

DAFTAR PUSTAKA

- [1] L. Threestayanti, "Gawat, Tingkat Kasus *Malware* di Indonesia Tertinggi di Asia Pasifik," 3 Juli 2020. [Online]. Available: <https://infokomputer.grid.id/read/122225403/gawat-tingkat-kasus-malware-di-indonesia-tertinggi-di-asia-pasifik?page=all>.
- [2] T. A. Cahyanto, V. Wahhanggara and D. Ramadana, "Analisis dan Deteksi *Malware* Menggunakan Metode *Malware* Analisis Dinamis dan *Malware* Analisis Statis," *JUSTINDO*, vol. I, no. 2, pp. 19-30, 2017.
- [3] PT. Artha Mulia Trijaya, "Mengenal Jenis-Jenis *Malware* yang Dapat Mengancam Data Perusahaan," PT. Artha Mulia Trijaya, 13 April 2022. [Online]. Available: <https://amt-it.com/blog/mengenal-jenis-jenis-malware-yang-dapat-mengancam-data-perusahaan/>. [Accessed 14 Juni 2022].
- [4] B. J. Rothstein, R. J. Hedges and E. C. Winggins, "Managing Discovery of Electronic Information: A Pocket Guide for Judges," *Federal Judicial Center*, p. 24, 2007.
- [5] Wikipedia, "VirusTotal," [id.wikipedia.org](https://id.wikipedia.org/wiki/VirusTotal), 12 Maret 2021. [Online]. Available: <https://id.wikipedia.org/wiki/VirusTotal>. [Accessed 28 Juni 2022].
- [6] V. A. H. Firdaus, D. Suprianto and R. Agustina, "Analisis Forensik Digital Memori Volatile untuk Mendapatkan Kunci Enkripsi Aplikasi DM-Crypt," *Jurnal Sistem Komputer dan Informatika (JSON)*, vol. 3, no. 2, p. 3, 2021.
- [7] F. Bahtiar, N. Widiyasono and A. P. Aldya, "Memori Volatile Forensik untuk Deteksi *Malware* Menggunakan Algoritma Machine Learning," *Jurnal Teknik Informatika dan Sistem Informasi*, vol. II, no. 4, pp. 242-253, 2018.
- [8] T. A. Cahyanto, V. Wahanggara and D. Ramadana, "Analisis dan Deteksi *Malware* Menggunakan Metode *Malware* Dinamis dan *Malware* Analisis Statis," *JUSTINDO, Jurnal Sistem & Teknologi Informasi Indonesia*, vol. I, no. 2, pp. 19-30, 2017.
- [9] B. Khilosiya and K. Makadiya, "MALWARE ANALYSIS AND DETECTION USING MEMORY FORENSICS," *Multidisciplinary International Research Journal of Gujarat Technological University*, vol. II, no. 2, 2020.

- [10] R. Hikmawan, P. S.T., M.T. and G. A. Mutiara., S.T., M.T., "Forensik Digital Random Access Memory Pada Sistem Operasi Linux Menggunakan Metode DumpMemory," *e-Proceeding of Applied Science*, vol. III, no. 3, 2017.
- [11] B. Ramadhan, Y. Purwanto and M. F. Ruriawan, "Forensic Malware Identification Using Naive Bayes Method," *International Conference on Information Technology Systems and Innovation (ICITSI)*, 2020.
- [12] D. S, S. G. S, D. D. Gonsalvez and A. T. Pillai, "Forensic Reconstruction of Executables from Windows 7 Physical Memory," *IEEE International Conference on Computation Intelligence and Computing Research*, 2016.
- [13] C. W. Tien, J. W. Liao, S. C. Chang and S.-Y. Kuo, "Memory Forensics Using Virtual Machine Introspection for Malware Analysis," *IEEE Conference on Dependable and Secure Computing*, 2017.
- [14] A. H. Lashkari, B. Li, T. L. Carrier and G. Kaur, "VolMemLyzer: Volatile Memory Analyzer for Malware Classification using Feature Engineering," *Reconciling Data Analytics, Automotion, Privacy, and Security: A Big Data Challenge (RDAAPS)*, 2021.
- [15] D. S, A. J, I. V and S. M, "Cyber Forensics: Discovering Traces of Malware on Windows Systems," *IEEE Recent Advances in Intelligent Computational System (RAICS)*, 2020.
- [16] Github, Inc., "reversinglabs-yara-rules," 14 4 2021. [Online]. Available: <https://github.com/reversinglabs/reversinglabs-yara-rules>. [Accessed 10 4 2022].
- [17] C. Angga, "Analisis Cara Kerja Beragam Fungsi Hash Yang Ada," Bandung, 2011.