ABSTRAK

Perkembangan teknologi informasi yang pesat turut meningkatkan risiko serangan siber, khususnya *malware* yang mampu mengakses sistem secara jarak jauh dan menimbulkan kerugian besar. Penelitian ini bertujuan untuk mengembangkan dan menguji sistem deteksi *malware* berbasis algoritma *Decision Tree*, melalui simulasi serangan dan analisis performa deteksi. Proses penelitian mencakup simulasi serangan menggunakan *Metasploit* dengan dua skenario *file* (*malware* dan normal), ekstraksi lalu lintas jaringan melalui *Wireshark*, serta pengolahan *data* (*labeling*, pembersihan, normalisasi, dan pembagian data). Data dalam format *PCAP* diubah menjadi *CSV*, kemudian diklasifikasi menggunakan *Decision Tree* dengan pencarian parameter optimal melalui *Grid Search* (108 kombinasi).

Model terbaik memiliki konfigurasi: *Criterion 'gini'*, *Max Depth* 10, *Max Features* 15, *Min Samples Leaf* 500, dan *Min Samples Split* 1000. Hasil evaluasi menunjukkan kinerja luar biasa dengan akurasi, *precision*, *recall*, dan *F1*-Score masing-masing sebesar 99.95%, serta *ROC-AUC* 100%. Deteksi *malware* mencapai akurasi 99.96%, sedangkan trafik *normal* 99.94%, dengan *false positive rate* hanya 0.06%. Rata-rata waktu pelatihan 13.40 ± 2.14 detik menunjukkan efisiensi komputasi tinggi. Fitur *Fragment Offset* menjadi penentu utama dengan kontribusi 91.20%. Tidak ditemukan indikasi *overfitting* berdasarkan kesenjangan akurasi dan *F1* yang sangat kecil.

Secara keseluruhan, penelitian ini berhasil menghasilkan sistem deteksi *malware* yang akurat, cepat, dan hemat sumber daya, serta dapat diterapkan secara efektif untuk proteksi jaringan secara *real-time*, baik di lingkungan kecil maupun skala *enterprise*.

Kata Kunci: *Decision Tree*, deteksi *malware*, keamanan siber, *machine learning*, analisis *traffic* jaringan