BHATARA: Jurnal Multidisiplin
Vol. 3, No.2, April 2026, pp. 40-46, ISSN: 2476-9843

Analisis Bukti Digital Forensik Kasus Cyber Sexual Harassment Menggunakan Teknik Steganografi

Zepin Nossa[1], Joko Dwi Santoso[2], Hastari Utama[3]
Program Studi Teknik Komputer, Fakultas Ilmu Komputer, Universitas Amikom Yogyakarta
Jl. Ring Road Utara, Ngringin, Condongcatur, Kec. Depok, Kabupaten Sleman, Daerah Istimewa Yogyakarta 55281

Coresponding e-mail: [1]zepinnossa@students.amikom.ac.id

Abstrak

Perkembangan teknologi digital tidak hanya membawa dampak positif tetapi juga memicu peningkatan kejahatan siber, termasuk cyber sexual harassment. Modus kejahatan ini sering kali memanfaatkan teknik steganografi untuk menyembunyikan bukti digital dalam media seperti gambar. Penelitian ini bertujuan untuk menganalisis bukti digital forensik terkait penggunaan teknik steganografi pada media flashdisk dalam konteks kasus cyber sexual harassment. Metode yang digunakan adalah kerangka kerja National Institute of Standards and Technology (NIST) yang terdiri dari empat tahap: collection, examination, analysis, dan reporting. Alat yang digunakan meliputi FTK Imager untuk akuisisi, Autopsy untuk pemeriksaan dan pemulihan data, serta OpenStego dan Steganographystudio untuk steganalisis. Hasil penelitian menunjukkan bahwa proses akuisisi berhasil dengan integritas terjaga (hash MD5 & SHA-1 terverifikasi). Autopsy berhasil memulihkan 10 file gambar yang terhapus. Analisis histogram mengindikasikan adanya anomali pada semua file. Namun, ekstraksi pesan tersembunyi hanya berhasil sebagian: OpenStego berhasil pada 1 file (10%), sedangkan Steganographystudio pada 2 file (20%). Simpulan penelitian menyatakan bahwa pendekatan NIST efektif, namun efektivitas steganalisis sangat bergantung pada alat dan teknik penyembunyian yang digunakan, sehingga diperlukan strategi multi-alat dalam investigasi forensik digital untuk kasus serupa.

Kata Kunci: *Steganalisis, Forensik Digital, Cyber Sexual Harassment, Autopsy*

Abstract

The advancement of digital technology brings not only positive impacts but also an increase in cybercrime, including cyber sexual harassment. This crime often utilizes steganography techniques to hide digital evidence within media such as images. This research aims to analyze digital forensic evidence related to the use of steganography techniques on flash drives in the context of cyber sexual harassment cases. The method used is the National Institute of Standards and Technology (NIST) framework, consisting of four stages: collection, examination, analysis, and reporting. Tools used include FTK Imager for acquisition, Autopsy for examination and data recovery, and OpenStego and Steganographystudio for steganalysis. The results show that the acquisition process was successful with maintained integrity (MD5 & SHA-1 hashes verified). Autopsy successfully recovered 10 deleted image files. Histogram analysis indicated anomalies in all files. However, the extraction of hidden messages was only partially successful: OpenStego succeeded on 1 file (10%), while Steganographystudio succeeded on 2 files (20%). The study concludes that the NIST approach is effective, but the effectiveness of steganalysis is highly dependent on the tools and concealment techniques used, necessitating a multi-tool strategy in digital forensic investigations for similar cases.

