Abstrak

Malware adalah perangkat lunak atau program berbahaya yang dapat merusak sistem operasi komputer dan jaringan. Banyak penelitian telah dilakukan untuk mencegah serangan malware yang dapat menimbulkan kerugian. Para peneliti telah mengembangkan metode deteksi dan klasifikasi malware berdasarkan metode statis dan dinamis. Namun, kedua metode ini memiliki kekurangan masing-masing, seperti metode statis yang kurang efektif dalam mendeteksi jenis file baru, dan metode dinamis yang lebih memakan sumber daya dan memiliki biaya yang lebih tinggi. Para peneliti juga telah mengembangkan berbagai teknik untuk mendeteksi malware berdasarkan fitur-fitur Pe-Probe. Untuk mengatasi masalah tersebut, tugas akhir ini mengusulkan pengembangan algoritma deteksi malware berbasis fitur Pe-Probe menggunakan machine learning untuk meningkatkan akurasi deteksi dan klasifikasi. Metode yang digunakan dalam penelitian ini adalah studi literatur tentang deteksi dan klasifikasi malware, pengembangan algoritma klasifikasi untuk deteksi malware berbasis metode Pe-Probe, pengembangan prototype, pengujian performansi, dan analisis. Penelitian ini menggunakan dataset sebanyak 19611 file Pe-Probe, yang terdiri dari data Pe-Probe yang terinfeksi malware dan tidak terinfeksi malware. Dengan menggunakan model machine learning stacking dan parameter tuning, hasil validasi menunjukkan nilai akurasi sebesar 0.978, detection rate sebesar 0.9905, dan false alarm rate sebesar 0.057.

Kata Kunci: Malware, Machine Learning, Pe-probe.