ABSTRAK

Malware merupakan sebuah perangkat lunak untuk merusak dan mencuri informasi berbagai sumber jaringan atau server yang tidak diketahui oleh pemiliknya, virus *malware* yang berbahaya rentan terhadap keamanan pada sistem agar *malware* mendapatkan akses untuk mengganggu layanan pada sistem serta mengambil informasi yang ditargetkan. Proses analisis yang dilakukan untuk mengidentifikasi apakah suatu file itu *malware* atau bukan.

Semakin meningkat perkembangan *malware* bisa membuat *malware* tidak bisa terdeteksi karena dapat menghindari teknik analisis *malware* yang dilakukannya untuk mendeteksi *malware* dengan analisis *malware*, perkembangan *malware* dapat menghindari teknik analisis agar *malware* tidak dapat terdeteksi. Oleh karena itu penelitian ini membuat atau merancang sebuah sistem otomatis mendeteksi *malware* menggunakan proses analisis dinamis dengan cuckoo *Sandbox* untuk dapat menghasilkan data yang diklasifikasikan. Proses analisis yang diklasifikasikan menggunakan sebuah algoritma *K-Nearest Neighbors* yang digunakan untuk mengklasifikasi file *malware*, pada metode ini *K-Nearest Neighbors* lebih memilih jalur terdekat dari tetangganya agar mendapatkan hasil akurasi yang optimal.

Proses identifikasi file *malware* dan *goodware* pada algoritma *K-Nearest Neighbors* memiliki akurasi 95% deteksi menggunakan karakteristik dinamis hasil pengujian menggunakan Kfold Cross validation mendapat nilai rata 92%.

Keyword**:** *Malware, Analisis Dinamis,* Klasifikasi*, K-Nearest Neighbors,* Cuckoo *Sandbox*