Keywords: *Steganalysis, Digital Forensics, Cyber Sexual Harassment, Autopsy*

1. Pendahuluan

Perkembangan teknologi digital dan komunikasi telah memberikan banyak kemudahan dalam berbagai aspek kehidupan, termasuk akses informasi yang cepat dan luas. Namun, di sisi lain, kemajuan ini juga membuka peluang bagi tindak kejahatan siber, salah satunya adalah *cyber sexual harassment* atau pelecehan seksual daring. Cyber sexual harassment merupakan bentuk kejahatan yang memanfaatkan teknologi digital untuk melakukan pelecehan secara tidak langsung, misalnya melalui pengiriman pesan, gambar, atau konten bernuansa seksual tanpa persetujuan korban (Henry & Powell, 2018). Fenomena ini menjadi perhatian serius mengingat dampak psikologis dan sosial yang dapat ditimbulkannya terhadap korban. Sebagai upaya menyembunyikan aktivitas ilegalnya, para pelaku kejahatan siber sering kali memanfaatkan teknik-teknologi penyembunyian data. Salah satu teknik yang populer adalah steganografi, yaitu seni menyembunyikan pesan rahasia di dalam media digital seperti gambar, audio, atau video tanpa menimbulkan kecurigaan (Johnson et al., 2000). Teknik ini memungkinkan pelaku untuk menyisipkan informasi pribadi korban atau instruksi kejahatan ke dalam file yang tampak biasa, sehingga menyulitkan pendeteksian oleh pihak yang tidak berwenang. Pada konteks investigasi forensik digital, analisis terhadap bukti digital yang menggunakan teknik steganograf disebut steganalisis yang menjasdimenjadi tantangan tersendiri. Steganalisis adalah proses untuk mendeteksi, menganalisis, dan mengekstrak informasi tersembunyi dari suatu media (Patel et al., 2007). Efektivitas investigasi sangat bergantung pada kemampuan alat dan metodologi yang digunakan untuk mengungkap bukti-bukti tersembunyi tersebut, terutama dalam kasus-kasus sensitif seperti pelecehan seksual daring.

Penelitian ini berfokus pada penerapan metodologi forensik digital yang terstruktur untuk menganalisis bukti digital pada media penyimpanan flashdisk yang diduga digunakan dalam kasus cyber sexual harassment dengan memanfaatkan teknik steganografi. Penelitian ini mengadopsi kerangka kerja dari *National Institute of Standards and Technology* (NIST) yang terdiri dari empat tahap utama: *collection*, *examination*, *analysis*, dan *reporting* (NIST, 2012). Kerangka ini dipilih karena memberikan panduan sistematis dan standar yang diakui secara internasional dalam penyelidikan forensik digital. Melalui penelitian ini, diharapkan dapat dievaluasi efektivitas beberapa alat steganalisis open-source, yaitu OpenStego dan Steganographystudio, dalam mengidentifikasi dan mengekstrak pesan tersembunyi pada file gambar. Hasil penelitian ini diharapkan dapat memberikan kontribusi dalam pengembangan metode investigasi forensik digital, khususnya dalam mengungkap kejahatan siber yang memanfaatkan teknik steganografi, serta menjadi referensi bagi penegak hukum dan peneliti di bidang keamanan siber dan forensik digital.

2. Metode Penelitian

Penelitian ini menggunakan pendekatan forensik digital eksperimental dengan menerapkan kerangka kerja yang sistematis dan terstandarisasi. Metode utama yang diadopsi adalah National Institute of Standards and Technology (NIST) Digital Forensic Framework, yang terdiri dari empat fase utama: collection, examination, analysis, dan reporting (NIST, 2012). Kerangka ini dipilih karena memberikan panduan yang jelas, dapat direplikasi, dan memastikan integritas bukti digital selama proses investigasi. Penelitian dilakukan dalam lingkungan terkendali dengan skenario kasus simulasi cyber sexual harassment, di mana bukti digital berupa file gambar yang disisipi pesan rahasia menggunakan teknik steganografi disimpan dan dihapus dari sebuah flashdisk. Penelitian ini bertujuan untuk mengevaluasi efektivitas kombinasi alat forensik digital dan teknik steganalisis dalam mengidentifikasi dan mengekstrak bukti tersembunyi. Gambar 2 menjyajikan alur penelitian yang dimulai dengan tinjauan pustaka. Tahap ini melibatkan studi literatur untuk memahami konsep forensik digital, steganografi, steganalisis, dan kerangka hukum terkait cyber sexual harassment (Casey, 2011; Henry & Powell, 2018). Persiapan juga mencakup instalasi dan konfigurasi seluruh perangkat lunak yang akan digunakan.

