DAFTAR PUSTAKA

[1] A. Umbara and D. A. Setiawan, "Analisis Kriminologis Terhadap Peningkatan Kejahatan Siber di Masa Pandemi Covid-19," *J. Ris. Ilmu Huk.*, vol. 2, pp. 81–88, 2022, doi: 10.29313/jrih.v2i2.1324.

[2] M. J. Islami, "Tantangan Dalam Implementasi Strategi Keamanan Siber Nasional Indonesia Ditinjau Dari Penilaian Global Cybersecurity Index," *Masy. Telemat. Dan Inf. J. Penelit. Teknologi*, vol. 8, no. 2, p. 137-144, 2018, doi: 10.17933/mti.v8i2.108.

[3] Pusiknas Bareskrim Polri, "Kejahatan Siber di Indonesia Naik Berkali-kali Lipat," *Pusiknas Bareskrim Polri*, 2022. https://pusiknas.polri.go.id/detail_artikel/kejahatan_siber_di_indonesia_naik_berkali-kali_lipat

[4] R. Ariana, *Perbandingan Hasil Analisa Foto Hoax Menggunakan Metode Exif/Metadata Reverse Image dan Image Forensics*, Bandung: Widina Bhakti Persada Bandung (Grup CV. Widina Media Utama), 2016.

[5] F. Baso, "Performance Analysis of The Last Significant Bit (LSB) Method in Steganography for Data Hiding in Image Data," *J. Secur. Comput. Information, Embed. Network, Intell. Syst.*, vol. 1, pp. 58–62, 2023, doi: 10.61220/scientist.v1i2.20234.

[6] geeksforgeeks, "Analysis of Data Source Using Autopsy," *Geeksforgeeks.Org*, 2024. https://www.geeksforgeeks.org/analysis-of-data-source-using-autopsy/

[7] I. Y. Wirdani, M. Habibi, M. Nirbaya, and S. I. Dinbiru, "Implementasi Digital Forensik pada VMware ESXi Server Berbasis OS Windows 10 Menggunakan GCFIM," *JRIIN (Jurnal Riset Informatika dan Inovasi),* vol. 1, no. 7, pp. 765–773, 2024.

[8] A. Yudhana, A. Fadlil, and M. R. Setyawan, "Analysis of Skype Digital Evidence Recovery based on Android Smartphones Using the NIST Framework," *J. RESTI (Rekayasa Sist. dan Teknol. Informasi)*, vol. 4, no. 4, pp. 682–690, 2020, doi: 10.29207/resti.v4i4.2093.

[9] Sunardi, I. Riadi, and M. H. Akbar, "Penerapan Metode Static Forensics untuk Ekstraksi File Steganografi pada Bukti Digital Menggunakan Framework DFRWS," *J. RESTI (Rekayasa Sist. dan Teknol. Informasi)*, vol. 4, no. 3, pp. 576–583, 2020.

[10] S. Sunardi, I. Riadi, and M. H. Akbar, "Steganalisis Bukti Digital pada Media Penyimpanan Menggunakan Metode Static Forensics," *J. Nas. Teknol. dan Sist. Inf.*, vol. 6, no. 1, pp. 1–8, 2020, doi: 10.25077/teknosi.v6i1.2020.1-8.

[11] N. Saputri and R. Indrayani, "Analisis Data Forensik Investigasi Kasus Peredaran Narkoba pada Smartphone Berbasis Android," *Dharmawangsa: Jurnal Teknologi Informasi dan Ilmu Komputer*, vol. 6, no. 2, pp. 198–204,

2022.

[12] R. Maya, F. Lubis, and J. Panjaitan, “Analisis Perbandingan Aplikasi Open Source Forensic Image Untuk Akuisisi Bukti Digital Ke Dalam Bentuk Image File,” *JUTISAL (J. Tek. Inform. Komput. Univers.)*, vol. 2, no. 1, pp. 25–33,2022.

