DAFTAR PUSTAKA

[1] O. Aslan and R. Samet, "Investigation of possibilities to detect malware using existing tools," in *Proceedings of IEEE/ACS International Conference on Computer Systems and Applications, AICCSA*, 2018, vol. 2017-Octob, pp. 1277–1284, doi: 10.1109/AICCSA.2017.24.

[2] Kaspersky lab, "Kaspersky Security Bulletin 2018 STATISTICS," p. 25, 2018, [Online]. Available: https://go.kaspersky.com/rs/802-IJN-240/images/KSB_statistics_2018_eng_final.pdf.

[3] Malwarebytes LABS, "2019 State of Malware," p. 33, 2019, [Online]. Available: https://resources.malwarebytes.com/resource/2019-state-malware-malwarebytes-labs-report/.

[4] N. Sarantinos, C. Benzaïd, O. Arabiat, and A. Al-Nemrat, "Forensic malware analysis: The value of fuzzy hashing algorithms in identifying similarities," in *Proceedings - 15th IEEE International Conference on Trust, Security and Privacy in Computing and Communications, 10th IEEE International Conference on Big Data Science and Engineering and 14th IEEE International Symposium on Parallel and Distributed Proce*, 2016, pp. 1782–1787, doi: 10.1109/TrustCom.2016.0274.

[5] K. O. Babaagba and S. O. Adesanya, "A study on the effect of feature selection on malware analysis using machine learning," in *ACM International Conference Proceeding Series*, 2019, vol. Part F1481, pp. 51–55, doi: 10.1145/3318396.3318448.

[6] A. Shalaginov, S. Banin, A. Dehghantanha, and K. Franke, "Machine learning aided static malware analysis: A survey and tutorial," *Adv. Inf. Secur.*, vol. 70, no. 1, pp. 7–45, 2018, doi: 10.1007/978-3-319-73951-9_2.

[7] O. R. I. Or-meir, N. I. R. Nissim, Y. Elovici, and L. Rokach, "Dynamic Malware Analysis in the Modern Era — A State of the Art Survey," vol. 52, no. 5, 2019.

[8] G. Kaur, R. Dhir, and M. Singh, "A stress testing web-based framework for

automated malware analysis," *J. Inf. Optim. Sci.*, vol. 38, no. 6, pp. 937–944, 2017, doi: 10.1080/02522667.2017.1372139.

[9] H. S. Anderson and P. Roth, "EMBER: An Open Dataset for Training Static PE Malware Machine Learning Models," 2018, [Online]. Available: http://arxiv.org/abs/1804.04637.

[10] S. Kim, "PE Header Analysis for Malware Detection," 2018.

[11] M. Smith *et al.*, "Dynamic Analysis of Executables to Detect and Characterize Malware," in *Proceedings - 17th IEEE International Conference on Machine Learning and Applications, ICMLA 2018*, 2019, pp. 16–22, doi: 10.1109/ICMLA.2018.00011.

[12] S. K. Sahay and M. Chaudhari, "An Efficient Detection of Malware by Naive Bayes Classifier Using GPGPU," *Adv. Intell. Syst. Comput.*, vol. 924, pp. 255–262, 2019, doi: 10.1007/978-981-13-6861-5_22.

[13] O. Qasim and K. Al-Saedi, "Malware Detection using Data Mining Naïve Bayesian Classification Technique with Worm Dataset," *Int. J. Adv. Res. Comput. Commun. Eng.*, vol. 6, no. 11, pp. 211–213, 2017, doi: 10.17148/IJARCCE.2017.61131.

[14] N. Salmi and Z. Rustam, "Naïve Bayes Classifier Models for Predicting the Colon Cancer," *IOP Conf. Ser. Mater. Sci. Eng.*, vol. 546, no. 5, 2019, doi: 10.1088/1757-899X/546/5/052068.

[15] A. F. Y. Fitriah, M. Rachmadi, and N. Carsono, "Principal Component Analysis (PCA) Karakter-karakter Umbi Wortel (Daucus carota L.) Varietas Lokal Asal Sibayak," *Zuriat*, vol. 29, no. 2, p. 67, 2019, doi: 10.24198/zuriat.v29i2.19803.