BHATARA: Jurnal Multidisiplin
Vol. 3, No.2, April 2026, pp. 40-46, ISSN: 2476-9843

Gambar 1. Alur Penelitian

Tahap berikutnya adalah perancangan dan implementasi Skenario Kasus Simulasi. Skenario dirancang untuk mereplikasi modus operandi dalam kasus *cyber sexual harassment*, di mana pelaku menyembunyikan informasi atau gambar korban di dalam file gambar biasa menggunakan perangkat lunak steganografi, kemudian menyimpannya di flashdisk dan menghapusnya untuk menghilangkan jejak.

Selanjutnya adalah tahap pengumpulan data sesuai pedoman NIST untuk mengamankan bukti asli tanpa mengubahnya (NIST, 2012). Pada penelitian ini, proses akuisisi forensik terhadap flashdisk dilakukan menggunakan FTK Imager untuk membuat salinan bit-by-bit (*forensic image*) dalam format *raw (dd)*. Nilai hash (MD5 dan SHA-1) dihitung dan diverifikasi untuk memastikan integritas dan keaslian dari citra forensik yang dihasilkan. Tahap selanjutnya adalah tahap Examination atau pemeriksaan data citra. Citra forensik dianalisis menggunakan Autopsy, sebuah platform forensik digital sumber terbuka. Tahap ini berfokus pada pemulihan (*recovery*) file-file yang telah terhapus dari flashdisk dan mengidentifikasi file-file yang berpotensi menjadi *carrier* steganografi. Autopsy digunakan untuk mengekstrak artefak digital dan menyaring file berdasarkan jenis, metadata, dan status penghapusan.

Tahapan analisis merupakan inti dari penelitian ini, yang menerapkan teknik steganalisis. Analisis dilakukan dalam dua lapis: pertama, analisis visual menggunakan histogram untuk mendeteksi anomali statistik pada file gambar yang mengindikasikan adanya penyisipan data (Provos & Honeyman, 2003). Kedua, analisis ekstraksi menggunakan dua alat steganalisis berbeda, yaitu OpenStego (versi 0.8.6) dan Steganographystudio (versi 1.0.2), untuk mencoba mengekstrak pesan tersembunyi dari setiap file gambar yang berhasil dipulihkan. Perbandingan hasil dari kedua alat ini dilakukan untuk mengevaluasi efektivitasnya.

Tahap akhir adalah pelaporan temuan, dimana semua temuan dari setiap fase didokumentasikan secara rinci. Laporan mencakup metodologi, alat yang digunakan, hasil akuisisi dan pemulihan, hasil analisis steganalisis (termasuk tingkat keberhasilan ekstraksi), serta interpretasi dari bukti digital yang berhasil ditemukan. Hasil evaluasi terhadap efektivitas alat dan metode juga disajikan dalam fase ini. Adapun alat dan bahan penelitian ini menggunakan perangkat keras berupa laptop dengan spesifikasi standar dan sebuah flashdisk sebagai media

bukti simulasi. Perangkat lunak utama terdiri dari, a) FTK Imager 4.5.0.3, untuk akuisisi citra forensik, b) Autopsy 4.17.0 untuk pemeriksaan forensik dan pemulihan data, c) OpenStego 0.8.6: untuk analisis dan ekstraksi steganografi, d) Steganographystudio 1.0.2 untuk analisis dan ekstraksi steganografi sebagai alat pembanding dan e) Sepuluh file gambar format JPEG yang telah dimanipulasi dengan teknik steganografi sebagai sampel bukti digital.

