstraksi bukti digital dari aplikasi TikTok. Hasil menunjukkan bahwa tingkat keberhasilan dalam mengangkat bukti digital dari smartphone yang sudah di-root adalah 85,7%, sedangkan dari smartphone yang belum di-root adalah 42,8%. Penelitian ini merekomendasikan penggunaan smartphone yang sudah di-root untuk akuisisi bukti digital yang lebih komprehensif. | Penelitian ini relevan dengan topik saya karena kedua penelitian menggunakan metode NIJ sebagai kerangka analisis, yang memungkinkan perbandingan hasil dan teknik. Kedua, fokus pada platform TikTok sebagai media sosial yang berpotensi menjadi sarana penyebaran informasi palsu atau pencemaran nama baik menunjukkan relevansi yang kuat. Selanjutnya, keduanya menekankan pentingnya pengumpulan dan analisis bukti digital untuk mengidentifikasi kejahatan, serta menggarisbawahi isu cybercrime yang muncul dari aktivitas di media sosial. |
| 180 | Halimah Septya Mikayla, Ari Kusyanti, Primantara Hari Trisnawan. (2024). Analisis Forensik Digital Untuk Investigasi Kasus Cyberbullying Pada Media Sosial Tiktok | Penelitian ini menggunakan metode eksperimen dengan skenario kasus cyberbullying yang dirancang untuk mengumpulkan dan menganalisis bukti digital. Proses investigasi forensik digital mengikuti tahapan seperti perencanaan, pengumpulan, transportasi, pemeriksaan, identifikasi, analisis, klasifikasi, pelaporan, dan presentasi. | Tujuan dari penelitian ini adalah untuk mengumpulkan dan menganalisis bukti digital terkait kasus cyberbullying di platform TikTok, baik pada aplikasi Android maupun situs web, serta memberikan pemahaman yang lebih baik untuk akademisi, praktisi forensik digital, dan pihak berwenang. | Penelitian ini berhasil mendapatkan berbagai jenis bukti digital yang dapat digunakan untuk membuktikan kasus cyberbullying, dengan hasil yang menunjukkan perbedaan signifikan antara bukti yang ditemukan di TikTok Android dan TikTok web. Bukti digital yang diperoleh memiliki persentase keberhasilan 68%, dan penelitian ini menyimpulkan bahwa aplikasi TikTok Android lebih signifikan untuk penyelidikan kasus dibandingkan TikTok web. | Penelitian ini relevan dengan topik saya karena keduanya fokus pada platform TikTok, yang menghadapi masalah serius terkait penyalahgunaan, baik dalam konteks cyberbullying maupun penyebaran informasi palsu. Metode investigasi forensik yang digunakan dalam kedua penelitian bertujuan untuk mengidentifikasi dan menganalisis bukti digital untuk membuktikan tindakan ilegal. Selain itu, keduanya mengedepankan pentingnya tahapan pengumpulan dan analisis bukti digital yang sistematis. |
| 181 | Faul Isnaeni, Fahmi Fachri. (2025). Analisis Forensik Smarphone Android Pada Aplikasi Tiktok Menggunakan Metode NIST | Penelitian ini menggunakan metode National Institute of Standards and Technology (NIST) yang terdiri dari empat tahap:  Collection (Pengumpulan): Mengumpulkan dan mendokumentasikan barang bukti.  Examination (Pemeriksaan): Melakukan backup dan imaging data.  Analysis (Analisis): Menganalisis data yang telah diperoleh untuk menemukan bukti digital.  