# DAFTAR PUSTAKA


[1] J. Jang-Jaccard and S. Nepal, “A survey of emerging threats in cybersecurity,” *J. Comput. Syst. Sci.*, vol. 80, no. 5, pp. 973–993, 2014, doi: 10.1016/j.jcss.2014.02.005.

[2] T. A. Cahyanto, V. Wahanggara, and D. Ramadana, “Analisis dan Deteksi Malware Menggunakan Metode Malware Analisis Dinamis dan Malware Analisis Statis,” *Justindo, J. Sist. Teknol. Inf. Indones.*, vol. 2, no. 1, pp. 19–30, 2017, [Online]. Available: http://jurnal.unmuhjember.ac.id/index.php/JUSTINDO/article/view/1037.

[3] E. S. Lamdompak Sistem Komputer and F. Ilmu Komputer, “Klasifikasi Malware Trojan Ransomware Dengan Algoritma Support Vector Machine (SVM),” vol. 2, no. 1, pp. 122–127, 2016, [Online]. Available: http://ars.ilkom.unsri.ac.id.

[4] G. A. Sandag, J. Leopold, and V. F. Ong, “Klasifikasi Malicious Websites Menggunakan Algoritma K-NN Berdasarkan Application Layers dan Network Characteristics,” *CogITo Smart J.*, vol. 4, no. 1, p. 37, 2018, doi: 10.31154/cogito.v4i1.100.37-45.

[5] L. Wen and H. Yu, “An Android malware detection system based on machine learning,” *AIP Conf. Proc.*, vol. 1864, no. August 2017, 2017, doi: 10.1063/1.4992953.

[6] A. Bijalwan, “Botnet Forensic Analysis Using Machine Learning,” *Secur. Commun. Networks*, vol. 2020, 2020, doi: 10.1155/2020/9302318.

[7] N. Bhodia, P. Prajapati, F. Di Troia, and M. Stamp, “Transfer learning for image-based malware classification,” *ICISSP 2019 - Proc. 5th Int. Conf. Inf. Syst. Secur. Priv.*, pp. 719–726, 2019, doi: 10.5220/0007701407190726.

[8] Y. M. Cho and H. Y. Kwon, “API Call Time Interval을 활용한 머신러닝 기반의 악성코드 탐지,” vol. 30, no. 1, pp. 51–58, 2020.