3. Hasil dan Pembahasan

Berdasarkan penerapan metodologi NIST yang telah diuraikan, penelitian ini berhasil menjalankan seluruh tahapan forensik digital dan steganalisis terhadap bukti digital dalam skenario kasus cyber sexual harassment. Bab ini menyajikan temuan dari setiap fase investigasi, mulai dari hasil akuisisi citra forensik flashdisk yang divalidasi dengan nilai hash, pemulihan sepuluh file gambar yang telah dihapus menggunakan Autopsy, hingga analisis mendalam terhadap file-file tersebut dengan teknik histogram dan dua alat steganalisis berbeda. Pembahasan akan menginterpretasikan temuan tersebut, termasuk menguraikan efektivitas dan keterbatasan dari setiap alat yang digunakan, serta menganalisis implikasi dari tingkat keberhasilan ekstraksi pesan rahasia yang relatif rendah dalam konteks investigasi forensik digital untuk kasus kejahatan siber yang kompleks.

3.1. Hasil Akuisisi dan Validasi Bukti Digital (Tahap Collection)

Proses akuisisi terhadap flashdisk bukti berkapasitas 15 GB menggunakan FTK Imager berhasil menghasilkan satu citra forensik utuh dalam format raw (dd) yang terbagi menjadi 10 fragment file berukuran 1,5 GB masing-masing. Validasi integritas dilakukan dengan membandingkan nilai hash antara media asli dan citra forensik yang dihasilkan. Hasil perhitungan menunjukkan bahwa nilai MD5 (d354f8da01cdf52ff8d4da47f665427) dan SHA-1 (8670792b60cab9a696b5e39aaa95d566e42eb25d) pada sumber dan citra forensik identik, yang mengonfirmasi bahwa proses akuisisi berjalan tanpa kesalahan dan integritas bukti digital terjaga.

Tabel 1. Hasil Validasi Hash pada Proses Akuisisi dengan FTK Imager

Deskripsi	Nilai Hash MD5	Nilai Hash SHA-1	Status Verifikasi
Sumber (Flashdisk Asli)	d354f8da01cdf52ff8d4da47f665427	8670792b60cab9a696b5e39aaa95d566e42eb25d	-
Citra Forensik Hasil Akuisisi	d354f8da01cdf52ff8d4da47f665427	8670792b60cab9a696b5e39aaa95d566e42eb25d	Verified

3.2. Hasil Pemeriksaan dan pemulihan data

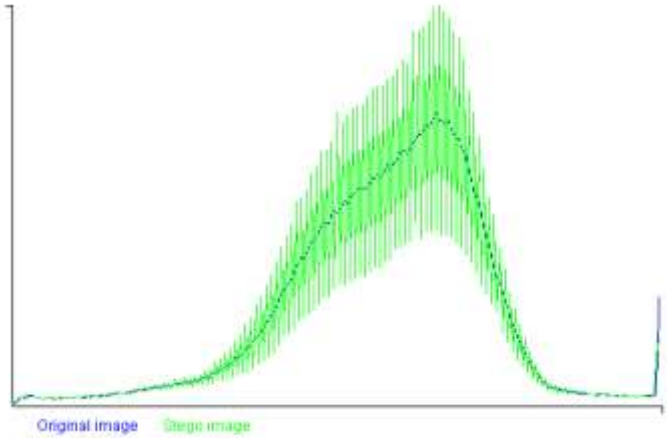
Pemeriksaan terhadap citra forensik menggunakan Autopsy berhasil mengidentifikasi dan memulihkan (*recovery*) **10 (sepuluh) file gambar** berformat JPEG yang sebelumnya telah dihapus dari flashdisk. Kesepuluh file tersebut, yang diberi label *Ilustrasi1.jpg* hingga *Ilustrasi10.jpg*, berhasil diekstrak dari *unallocated space* media penyimpanan dan siap untuk dianalisis lebih lanjut. Proses ini menunjukkan efektivitas Autopsy dalam melakukan *file carving* dan pemulihan artefak digital yang terhapus.

