ABSTRAK

Kemunculan arsitektur Software Define Network yang tidak terfokus pada keamanan jaringan sehingga memiliki kekurangan pada keamanan jaringan[3], Dalam pengontrol OpenFlow memiliki keterbatasan dalam menyimpan flow enties sehingga dapat menyebabkan OpenFlow Flow Table, kekurangan ini dapat dieksploitasi oleh hacker untuk melakukan pembajakan. Dengan adanya sisi negatif pada penggunaan jaringan komputer ini diperlukan pengembangan pada forensik jaringan untuk dapat melakukan identifikasi penyelidikan.Untuk meningkatkan efisiensi cost waktu dalam proses investigasi diperlukan analisis agar file log dapat dilakukan secara otomatis. Metode Clustering dipilih karena dapat menangani noise dan dapat melakukan clustering pada dimensi data (atribut) yang tinggi dan K-Mean Clustering dipilih karena pada algoritma ini memiliki waktu komputasi yang cepat dan efisien dengan jumlah data yang cukup besar. Hasil Pengujiaan ini akan menampilkan penyerang sehingga file log dapat dengan mudah dibaca oleh orang awam.

Kata Kunci : Software Define Network(SDN), OpenFlow, OverTable, Forensik, Bukti Digital