Reporting (Pelaporan): Menyusun laporan mengenai hasil analisis. | Tujuan penelitian ini adalah untuk menginvestigasi pencemaran nama baik di TikTok dengan memulihkan video, hashtag, dan pesan teks yang telah dihapus dari perangkat smartphone Android, menggunakan tools Mobiledit dan FTK Imager. | Penelitian berhasil mendapatkan bukti digital berupa kontak, video, info akun, dan gambar dari tools Mobiledit, sedangkan FTK Imager hanya menemukan bukti berupa teks. Hasil analisis menunjukkan bahwa Mobiledit memperoleh 25,5% dari total data yang dicari, sementara FTK Imager memperoleh 74,4%. Penelitian merekomendasikan penggunaan tools lain untuk memperluas cakupan analisis. | Penelitian ini relevan dengan topik saya karena Keduanya berfokus pada platform TikTok yang sama, relevan dalam konteks kejahatan digital. Meskipun menggunakan metodologi yang berbeda (NIST vs. NIJ), keduanya bertujuan memberikan pendekatan sistematis dalam pengumpulan dan analisis bukti digital. Penelitian tentang pencemaran nama baik di TikTok menekankan pemulihan data yang dihapus, sedangkan penelitian Anda berfokus pada penyebaran informasi palsu, yang juga memerlukan bukti valid untuk investigasi. |
| 182 | I Putu Ari Putra Maulana dan Ida Bagus Gede Dharma Putra. (2024). Tindak Kekerasan Seksual Verbal Di Ruang Siber: Analisis Linguistik Forensik Dalam Kolom Komentar Akun Tiktok Kinderflix | Penelitian ini menggunakan pendekatan deskriptif kualitatif dan kuantitatif. Teknik pengumpulan data dilakukan dengan metode simak menggunakan teknik random sampling bersyarat. Data yang dianalisis mencakup komentar-komentar yang mengandung kekerasan seksual verbal. | Menganalisis pola bahasa yang digunakan dalam kekerasan seksual verbal di kolom komentar akun TikTok Kinderflix. Mengkaji hubungan antara tindak kekerasan seksual verbal dengan Undang-Undang ITE dan TPKS. | Penelitian menemukan bahwa frasa merupakan unit bahasa yang paling banyak digunakan dalam kekerasan seksual verbal (52%).  Tindak tutur ilokusi yang dominan adalah asertif (52%). Ujaran kekerasan seksual verbal dalam komentar TikTok Kinderflix melanggar dua undang-undang terkait dan menunjukkan dampak negatif terhadap korban. | Penelitian ini relevan dengan topik saya karena kedua penelitian berfokus pada TikTok sebagai platform media sosial yang menjadi ruang interaksi publik, di mana berbagai perilaku, baik positif maupun negatif, terjadi. Selain itu, keduanya menggunakan pendekatan analisis forensik—penelitian pertama menggunakan analisis linguistik forensik, sementara artikel Anda menerapkan metodologi forensik digital. |
| 183 | Imam Riadi, Sunardi, Takdir Ruslan. (2023).  Analisis Forensik Digital Pada Whatsapp Dan Facebook Menggunakan Metode NIST | Penelitian ini menggunakan metode static forensics berdasarkan kerangka kerja yang dikembangkan oleh National Institute of Standards and Technology (NIST). Metode ini meliputi empat tahap: preservation (pemeliharaan), acquisition (akuisisi), examination (pengujian), dan reporting (pelaporan). | Tujuan dari penelitian ini adalah untuk:  Mengangkat dan menganalisis bukti digital dari aplikasi WhatsApp dan Facebook Messenger.  Mengukur kinerja alat forensik dalam mengembalikan data multimedia (audio dan video) yang telah dihapus pada perangkat smartphone berbasis Android. | Penelitian ini menyimpulkan bahwa:  Beberapa alat forensik, terutama Belkasoft dan Magnet Axiom, berhasil mengembalikan sebagian besar data audio dan video yang dihapus. Alat forensik MOBILedit tidak dapat mengembalikan data apapun. Data yang berhasil dipulihkan dapat digunakan sebagai bukti digital dalam kasus kejahatan terkait aplikasi pesan instan. | Penelitian ini relevan dengan topik saya karena kedua penelitian menggunakan metodologi forensik untuk mengungkap bukti digital, meskipun dengan kerangka kerja yang berbeda (NIST dan NIJ). Berfokus pada aplikasi digital yang berbeda, WhatsApp dan Facebook Messenger dibandingkan dengan TikTok, menunjukkan tantangan serupa dalam pengumpulan dan pemulihan data. |
