ABSTRAK

Malware adalah sejenis perangkat lunak yang, jika diinstal pada perangkat korban, dapat melakukan tindakan jahat. Tindakan jahat dapat berupa pencurian data, kegagalan sistem, atau penolakan layanan. Analisis *malware* adalah proses untuk mengidentifikasi apakah suatu perangkat lunak adalah *malware* atau tidak. Namun, dengan kemajuan tekno*log*i *malware*, ada beberapa teknik penghindaran yang dapat diterapkan oleh pengembang *malware* untuk mencegah analisis, seperti polimorfik dan oligomorfik. Oleh karena itu, dalam penelitian ini kami mengusulkan sistem deteksi *malware* otomatis. Dalam sistem kami, data karakteristik *malware* diperoleh melalui proses analisis statis dan dinamis. Data dari proses analisis diklasifikasikan menggunakan algoritma Naive Bayes untuk mengidentifikasi apakah perangkat lunak itu *malware* atau tidak. Proses mengidentifikasi file *malware* dan *goodware* menggunakan metode pembelajaran mesin Naive Bayes memiliki nilai akurasi 93 persen untuk proses deteksi menggunakan karakteristik statis dan 85 persen untuk deteksi melalui karakteristik dinamis.

Keyword: *Malware, Naive Bayes, Analisis Statis, Analisis Dinamis, Portable Executable, API Call Sequence.*