DAFTAR PUSTAKA

Abuse.ch., 2020. *About: MALWARE bazaar.* [Online] Available at: https://bazaar.abuse.ch [Accessed 17 August 2025].

Al-Asli, M. & Ghaleb, T. A., 2019. *Review of Signature-based Techniques in Antivirus Products.* Sakaka, IEEE.

Alenezi, M. N., Alabdulrazzaq, H., Alshaher, A. A. & Alkharang, M. M., 2020. Evolution of *Malware* Threats and Techniques: A Review. *International Journal of Communication Networks and Information Security (IJCNIS) ,* Volume 12, pp. 326-337.

Azmi, S. D., Deris, S. & Tata, S., 2023. Implementasi Sistem Deteksi Ransomware Menggunakan Deep Packet Inspection pada Layanan SMK Negeri 1 Palembang. *Indonesian Journal of Multidisciplinary on Social and Technology,* pp. 176-183.

Badan Siber dan Sandi Negara, 2024. *Publikasi: BSSN.go.id.* [Online] Available at: https://www.bssn.go.id/monitoring-keamanan-siber/ [Accessed 23 May 2025].

Badan Siber dan Sandi Negara, 2025. *Publikasi: BSSN.go.id.* [Online] Available at: https://www.bssn.go.id/monitoring-keamanan-siber/ [Accessed 23 May 2025].

Bat-Erdene, M. et al., 2016. Entropy analysis to classify unknown packing algorithms for *malware* detection. *International Journal of Information Security,* Volume 16, pp. 227-248.

Biau, G. & Scornet, E., 2016. A random forest guided tour. *TEST,* Volume 25, p. 197–227.

Chen, Z., Zhang, X. & Kim, S., 2021. A Learning-based Static *Malware* Detection System with Integrated Feature. *Intelligent Automation & Soft Computing.*

Davies, S. R., Macfarlane, R. & Buchanana, W. J., 2021. Differential Area Analysis for Ransomware Attack Detection within Mixed *File Dataset*s. *Computer and Security,* Volume 108, p. 102377.

Davies, S. R., Macfarlane, R. & Buchanan, W. J., 2022. Comparison of Entropy Calculation Methods for Ransomware Encrypted *File* Identification. *Entropy,* Volume 24, p. 1503.

Davies, S. R., Macfarlane, R. & Buchanan, W. J., 2022. NapierOne: A modern mixed *file* data set alternative to Govdocs1. *Forensic Science International: Digital Investigation,* Volume 40, pp. 301330 - 301344.

Gaspari, F. D. et al., 2020. *EnCoD: Distinguishing Compressed and Encrypted File Fragments using Entropy-Based Classification.* Cham, Springer.

Gibert, D., Mateu, C., Planes, J. & Vicens, R., 2018. *Classification of Malware by Using Structural Entropy on Convolutional Neural Networks.* New Orleans, PKP Publishing Services Network.

Higuera, J. B. et al., 2020. *Systematic Approach to Malware Analysis (SAMA): Applied Science: Journals: MDPI.* [Online]

Available at: https://doi.org/10.3390/app10041360 [Accessed 24 April 2024].

Hsu, C.-M.et al., 2021. Enhancing *File* Entropy Analysis to Improve Machine Learning Detection Rate of Ransomware. *IEEE Access,* Volume 9, pp. 138345- 138351.

Huo, T., Glueck, D. H., Shenkman, E. A. & Muller, K. E., 2023. Stratified split sampling of electronic health records. *BMC Medical Research Methodology,* Volume 23, p. 128.

Jones, K. J. & Wang, Y., 2020. *Malgazer: An Automated Malware Classifier With Running Window Entropy And Machine Learning.* Miami Beach, IEEE Xplore.

Kamboj, A., Kumar, P., Bairwa, A. K. & Joshi, S., 2022. Detection of *malware* in downloaded *file*s using various machine learning models. *Egyptian Informatics Journal,* Volume 24, pp. 81-94.

Keyes, D. S. et al., 2021. *EntropLyzer: Android Malware Classification and Characterization Using Entropy Analysis of Dynamic Characteristics.* Hamilton, IEEE Xplore.

Kirkland, J. et al., 2024. *Automated Detection of Crypto Ransomware Using Machine Learning and File Entropy Analysis: TechRxiv.* [Online] Available at: https://doi.org/10.36227/techrxiv.172833027.76280291/v1 [Accessed 14 5 2025].

O'Neill, B., 2024. *What is a Double Extension File?,* California: Cloudmersive.

Prayitno, D., Santoso, N. A. & Kurniawan, R. D., 2022. Systematic Literature Review: Implementasi Metode Statis dan Dinamis pada Analisa *Malware*. 16(2).

RevoU, 2025. *Cross Validation: Kosakata: RevoUpedia.* [Online] Available at: https://www.revou.co/kosakata/cross-validation [Accessed 14 June 2025].

Ridho A. P., C., 2025. *Posts: BANJARMASIN-CSIRT.* [Online] Available at: https://csirt.banjarmasinkota.go.id/ [Accessed 6 May 2025].

Rigatti, S. J., 2017. Random Forest. *Journal of Insurance Medicine,* 47(1), p. 31–39.

Sadaiyandi, J., Arumugam, P., Sangaiah, A. K. & Zhang, C., 2023. Stratified Sampling-Based Deep Learning Approach to Increase Prediction Accuracy of Unbalanced *Dataset*. *Electronics,* Volume 12, p. 4423.

Sanmocte, E. M. T. & Costales, J. A., 2025. Exploring Effectiveness in Software Development: A Comparative Review of System Analysis and Design Methodologies. *International Journal of Computer Theory and Engineering,* Volume 17, pp. 36-43.

Sathyanarayanan, S. & Tantri, B., 2024. Confusion Matrix-Based Performance Evaluation Metrics. *African Journal of Biomedical Research,* Volume 27, pp. 4023-4031.

Singh, J. & Singh, J., 2020. A survey on machine learning-based *malware* detection in executable *file*s. *Journal of Systems Architecture,* pp. 1-24.

Sokolova, M. & Lapalme, G., 2009. A systematic analysis of performance measures for classification tasks. *Information Processing & Management,* 45(4), pp. 427-437.

Sujon, K. M. et al., 2025. A Novel Framework for *Malware* Detection Using Entropy-Based Statistical Features and Machine Learning Models Across *File* Types. *Engineering Research Express,* Volume 7, p. 025257.

Sukhdeve, S. & Sukhdeve, S., 2023. Google Colaboratory. *Google Cloud Platform for Data Science,* Volume 1, pp. 11-34.

Tai, D. Q., Gallus, P. & Františ, P., 2023. *Macro Malware Development Issuses.* Brno, IEEE Xplore.

Tyagi, S. et al., 2022. *Malware Detection in PE files using Machine Learning.* Chhattisgarh, IEEE Xplore.

Williams, M. et al., 2024. *Entropy-Based Network Traffic Analysis for Efficient Ransomware Detection.* [Online] Available at: https://doi.org/10.36227/techrxiv.172840776.66718131/v1 [Accessed 1 May 2025].