| 184 | Rachmad Nur Fauzi, Nuril Anwar. (2023). Multimedia Forensic Analysis of TikTok Application Using National Institute of Justice (NIJ) Method | Jurnal ini menggunakan analisis forensik mobile dengan metode Error Level Analysis (ELA). Penelitian mengikuti metodologi National Institute of Justice (NIJ) yang mencakup sepuluh tahap penyelidikan forensik, termasuk pembuatan skenario, identifikasi, pengumpulan, penyelidikan, dan analisis. Penelitian ini juga memanfaatkan alat seperti MOBILedit Forensic Express Pro, FotoForensics, dan Forensically untuk mengumpulkan dan memverifikasi bukti digital. | Tujuan utama penelitian ini adalah untuk mengumpulkan bukti digital dari aplikasi TikTok yang terinstal pada perangkat mobile dan memverifikasi keaslian gambar menggunakan metode Error Level Analysis (ELA). Penelitian ini bertujuan untuk mengidentifikasi dan mengungkap kejahatan digital yang terjadi di platform TikTok, terutama terkait dengan penyebaran informasi yang salah. | Penelitian ini menyimpulkan bahwa analisis keaslian gambar sangat penting dalam konteks forensik digital. Bukti yang diperoleh menunjukkan bahwa gambar yang diekstrak dari aplikasi TikTok telah mengalami manipulasi yang dapat mempengaruhi keaslian dan integritasnya. Metode Error Level Analysis (ELA) terbukti efektif dalam mendeteksi kemungkinan manipulasi gambar, dan penerapan metodologi NIJ memberikan kerangka kerja yang kuat untuk investigasi forensik. | Penelitian ini relevan dengan topik saya karena kedua penelitian fokus pada TikTok sebagai platform yang sering digunakan untuk menyebarkan informasi palsu. Keduanya juga menggunakan metodologi National Institute of Justice (NIJ) dalam pendekatan forensik digital, menunjukkan kesamaan dalam kerangka kerja penyelidikan. Selain itu, teknik forensik digital, seperti Error Level Analysis (ELA), dapat digunakan dalam artikel Anda untuk menganalisis bukti manipulasi informasi. |
| 185 | Imam Riadi, Rusydi Umar, Imam Mahfudl Nasrulloh. (2018). Analisis Forensik Digital Pada Frozen Solid State Drive Dengan Metode National Institute Of Justice (NIJ) | Penelitian ini menggunakan metode analisis forensik yang diadaptasi dari National Institute of Justice (NIJ), yang mencakup lima tahap:  Identifikasi: Pemilahan barang bukti digital.  Pengumpulan: Mengumpulkan data untuk mendukung penyidikan.  Pemeriksaan: Memastikan data yang dikumpulkan adalah asli. Analisis: Meneliti data secara detail.  Pelaporan: Menyusun laporan hasil analisis. | Tujuan dari penelitian ini adalah untuk menganalisis pengaruh penggunaan software pembeku drive (seperti Shadow Defender) terhadap proses eksaminasi dan analisis forensik digital pada Solid State Drive (SSD) yang dibekukan. | Penelitian menunjukkan bahwa penggunaan software pembeku drive menghambat proses forensik digital, dengan tingkat keberhasilan restorasi file hanya mencapai 28,7%. Hal ini menjadi hambatan dalam memperoleh bukti digital yang valid dari SSD yang dibekukan. | Penelitian ini relevan dengan topik saya karena keduanya menggunakan metodologi dari NIJ, yang menekankan pendekatan sistematis dalam pengumpulan dan analisis bukti digital. Fokus utama pada kedua penelitian adalah pada pengumpulan bukti digital terkait kejahatan; satu berfokus pada kejahatan berbasis perangkat keras, sementara yang lainnya menyentuh aspek informasi palsu di platform media sosial. |
