Abstrak

Keamanan sistem dari kejahatan dunia maya telah mendorong munculnya forensik jaringan (*network forensic*), yaitu suatu sistem yang dapat memonitor, menangkap, mengamankan dan menganalisa barang bukti, yang ditransmisikan melalui jaringan.

Dalam tugas akhir ini, digunakan metode *Support Vector Machine* (SVM) yang merupakan teknik inteligensia buatan untuk klasifikasi multi-label pada manajemen data forensik jaringan. Mesin inteligensia buatan tersebut bekerja dengan melakukan klasifikasi intrusi paket TCP pada data trafik jaringan.

Analisa data dilakukan dengan membandingkan nilai akurasi pada berbagai skenario pengujian sistem. Skenario dirancang untuk dapat menggambarkan kinerja sistem bila diaplikasikan dengan variasi parameter SVM yang diterapkan pada berbagai kondisi.

Hasil yang didapatkan dari proses klasifikasi serangan ini menunjukkan akurasi dapat dipertahankan tinggi bila data dikumpulkan terlebih dahulu secara offline. Kesimpulan yang diperoleh SVM lebih tepat digunakan untuk data offline dimana karakteristik data uji dibuat semirip data latih.

Kata kunci: forensik jaringan, *support vector machine*, intrusi paket TCP, klasifikasi multi-label.