Abstrak

Teknologi yang semakin berkembang menyebabkan arsitektur *Software Define Network* (SDN) menjadi semakin populer. Semakin banyak digunakan, maka perlu untuk mempertimbangkan masalah keamanan. Di dalam jaringan SDN OpenFlow terdapat masalah keamanan berupa serangan yang dieksploitasi oleh *hacker*, salah satunya adalah Pembajakan Lokasi Host. Serangan ini berupa pembelokan paket ke penyerang, data dari korban diduplikasi sehingga muncul layanan palsu dan dapat menyebabkan layanan terputus. Dengan adanya masalah keamanan tersebut, diperlukan proes forensik jaringan dengan melakukan analisis log untuk mendapatkan bukti serangan. Namun analisis log masih dilakukan secara manual, maka diperlukan sistem analisis log secara otomatis agar dapat mempermudah proses penyelidikan. Metode *Clustering K-Means* digunakam untuk otomatisasi analisis log dalam mendeteksi serangan. Hasil penelitian ini menghasilkan sistem yang dapat menampilkan serangan Pembajakan Lokasi Host berdasarkan data log yang ada pada jaringan SDN OpenFlow. Hasil akurasi yang didapat menunjukkan bahwa nilai *cluster* mempengaruhi nilai akurasi, semakin tinggi nilai *cluster* maka semakin rendah nilai akurasi yang didapatkan, artinya semakin banyak serangan yang dikelompokkan maka semakin sedikit sistem akan mendeteksi serangan.

Kata Kunci : SDN OpenFlow, Pembajakan Lokasi Host, Forensik, *Clustering K-Means*