| 186 | Imam Riadi, Sunardi, Sahiruddin. (2019). Analisis Forensik Recovery Pada Smartphone Android Menggunakan Metode National Institute Of Justice (NIJ) | Penelitian ini menggunakan metode yang dikembangkan oleh National Institute of Justice (NIJ), yang terdiri dari langkah-langkah sebagai berikut: Identifikasi: Mengidentifikasi masalah dan mengumpulkan informasi. Solusi: Mengajukan solusi untuk pemecahan masalah. Uji Coba: Melakukan uji coba terhadap smartphone menggunakan solusi yang diajukan.  Evaluasi: Mengevaluasi hasil uji coba.  Laporan: Menyusun laporan hasil penelitian. | Tujuan penelitian ini adalah untuk menganalisis dan mengembalikan data yang telah dihapus pada smartphone Android melalui metode forensik untuk mendapatkan bukti digital dalam kasus kejahatan. | Data yang telah dihapus pada perangkat smartphone Android dapat dikembalikan menggunakan tool Wondershare dan Belkasoft. Tool forensik yang digunakan tidak efektif untuk mengembalikan data gambar, video, dan file dokumen. Wondershare dan Belkasoft berhasil mengembalikan data kontak, log panggilan, dan pesan, sedangkan MOBILedit hanya dapat menampilkan data yang belum dihapus. | Penelitian ini relevan dengan topik saya karena penggunaan metodologi yang sama, yaitu NIJ, yang mencakup langkah-langkah sistematis untuk mengidentifikasi dan menyelesaikan masalah forensik digital. Keduanya fokus pada pentingnya bukti digital dalam konteks kejahatan, dengan penelitian pertama menyoroti pemulihan data dari smartphone dan artikel Anda menganalisis penyebaran informasi palsu di TikTok. |
| 187 | Desti Mualfah dan Rizdqi Akbar Ramadhan. (2021). Analisis Digital Forensik Rekamankamera CCTV Menggunakan Metode NIST (National Institute Of Standards Technology) | Penelitian ini menggunakan metode akuisisi berdasarkan pedoman dan standar dalam SNI 27037:2014 dan menerapkan metode NIST (National Institute of Standards Technology) untuk menganalisis metadata rekaman kamera CCTV. Tahapan penelitian meliputi pengumpulan data (collection), pemeriksaan (examination), analisis (analysis), dan pelaporan (reporting). | Tujuan dari penelitian ini adalah untuk memperoleh dan menganalisis bukti digital dari rekaman kamera CCTV agar informasi metadata dapat diolah dan diterapkan dalam dokumen Chain of Custody, sehingga integritas bukti digital terjaga dan dapat diterima dalam proses hukum. | Penelitian ini berhasil menunjukkan bahwa dengan menggunakan metode NIST, informasi metadata dari rekaman CCTV dapat diolah menjadi alat bukti yang sah dan dapat dipertanggungjawabkan di pengadilan. Proses dokumentasi yang baik dalam Chain of Custody memastikan bahwa bukti digital tidak dimanipulasi dan tetap valid sepanjang proses investigasi. | Penelitian ini relevan dengan topik saya karena keduanya menggunakan metodologi forensik untuk menganalisis bukti digital, meskipun dengan pendekatan yang berbeda (NIST dan NIJ). Fokus pada pengumpulan dan validasi bukti digital menjadi inti dari kedua penelitian, dengan CCTV memanfaatkan rekaman video dan TikTok mengandalkan konten digital. |
| 188 | Steven Marcellino, Henki Bayu Seta, Wayan Widi. (2023). Analisis Forensik Digital Recovery Data Smartphone Pada Kasus Penghapusan Berkas Menggunakan Metode National Institute Of Justice (NIJ) | Penelitian ini menggunakan Metode National Institute of Justice (NIJ), yang terdiri dari lima tahapan: Identification: Proses identifikasi masalah dan bukti. Collection: Pengumpulan data digital dan bukti fisik.  Examination: Pemeriksaan barang bukti secara manual atau otomatis.  Analysis: Analisis mendalam terhadap data yang diperoleh.  Reporting: Penyusunan laporan hasil analisis. | Tujuan penelitian ini adalah untuk menggunakan metode NIJ dalam proses investigasi digital forensik pada smartphone Android, serta untuk membandingkan efektivitas dua alat recovery data, yaitu Wondershare Dr Fone dan EaseUS Data Recovery, dalam mengembalikan data yang dihapus. | Hasil Recovery: EaseUS Data Recovery lebih efektif dibandingkan Wondershare Dr Fone, dengan tingkat keberhasilan 100% dalam mengembalikan data, sementara Wondershare Dr Fone hanya 63%.  