3.3. Hasil Analisis Steganografi

Analisis dilakukan dalam dua tahap: analisis indikatif menggunakan histogram dan analisis ekstraksi menggunakan dua perangkat lunak steganalisis.Analisis visual terhadap histogram dari setiap file yang dipulihkan menunjukkan pola yang konsisten. Pada semua file, grafik histogram Gambar 2 menampilkan distribusi warna yang tidak merata dengan adanya puncak-puncak tajam pada nilai intensitas tertentu, berbeda dengan pola histogram yang halus yang biasanya ditemukan

BHATARA: Jurnal Multidisiplin
Vol. 3, No.2, April 2026, pp. 40-46, ISSN: 2476-9843

pada gambar asli tanpa modifikasi. Anomali statistik ini merupakan indikator kuat bahwa telah terjadi manipulasi pada bit-bit least significant bit (LSB) dari gambar, yang mengarah pada kemungkinan adanya data tersembunyi di dalamnya (Provos & Honeyman, 2003).



Gambar 2. Histogram Steganography hasil analisis

Proses ekstraksi pesan rahasia dari kesepuluh file gambar dilakukan secara terpisah menggunakan OpenStego (v0.8.6) dan Steganographystudio (v1.0.2). Tingkat keberhasilan kedua alat tersebut berbeda signifikan, seperti yang dirangkum dalam Tabel 2.

Tabel 2. Hasil Ekstraksi File Steganografi Menggunakan Dua Alat Steganalisis

Nama File Bukti	Hasil Ekstraksi (OpenStego)	Hasil Ekstraksi (Steganographystudio)
Ilustrasi1.jpg	Tidak Berhasil	Tidak Berhasil
Ilustrasi2.jpg	Tidak Berhasil	Berhasil
Ilustrasi3.jpg	Tidak Berhasil	Tidak Berhasil
Ilustrasi4.jpg	Tidak Berhasil	Tidak Berhasil
Ilustrasi5.jpg	Tidak Berhasil	Berhasil
Ilustrasi6.jpg	Berhasil	Tidak Berhasil
Ilustrasi7.jpg	Tidak Berhasil	Tidak Berhasil
Ilustrasi8.jpg	Tidak Berhasil	Tidak Berhasil
Ilustrasi9.jpg	Tidak Berhasil	Tidak Berhasil
Ilustrasi10.jpg	Tidak Berhasil	Tidak Berhasil
Total Keberhasilan	1 dari 10 File	2 dari 10 File

Berdasarkan Tabel 2, OpenStego hanya berhasil mengekstrak konten tersembunyi dari satu file (*Ilustrasi6.jpg*), sementara Steganographystudio berhasil mengekstrak dari dua file yang berbeda (*Ilustrasi2.jpg* dan *Ilustrasi5.jpg*). Tidak ada file yang berhasil diekstrak oleh kedua alat secara bersamaan. Konten yang berhasil diekstrak dari ketiga file tersebut adalah gambar lain yang berupa foto korban simulasi, yang mengonfirmasi skenario *cyber sexual harassment*. Berdasarkan data pada Tabel 2, tingkat keberhasilan (*success rate*) masing-masing alat dihitung dengan rumus:

$$P = \frac{E}{T} \times 100\%$$

Dimana P adalah presentase keberhasilan, E adalah jumlah ekstraksi berhasil, dan T adalah total file yang dianalisis (10 file), dimana:

a) **Tingkat Keberhasilan OpenStego:** $P = \frac{1}{10} \times 100\% = 10\%$

b) **Tingkat Keberhasilan Steganographystudio:** $P = \frac{2}{10} \times 100\% = 20\%$

