ABSTRAK

Seiring berjalannya perkembangan teknologi, semakin banyak orang menggunakan komputer dalam mempermudah perkerjaannya. Dengan semakin berkembangnya teknologi kejahatan di dunia digital semakin meningkat, seperti serangan malware. Penggunaan komputer dalam kejahatan digital semakin sering terjadi namun banyak yang belum bisa identifikasi apa yang terjadi pada perangkat yang di akuisisi.

Maka dari itu, digital forensik memori volatile menjadi salah satu atau jalan keluar untuk mengatasi masalah tersebut. Tugas akhir ini merancang sebuah aplikasi yang dapat melakukan analisis dan prediksi anomali pada memori volatile. Metode penelitian menggunakan metode NIST (Nasional Institute of Standards and Technology).

Analisis hasil *dump* memori volatile menggunakan *decision tree* untuk klasifikasi anomali dengan otomatis membaca dan menghitung akurasi. Proses klasifikasi berdasarkan nilai informasi file *dump* dari sampel memori. Aplikasi analisis dan klasifikasi ini mampu melakukan fungsionalitasnya pada memori *dump*.

Kata Kunci: *Digital Forensik, memori volatile, memori*