Pentingnya Bukti Digital: Bukti digital sangat penting dalam mengungkap kasus kejahatan, karena setiap tindakan kejahatan meninggalkan jejak digital yang dapat diperiksa melalui forensic digital. | Penelitian ini relevan dengan topik saya karena Kedua penelitian menggunakan Metode National Institute of Justice (NIJ), yang memberikan kerangka kerja sistematis untuk analisis forensik digital. Keduanya menekankan pentingnya bukti digital; yang pertama berfokus pada pemulihan data dari smartphone yang dihapus, sedangkan penelitian Anda meneliti penyebaran informasi palsu di TikTok. |
| 189 | Imam Riadi, Sunardi, Takdir Ruslan. (2023). Analisis Forensik Digital Pada Whatsapp Dan Facebook Menggunakan Metode NIST | Penelitian ini menggunakan metode static forensics dengan kerangka kerja yang dikembangkan oleh National Institute of Standards and Technology (NIST). Metode ini meliputi tahapan: Preservation: Mengamankan dan menjaga data agar tidak berubah. Acquisition: Mengumpulkan bukti digital dari perangkat.  Examination: Mengidentifikasi dan menguji bukti digital.  Reporting: Membuat laporan dari hasil analisis. | Tujuan dari penelitian ini adalah untuk:  Mengangkat barang bukti digital.  Menilai kinerja alat forensik dalam mengembalikan data multimedia yang telah dihapus (audio dan video) pada aplikasi WhatsApp dan Facebook Messenger di perangkat smartphone berbasis Android. | Hasil penelitian menunjukkan bahwa:  Alat forensik Belkasoft dan Magnet Axiom berhasil mengembalikan sebagian besar data yang telah dihapus dari aplikasi WhatsApp, sedangkan untuk Facebook Messenger hasilnya lebih rendah.  MOBILedit tidak berhasil mengembalikan data apa pun. Data yang berhasil dikembalikan dapat digunakan sebagai bukti digital dalam penanganan kejahatan digital. | Penelitian ini relevan dengan topik saya karena berada dalam bidang forensik digital yang bertujuan untuk mengangkat dan menganalisis bukti digital. Meskipun menggunakan metodologi yang berbeda (NIST dan NIJ), keduanya memiliki fokus yang sama dalam mengidentifikasi bukti yang relevan untuk mengungkap kejahatan digital. |
| 190 | Dina Yuliana, Trihastuti Yuniati, Bita Parga Zen. (2022). Analisis Forensik Terhadap Kasus Cyberbullying Pada Instagram Dan Whatsappmenggunakan Metode National Institute Of Justice (NIJ) | Metode yang digunakan adalah National Institute of Justice (NIJ), yang mencakup tahapan: Assessment (Penilaian): Menilai bukti digital terkait kasus. Acquisition (Akuisisi): Mengamankan dan melestarikan bukti.  Examination (Pemeriksaan): Mengekstraksi dan menganalisis bukti digital.  Documenting & Reporting (Pendokumentasian & Pelaporan): Mendokumentasikan semua tindakan dan hasil analisis. | Tujuan dari penelitian ini adalah untuk menganalisis proses digital forensik dalam kasus cyberbullying yang terjadi di aplikasi Instagram dan WhatsApp, serta untuk mengevaluasi hasil dari aplikasi forensik MOBILedit, Autopsy, dan FTK Imager dalam pencarian bukti digital. | Penelitian menunjukkan bahwa metode NIJ berhasil diterapkan dalam analisis forensik kasus cyberbullying. Hasilnya, aplikasi Autopsy dan FTK Imager dapat menemukan hampir semua data sesuai skenario, sementara hasil dari aplikasi MOBILedit pada ponsel non-root sangat terbatas. Dalam kondisi root, terdapat peningkatan dalam jumlah data yang berhasil diekstrak, namun beberapa file tidak dapat diputar. | Penelitian ini relevan dengan topik saya karena pada penggunaan metode NIJ yang sama, yang mencakup tahapan sistematis dalam analisis forensik digital. Keduanya berfokus pada pencarian dan analisis bukti digital, meskipun dengan konteks yang berbeda: cyberbullying di media sosial dan penyebaran informasi palsu di TikTok. |