Dengan demikian, Steganographystudio menunjukkan efektivitas dua kali lipat dibandingkan OpenStego dalam konteks penelitian ini, meskipun tingkat keberhasilannya secara absolut masih tergolong rendah. Berdasarkan hasil perhitungan prosenstase diatas, maka penelitian ini dikatakan berhasil dalam mendemonstrasikan penerapan metode forensik digital NIST dalam menyelidiki kasus *cyber sexual harassment* dengan bukti digital berbasis steganografi. Hasil yang diperoleh memberikan wawasan penting mengenai efektivitas alat, kompleksitas steganalisis, dan implikasi praktis bagi investigasi forensik digital. Adapun beberapa wawasan yang berkaitan dengan hasil analisis keberhasilan forensika digital ini adalah: pertama validitas metode NIST dan integritas bukti digital, keberhasilan validasi nilai hash MD5 dan SHA-1 yang identik antara flashdisk asli dan citra forensik membuktikan bahwa tahap *collection* telah memenuhi prinsip utama forensik digital: menjaga integritas dan keaslian bukti tanpa mengubahnya (NIST, 2012). Prosedur akuisisi yang tepat dengan FTK Imager memastikan bahwa seluruh analisis selanjutnya dilakukan pada salinan forensik, bukan pada bukti asli, sehingga memenuhi standar adminsibilitas bukti di pengadilan (Casey, 2011). Hal ini menjadi fondasi krusial yang menjustifikasi validitas seluruh temuan penelitian. Kedua efektivitas alat dalam pemulihan data dan deteksi awal penggunaan Autopsy pada tahap *examination* terbukti sangat efektif. Kemampuannya dalam memulihkan sepuluh file gambar yang telah dihapus menunjukkan bahwa penghapusan biasa (*simple deletion*) tidak menghilangkan data secara fisik, melainkan hanya menghapus penanda alokasinya.

Temuan ini sejalan dengan penelitian sebelumnya yang menyatakan bahwa *file carving* pada *unallocated space* sering kali berhasil memulihkan artefak kunci (Riskiyadi, 2020). Selanjutnya, analisis histogram yang dilakukan pada semua file yang dipulihkan secara konsisten mengindikasikan adanya anomali statistik. Pola histogram yang tidak wajar ini, berupa distribusi yang terpotong atau puncak tajam pada nilai intensitas tertentu, merupakan indikator kuat manipulasi LSB (*Least Significant Bit*), teknik steganografi yang paling umum (Provos & Honeyman, 2003). Dengan demikian, kombinasi Autopsy dan analisis histogram berfungsi sebagai filter yang kuat untuk mengidentifikasi file-file yang berpotensi menjadi *stego-object* sebelum proses ekstraksi yang lebih intensif.

Ketiga, menjadi sebuah analisis komparatif efektivitas alat steganalisis tentang perbedaan tingkat keberhasilan ekstraksi antara OpenStego (10%) dan Steganographystudio (20%). Perbedaan ini dapat dijelaskan oleh beberapa faktor antara lain: a) Kompatibilitas algoritma. Steganographystudio mungkin dilengkapi dengan lebih banyak algoritma deteksi dan ekstraksi yang cocok dengan metode penyisipan tertentu yang digunakan dalam skenario ini, sementara OpenStego mungkin terbatas pada algoritma bawaan tertentu dan, b) Faktor konfigurasi dan kepekaan (*sensitivity*). Steganographystudio mungkin memiliki parameter analisis yang lebih agresif atau sensitif dalam mendeteksi modifikasi pada bit-bit gambar. Rendahnya tingkat keberhasilan secara keseluruhan (maksimal 20%) menggarisbawahi tantangan dalam steganalisis *blind* (tanpa pengetahuan awal tentang algoritma steganografi yang digunakan). Hasil ini memperkuat temuan penelitian Damayanti & Utomo (2021) yang menyatakan bahwa tidak ada alat steganalisis tunggal yang dapat menyelesaikan permasalahan forensika digital pada kasus forensika citra.

