

DAFTAR PUSTAKA

- Baldangombo, U., Jambaljav, N., & Horng, S.-J. (2013). *A Static Malware Detection Sistem Using Data Mining Methods. ArXiv:1308.2831 [Cs]*. Retrieved from <https://arxiv.org/abs/1308.2831>
- Cahyanto, T., Wahanggara, V., & Ramadana, D. (2017). *Analisis dan Deteksi Malware Menggunakan Metode Malware Analisis Dinamis dan Malware Analisis Statis*.
- Damodaran, A., Troia, F. D., Visaggio, C. A., Austin, T. H., & Stamp, M. (2015). A comparison of *static*, dynamic, and hybrid analysis for *malware detection*. *Journal of Komputer Virology and Hacking Techniques*, 13(1), 1–12. <https://doi.org/10.1007/s11416-015-0261-z>
- Fuyong, Z., & Tiezhu, Z. (2017, July 1). *Malware Detection and Classification Based on N-Grams Attribute Similarity*. <https://doi.org/10.1109/CSE-EUC.2017.157>
- Fox, N. (2021, October 6). PeStudio Overview: Setup, Tutorial and Tips. Retrieved from www.varonis.com website: <https://www.varonis.com/blog/pestudio>
- Irfan, I. (2021). PERFORMANCE EVALUATION OF PRE-VULCANIZED LIQUID NATURAL RUBBER (PVLNR) IN HOT MIX ASPHALTIC CONCRETE. *International Journal of GEOMATE*, 20(78). <https://doi.org/10.21660/2021.78.j2029>
- Jerlin, M. A. (2015). A Dynamic *Malware* Analysis for Windows Platform - A Survey. *Indian Journal of Science and Technology*, 8(1), 1–5. <https://doi.org/10.17485/ijst/2015/v8i26/81172>

- Karl-Bridge-Microsoft. (2022, June 24). PE Format - Win32 apps. Retrieved from learn.Microsoft.com website: <https://learn.microsoft.com/en-us/windows/win32/debug/pe-format>
- Kim, D., Mirsky, D., Majlesi-Kupaei, A., & Barua, R. (2018). *A Hybrid Static Tool to Increase the Usability and Scalability of Dynamic Detection of Malware*.
- Malin, C. H., Casey, E., Aquilina, J. M., & Rose, C. W. (2012). *Malware forensic field guide for Windows systems digital forensics field guides*. Amsterdam Elsevier Rockland, Mass. Syngress Waltham, Mass. Syngress.
- Mangialardo, R. J., & Duarte, J. C. (2015). Integrating *Static* and Dynamic *Malware* Analysis Using Machine Learning. *IEEE Latin America Transactions*, 13(9), 3080–3087.
<https://doi.org/10.1109/tla.2015.7350062>
- Moser, A., Kruegel, C., & Kirda, E. (2007, December 1). Limits of *Static* Analysis for *Malware Detection*.
<https://doi.org/10.1109/ACSAC.2007.21>
- Pan, Y., Ge, X., Fang, C., & Fan, Y. (2020). A Sistematic Literature Review of *Android Malware Detection* Using *Static* Analysis. *IEEE Access*, 8(2169-3536), 116363–116379.
<https://doi.org/10.1109/access.2020.3002842>
- priyampatel9911. (2022, September 14). What is PeStudio? Retrieved January 20, 2023, from GeeksforGeeks website:
<https://www.geeksforgeeks.org/what-is-pestudio/>

- Samonas, S., & Coss, D. (2014). *THE CIA STRIKES BACK: REDEFINING CONFIDENTIALITY, INTEGRITY AND AVAILABILITY IN SECURITY*. Retrieved from <https://www.proso.com/dl/Samonas.pdf>
- Saurabh. (2018). *Advance Malware Analysis Using Static and Dynamic Methodology*.
- Schmidt, A.-D. ., Bye, R., Schmidt, H.-G. ., Clausen, J., Kiraz, O., Yuksel, K. A., ... Albayrak, S. (2009, June 1). *Static Analysis of Executables for Collaborative Malware Detection on Android*. <https://doi.org/10.1109/ICC.2009.5199486>
- Shalaginov, A., Banin, S., Dehghantanha, A., & Franke, K. (2018). Machine Learning Aided *Static Malware Analysis*: A Survey and Tutorial. *Advances in Information Security*, 7–45, 7–45. https://doi.org/10.1007/978-3-319-73951-9_2
- Sibi Chakkaravarthy, S., Sangeetha, D., & Vaidehi, V. (2019). A Survey on *malware analysis and mitigation techniques*. *Komputer Science Review*, 32, 1–23. <https://doi.org/10.1016/j.cosrev.2019.01.002>.