| 191 | Agil Nofiyan dan Mushlihudin. (2020). Analisis Forensik pada Web Phishing Menggunakan Metode National Institute Of Standards And Technology (NIST) | Penelitian ini menggunakan metode National Institute of Standards and Technology (NIST) yang terdiri dari empat tahapan: Collection (Pengumpulan), Examination (Pemeriksaan), Analysis (Analisis), dan Reporting (Pelaporan). Penelitian juga menggunakan alat seperti Wireshark untuk menangkap data dan Hashcalc untuk pemeriksaan nilai hash. | Tujuan penelitian ini adalah untuk menganalisis proses investigasi kasus cybercrime, khususnya serangan phishing, serta mengidentifikasi dan menghasilkan barang bukti digital yang relevan dari serangan tersebut. | Penelitian berhasil menghasilkan barang bukti digital melalui proses yang sistematis sesuai dengan metode NIST. Hasil analisis menunjukkan adanya tujuh paket data yang terkait dengan kejahatan phishing, termasuk identifikasi URL phishing, DNS yang digunakan, dan informasi pelaku. Penelitian ini juga menyoroti pentingnya keamanan dalam proses investigasi kejahatan siber. | Penelitian ini relevan dengan topik saya karena berfokus pada forensik digital untuk mengidentifikasi dan menganalisis bukti kejahatan siber. Meskipun metodologinya berbeda, yaitu NIST dan NIJ, tujuan utama masing-masing penelitian adalah untuk mengungkap dan mendalami bukti digital yang terkait dengan tindakan kriminal di platform digital. |
| 192 | Rahmat Novrianda Dasmen, Muhammad Reihan Pratama, Husni Yasir, Ariff Budiman. (2024). Analisis Forensik Digital Pada Kasus Cyberbullying dengan Metode National Institute of Standard and Technology SP 800-86 | Metode penelitian yang digunakan adalah National Institute of Standard and Technology (NIST) SP 800-86. Metode ini meliputi tahapan:  Collection: Pengumpulan dan pengamanan barang bukti.  Examination: Pemulihan data digital yang terhapus menggunakan alat Autopsy.  Analysis: Analisis data yang berhasil ditemukan.  Reporting: Penyusunan laporan hasil analisis. | Tujuan penelitian ini adalah untuk:  Menganalisis dan memulihkan bukti digital yang dihapus dalam kasus cyberbullying.  Menilai efektivitas alat forensik Autopsy dalam mengembalikan data sebagai bukti digital. | Penelitian menunjukkan bahwa alat Autopsy mampu melakukan pemulihan bukti digital dari flashdisk dengan tingkat keberhasilan 100%. Terdapat 4 file dengan ekstensi PNG dan 1 file MP4 yang berhasil dipulihkan, yang menjadi bukti dari kasus cyberbullying yang diteliti. | Penelitian ini relevan dengan topik saya karena kedua penelitian berfokus pada forensik digital sebagai metode untuk mengungkap kejahatan siber, meskipun topik yang diteliti berbeda: cyberbullying dan penyebaran informasi palsu. Metodologi yang digunakan berbeda—NIST SP 800-86 untuk pemulihan bukti digital dan NIJ untuk pengumpulan dan analisis bukti yang lebih luas. |
| 193 | M. Syaiful Huda Mubarok, Rahmat Novrianda Dasmen, Ardiansyah, Viren Pranata, M. Ary Januarta. (2024). Analisis Digital Forensik Data: Digital Analysis of Forensic Data Recovery on Flash Drive Using National Institute Of Justice (NIJ) Method | Penelitian ini menggunakan metode National Institute of Justice (NIJ), yang terdiri dari lima tahap:  Persiapan, Pengumpulan, Pemeriksaan, Analisis, Pelaporan | Tujuan penelitian ini adalah untuk:  Mengidentifikasi dan menganalisis efektivitas alat pemulihan data, khususnya TestDisk, dalam mengembalikan