4. Kesimpulan

Berdasarkan hasil penelitian dan pembahasan yang telah dilakukan, dapat disimpulkan bahwa penerapan metodologi forensik digital National Institute of Standards and Technology (NIST) efektif dalam menyelidiki kasus *cyber sexual harassment* dengan bukti digital berupa file steganografi pada media flashdisk. Penelitian ini berhasil membuktikan bahwa integritas bukti dapat dijaga melalui proses akuisisi dengan FTK Imager, yang divalidasi melalui kesesuaian nilai hash MD5 dan SHA-1 antara media asli dan citra forensik. Selanjutnya, Autopsy terbukti efektif dalam melakukan *examination* dan berhasil memulihkan sepuluh file gambar yang telah terhapus. Pada tahap analisis, kombinasi teknik analisis histogram dan steganalisis terbukti berperan penting. Analisis histogram berhasil mengidentifikasi secara konsisten adanya indikasi anomali

statistik pada semua file yang dipulihkan, berfungsi sebagai alat *triage* awal yang andal. Namun, proses ekstraksi pesan tersembunyi menunjukkan hasil yang variatif. OpenStego berhasil mengekstrak pesan dari 1 file (10%), sementara Steganographystudio menunjukkan kinerja lebih baik dengan keberhasilan mengekstrak 2 file (20%). Temuan ini mengonfirmasi bahwa tidak ada alat steganalisis tunggal yang bersifat universal, dan efektivitasnya sangat bergantung pada kecocokan antara algoritma deteksi yang dimiliki alat dengan teknik steganografi spesifik yang digunakan oleh pelaku. Secara keseluruhan, penelitian ini menegaskan kompleksitas investigasi forensik digital untuk kejahatan siber yang memanfaatkan teknik penyembunyian data seperti steganografi. Kesuksesan investigasi sangat bergantung pada pendekatan metodologis yang terstruktur (seperti NIST), penggunaan beragam alat untuk fungsi yang saling melengkapi, serta kesadaran bahwa *tool dependency* yang berlebihan dapat berisiko. Oleh karena itu, pendekatan multi-alat dan multi-metode menjadi suatu keharusan bagi praktisi forensik digital guna meningkatkan probabilitas keberhasilan dalam mengungkap bukti digital tersembunyi dan mendukung proses hukum secara lebih andal.

Daftar Pustaka

1. Casey, E. (2011). *Digital evidence and computer crime: Forensic science, computers, and the internet* (3rd ed.). Academic Press.
2. Damayanti, H. M., & Utomo, Y. B. (2021). Penerapan teknik steganalysis menggunakan metode chi square attack pada stego image berformat jpeg berbasis Android. *Jurnal Sistem Telekomunikasi, Elektronika, Sistem Kontrol, Power, dan Sistem Komputer*, *1*(1), 51–58.
3. Henry, N., & Powell, A. (2018). Technology-facilitated sexual violence: A literature review of empirical research. *Trauma, Violence, & Abuse*, *19*(2), 195–208. https://doi.org/10.1177/1524838016650189
4. Johnson, N. F., Duric, Z., & Jajodia, S. (2000). *Information hiding: Steganography and watermarking—attacks and countermeasures*. Kluwer Academic Publishers.
5. National Institute of Standards and Technology (NIST). (2012). *Guide to integrating forensic techniques into incident response* (NIST Special Publication 800-86). U.S. Department of Commerce. https://doi.org/10.6028/NIST.SP.800-86
6. Patel, A., Shah, M., Chandramouli, R., & Subbalakshmi, K. P. (2007). Covert channel forensics on the internet: Issues, approaches, and experiences. *International Journal of Network Security*, *5*(1), 41–50.
7. Provos, N., & Honeyman, P. (2003). Hide and seek: An introduction to steganography. *IEEE Security & Privacy*, *1*(3), 32–44. https://doi.org/10.1109/MSECP.2003.1203220
8. Riskiyadi, M. (2020). Investigasi forensik terhadap bukti digital dalam mengungkap cybercrime. *Jurnal Teknologi Informasi dan Ilmu Komputer*, *7*(2), 265–272. https://doi.org/10.25126/jtiik.202072128