[13] B. S. Santoso and P. M. Sulaksono, “Static Forensic Pada USB Mass Storage Menggunakan Forensics Toolkit Imager,” *J. Komput. Terap.*, vol. 8, no. 1, pp. 132–142, 2022, doi: 10.35143/jkt.v8i1.5334.

[14] R. I. Utama, I. F. Adam, and W. A. Prabowo, “Analisis Hasil Implementasi Metode Threefry Sebagai Pembangkit Random Number Generator Pada Proses Spread Spectrum Image Steganogrhapy,” *J. Informatics, Inf. Syst. Softw. Eng. Appl.*, vol. 3, no. 1, pp. 69–75, 2020, doi: 10.20895/INISTA.V2I2.

[15] N. C. Lase, "Pengamanan Teks Terenkripsi dengan Algoritma RC4+ dan Steganografi DCS pada Citra Digital," *Pelita Informatika: Informatic Journal*, vol. 8, no. 1, pp. 18–24, 2023.

[16] M. A. Firdaus and A. Rahmatulloh, "Implementasi Steganografi Citra Digital LSB Menggunakan Enkripsi AES-256 dan Embedding Pseudorandom," *Jurnal Teknik Elektro Terapan (JITET)*, vol. 7, no. 1, pp. 47–52, 2023.

[17] G. J. Wibawa, *Anti Forensik Dalam Penyamaran File dengan Kriptografi dan Steganografi*, Skripsi, Program Studi Teknik Informatika, Fakultas Teknologi Industri, Universitas Islam Indonesia, Yogyakarta, 2012.

[18] Sunardi, I. Riadi, and M. H. Akbar, “Application of Static Forensics Method for Extracting Steganographic Files on Digital Evidence Using the DFRWS Framework,” *J. RESTI (Rekayasa Sist. dan Teknol. Informasi)*, vol. 4, no. 3, pp. 576–583, 2020, doi: 10.29207/resti.v4i3.1906.

[19] M. O. Abdillah, O. A. Pane, and F. R. A. Lubis, “Implementasi Keamanan Aset Informasi Steganografi Menggunakan Metode Least Significant Bit (LSB),” *J. Sains dan Teknol.*, vol. 3, no. 1, pp. 40–46, 2023, doi: 10.47233/jsit.v3i1.482.

[20] A. D. Susanti, A. I. Hadiana, F. R. Umbara, dan H. Himawan, "Hybrid Cryptosystem Using RC5 and SHA-3 with LSB Steganography for Image Protection," *Innovatics*, vol. 6, no. 2, pp. 35–45, 2024. doi: 10.1109/INNOVATICS.2024.11515.[Online].Tersedia: https://jurnal.unsil.ac.id/index.php/innovatics/article/view/11515.

[21] M. Adha, F. Yanto, L. Handayani, dan P. Pizaini, "Steganografi gambar menggunakan metode Least Significant Bit pada citra dengan operasi XOR," *Building of Informatics, Technology and Science (BITS)*, vol. 6, no. 1, pp. 1-10, 2022. doi: 10.47065/bits.v6i1.5262.

[22] Fathirma’ruf, *Metodologi Computer Forensik*, Tugas Mata Kuliah Digital Evidence, Program Pascasarjana Teknik Informatika, Fakultas Teknik Industri, Universitas Islam Indonesia, Yogyakarta, 2014.

[23] I. Riadi, A. Fadlil, and M. I. Aulia, “Investigasi Bukti Digital Optical Drive Menggunakan Metode National Institute of Standard and Technology (NIST),” *J. RESTI (Rekayasa Sist. dan Teknol. Informasi)*, vol. 4, no. 5, pp. 820–828, 2020, doi: 10.29207/resti.v4i5.2224.

[24] A. Alshammari, “Detection and Investigation Model for the Hard Disk Drive Attacks using FTK Imager,” *Int. J. Adv. Comput. Sci. Appl.*, vol. 14, no. 7, pp. 767–774, 2023, doi: 10.14569/IJACSA.2023.0140784.

[25] I. R. Khan, "An Overview on Python Programming," *Int. J. Res. Anal. Sci. Eng.*, vol. 4, no. 2, pp. 1–5, 2024.