data yang hilang dari flash drive. Memberikan wawasan tentang praktik terbaik dalam pemulihan data di bidang forensik digital. | Penelitian menyimpulkan bahwa alat forensik TestDisk sangat efektif dalam memulihkan data yang hilang atau dihapus, dengan tingkat keberhasilan mencapai 100%. Penelitian ini memberikan bukti kuat dalam konteks kejahatan digital dan merekomendasikan penggunaan alat forensik secara optimal untuk mendukung proses penyelidikan. | Penelitian ini relevan dengan topik saya karena pada penggunaan metodologi yang sama, yaitu NIJ, yang menyediakan kerangka kerja sistematis dalam investigasi forensik. Keduanya berfokus pada forensik digital, dengan penelitian pertama menganalisis pemulihan data dari flash drive, sementara penelitian Anda menyelidiki informasi palsu di TikTok. |
| 194 | Saleh Khalifah Saad, Rusydi Umar, Abdul Fadlil. (2020). Analisis Forensik Aplikasi Dropbox pada Android menggunakan Metode NIJ | Penelitian ini menggunakan Metode National Institute of Justice (NIJ). Metode ini terdiri dari beberapa tahap, yaitu:  Identifikasi: Menentukan bukti digital yang relevan.  Pengumpulan: Mengumpulkan data dari sumber yang relevan. Pemeriksaan: Memeriksa bukti secara manual atau otomatis.  Analisis: Menganalisis bukti untuk menentukan signifikansi. Pelaporan: Menyusun laporan dari hasil analisis. | Tujuan penelitian ini adalah untuk menganalisis aplikasi Dropbox pada perangkat Android dalam konteks penyembunyian berkas, serta untuk menilai efektivitas metode NIJ dalam penanganan bukti digital terkait kejahatan siber. | Penelitian menyimpulkan bahwa penggunaan Metode NIJ sangat efektif dalam mengurutkan tahapan forensik digital, mulai dari identifikasi hingga pelaporan. Hasil penelitian menunjukkan bahwa alat forensik yang digunakan dapat membaca akun pengguna di Google Drive, namun hanya satu alat (Oxygen Forensics) yang mampu membuka berbagai jenis file dengan baik. | Penelitian ini relevan dengan topik saya karena kedua penelitian menggunakan Metode NIJ, yang menunjukkan konsistensi dalam pendekatan metodologis. Kedua, fokus pada kejahatan digital menjadi inti dari kedua studi, dengan penelitian pertama berkaitan dengan penyimpanan berkas di Dropbox dan penelitian Anda mengenai informasi palsu di TikTok. |
| 195 | Muhammad Abdul Aziz, Imam Riadi, Rusydi Umar. (2018). Analisis Forensik Line Messenger Berbasis Web Menggunakan Framework National Institute Of Justice (NIJ) | Penelitian ini menggunakan metode analisis forensik yang merujuk pada tahapan National Institute of Justice (NIJ). Tahapan tersebut mencakup:  Preparation: Persiapan alat dan peralatan untuk penyelidikan. Collection: Pengumpulan data dan dokumen dari objek fisik. Examination: Pemeriksaan bukti digital yang diperoleh.  Analysis: Analisis detail terhadap bukti digital. Reporting: Pelaporan hasil analisis dan rekomendasi. | Tujuan dari penelitian ini adalah untuk menjelaskan tahapan investigasi kasus cybercrime yang terjadi di LINE messenger berbasis web, serta untuk memperoleh bukti digital yang dapat diperkuat dalam proses pengadilan | Penelitian ini berhasil menemukan lokasi file log, cache, dan bukti digital dari percakapan aplikasi LINE messenger berbasis web. Bukti digital yang diperoleh melalui simulasi penyadapan tidak hilang meskipun percakapan dihapus, dan diharapkan dapat memperkuat bukti dalam proses persidangan. | Penelitian ini relevan dengan topik saya karena enelitian menggunakan metodologi yang sama, yaitu NIJ, yang mencakup tahapan sistematis dalam analisis forensik. Kedua, fokus pada cybercrime menjadi inti dari kedua studi, meskipun konteksnya berbeda: LINE Messenger untuk kejahatan di platform pesan dan Tiktok untuk informasi palsu. |
