

## Abstrak

Internet sekarang ini sudah menjadi bagian yang tidak bisa dipisahkan dari kehidupan kita sekarang ini. Karena perkembangan Internet ini juga, maka resiko serangan yang terjadi pada jaringan juga akan semakin besar. Untuk menghindari dan mengurangi jumlah serangan yang terjadi maka harus dilakukan analisis pada trafik yang terjadi pada jaringan komputer. Namun, karena trafik ini berjumlah sangat banyak, maka akan sangat sulit jika dilakukan analisis secara manual. Karena itulah diperlukan suatu metode yang efektif dan sesuai dengan cara kerja para pakar *network forensic* dalam menganalisis jaringan itu sendiri.

Salah satu metode yang bisa digunakan untuk melakukan pendeteksian serangan ini adalah Artificial Neural Network yang sangat cocok digunakan untuk kasus pengklasifikasian dalam hal ini adalah pengklasifikasian ada serangan atau tidak. Metode yang digunakan adalah *Recurrent Neural Network (RNN)* yang bisa melakukan analisis serangan yang terjadi dan juga melakukan evidence extraction. RNN ini akan diaplikasikan ke *log file*, dimana *log file* sendiri merupakan suatu file yang mencatat akses pengguna pada saluran akses penyelenggara jasa akses.

Hasil akhir dari penelitian ini adalah bahwa dengan metode RNN ini, bisa dilakukan analisis pendeteksian serangan pada jaringan dengan efektif, terbukti dengan akurasi rata-rata terendah adalah 94% dan yang tertinggi adalah 98,67%

Kata kunci: *network forensic, RNN, log file*