## DAFTAR PUSTAKA


[1]. Agung, H. (2016). Kriptografi Menggunakan Hybrid Cryptosystem dan Digital Signature. *JATISI (Jurnal Teknik Informatika dan Sistem Informasi)*, *3*(1), 34–45. https://jurnal.mdp.ac.id/index.php/jatisi/article/view/62

[2]. Alherbawi, N., Shukur, Z., & Sulaiman, R. (2013). Systematic Literature Review on Data Carving in Digital Forensic. *Procedia Technology*, *11*(Iceei), 86–92. https://doi.org/10.1016/j.protcy.2013.12.165

[3]. Ali, R. R., Mohamad, K. M., Jamel, S., & Khalid, S. K. A. (2018). A review of digital forensics methods for JPEG file carving. *Journal of Theoretical and Applied Information Technology*, *96*(17), 5841–5856.

[4]. Ardiansyah, A., Hardi, N., & Gata, W. (2020). Identifikasi dan Recovery File JPEG dengan Metode Signature-Based Carving dalam Model Automata. *Komputika : Jurnal Sistem Komputer*, *9*(1), 75–83. https://doi.org/10.34010/komputika.v9i1.2733

[5]. E. Daniel, L. S. (2014). *File-type Detection Using Naïve Bayes and n-gram Analysis*. BIBSYS: Open Journals Systems Serviceboks 509, NO-4898 Grimstad, Norway. https://core.ac.uk/reader/228628450

[6]. Eloff J., B. M. B. (2017). *Software Failure Investigation A Near-Miss Analysis Approach*.

[7]. Hegarty, R., & Haggerty, J. (2016). SlackStick: Signature-Based File Identification for Live Digital Forensics Examinations. *Proceedings - 2015 European Intelligence and Security Informatics Conference, EISIC 2015*, 24–29. https://doi.org/10.1109/EISIC.2015.28

[8]. Karampidis, K., & Papadourakis, G. (2017). File Type Identification - Computational Intelligence for Digital Forensics. *The Journal of Digital Forensics, Security and Law*, *12*(2). https://doi.org/10.15394/jdfsl.2017.1472

[9]. Kustian, M. A. (2023). Analisis Forensik Penggunaan Fungsi Hash Dalam Menentukan Keaslian Video, Metadata Image Dan Magic Number File. *Jurnal Sains, Nalar, dan Aplikasi Teknologi Informasi*, *2*(2), 10–16. https://doi.org/10.20885/snati.v2i2.21

[10]. Muhammad Romzi, & Kurniawan, B. (2020). Pembelajaran Pemrograman Python Dengan Pendekatan Logika Algoritma. *JTIM: Jurnal Teknik Informatika Mahakarya*, *03*(2), 37–44.

[11]. Neaimi, M. Al, Hamadi, H. Al, Yeun, C. Y., & Jamal Zemerly, M. (2020). Digital Forensic Analysis of Files Using Deep Learning. *2020 3rd International Conference on Signal Processing and Information Security, ICSPIS 2020*, *May 2021*. https://doi.org/10.1109/ICSPIS51252.2020.9340141

[12]. Nugis, R. (2018). *Forensic Data Properties of Digital Signature BDOC and ASiC-E Files on Classic Disk Drives*.

[13]. Pabokory, F. N., Astuti, I. F., & Kridalaksana, A. H. (2016). Implementasi Kriptografi Pengamanan Data Pada Pesan Teks, Isi File Dokumen, Dan File Dokumen Menggunakan Algoritma Advanced Encryption Standard. *Informatika Mulawarman : Jurnal Ilmiah Ilmu Komputer*, *10*(1), 20. https://doi.org/10.30872/jim.v10i1.23

[14]. Prawiro, M. (2022). *Pengertian File, Contoh Jenis File Dan Fungsinya Dalam Komputer*. Web Page. https://www.maxmanroe.com/vid/teknologi/komputer/pengertian-file.html

[15]. Putri, M., Iranda, M. D., & Komala, M. P. (2023). Penggunaan Struktur Flow Control Algoritma Perulangan. *Journal Eric*, *10*(10), 6–11.

[16]. Rizal, R., Ruuhwan, R., & Chandra, S. (2020). Signature File Analysis Using The National Institute Standard Technology Method Base on Digital Forensic Concepts. *Jurnal Informatika Universitas Pamulang*, *5*(3), 364. https://doi.org/10.32493/informatika.v5i3.6073

[17]. Underwood, W. (2009). *Extensions of the UNIX File Command and Magic File for File Type Identification*. *September*.

[18]. Yip, M. (2008). Signature analysis and Computer Forensics. *School of Computer Science University of Birmingham*, 1–11. http://www.michaelyip.me.uk/projects/SaCF.pdf