| 196 | Andi Muh Afdal, Yulita Salim, Abdul Rachman Manga. (2022). Analisis Bukti Digital Forensik pada Discord Menggunakan Metode National Institute of Standards Technology (NIST) | Penelitian ini menggunakan metode NIST (National Institute of Standards and Technology) yang terdiri dari empat tahapan: Collection: Pengumpulan dan pengambilan data digital. Examination: Identifikasi data yang dapat dijadikan bukti.  Analysis: Analisis data secara rinci.  Reporting: Pelaporan hasil investigasi dan analisis. | Tujuan dari penelitian ini adalah untuk melakukan proses investigasi dan analisis terhadap aplikasi Discord berbasis Windows, serta untuk mendapatkan bukti digital yang relevan dalam konteks penyalahgunaan aplikasi tersebut, terutama terkait dengan kasus tindak pidana terorisme. | Hasil penelitian menunjukkan bahwa hanya ditemukan bukti digital berupa gambar dengan akurasi 38,46% dan video dengan akurasi 15,38% menggunakan tool FTK Imager. Teks percakapan dan informasi lainnya tidak berhasil diambil. Penelitian ini menyarankan agar penelitian selanjutnya dilakukan menggunakan perangkat atau sistem operasi lain untuk memperoleh lebih banyak bukti digital. | Penelitian ini relevan dengan topik saya karena menggunakan pendekatan metodologi forensik untuk menganalisis bukti digital, meskipun dengan metode yang berbeda (NIST dan NIJ). Fokus analisis konten digital menjadi inti dari kedua penelitian, di mana yang pertama mengeksplorasi penyalahgunaan aplikasi Discord, sementara yang kedua meneliti penyebaran informasi palsu di TikTok. |
| 197 | Marcel Afandi, Rifki Amrulloh, Khairunnisak Nur Isnaini, Didit Suhartono. (2024). Analisis Forensik Pemalsuan Dokumen PDF Menggunakan Metode National Institute of Justice (NIJ) | Metode penelitian yang digunakan dalam studi ini adalah pendekatan National Institute of Justice (NIJ), yang mencakup langkah-langkah sistematis: Identification: Mengidentifikasi dan mengklasifikasikan bukti digital. Collection: Mengumpulkan data bukti dari sumber yang akurat. Examination: Memvalidasi data yang diperoleh. Analysis: Menganalisis bukti digital dengan menggunakan teknik seperti pemeriksaan metadata dan analisis Principal Component Analysis (PCA). Reporting: Melaporkan hasil analisis dan memberikan rekomendasi. | Tujuan penelitian ini adalah untuk:  Mempelajari tantangan dalam analisis dokumen digital, terutama terkait pemalsuan dokumen PDF. Menggunakan metode NIJ dan PCA untuk mendeteksi perubahan dan mengautentikasi keaslian dokumen PDF.  Memberikan rekomendasi untuk pengembangan teknik forensik dalam mendukung keandalan dan keamanan dokumen digital. | metode NIJ dan analisis PCA efektif dalam membuktikan keaslian dokumen PDF. Penelitian berhasil mengidentifikasi kejanggalan dalam dokumen yang diduga telah dimanipulasi. Meskipun metode ini menunjukkan hasil yang baik, penelitian juga mencatat bahwa pendekatan ini masih mengandalkan metode manual dan perangkat lunak yang kurang modern, sehingga ada kebutuhan untuk mengembangkan teknik yang lebih canggih, termasuk penggunaan kecerdasan buatan dalam analisis forensik. | Penelitian ini relevan dengan topik saya karena menggunakan metodologi NIJ, yang menawarkan kerangka kerja sistematis untuk analisis forensik. Fokus utama kedua penelitian adalah mendeteksi dan menganalisis pemalsuan, baik dalam dokumen maupun informasi yang beredar di platform digital. Selain itu, penggunaan alat dan teknik forensik dalam kedua studi memungkinkan pengujian keaslian konten, seperti metadata dan integritas data. |