BAB 1
PENDAHULUAN

1.1. Latar Belakang

Software Defined Networking (SDN) adalah paradigma jaringan baru yang memisahkan *control plane* dan *data plane* dalam suatu jaringan yang memungkinkan administrator untuk mengkofigurasi, memantau, dan mengotomasi jaringan tanpa mengubah konfigurasi yang ada [4]. *Control Plane* menjadi inti dari SDN karena terdapat *controller* yang bertanggung jawab untuk mengelola arus lalu lintas paket di jaringan, meneruskan arus paket dan mengambil keputusan dalam perutean [18]. Untuk membangun komunikasi antara *control plane* dan *data plane* pada jaringan SDN dibutuhkan protokol yang disebut Openflow. Namun, sejak awal aristektur SDN OpenFlow memiliki kelemahan dari segi keamanan, hal ini menimbulkan kerentanan baru yang disebabkan oleh sebuah serangan [3]. *Denial of Service (DoS)* adalah salah satu serangan yang dapat ditimbulkan akibat kurangnya keamanan pada SDN, serangan ini paling mengancam bagi *controller* SDN karena sasaran serangan ini adalah untuk mengkomsumsi sumber daya dari server sehingga server tidak dapat melayani host yang sah [1].

Pada penelitian sebelumnya yaitu *"An Evidence-Based Technical Process for OpenFlow-Based Software Defined Networking Forensics"* bahwa didalam penelitian tersebut melakukan kegiatan forensik jaringan pada arsitektur SDN dan menghasilkan bukti berupa file log yang menunjukkan adanya beberapa serangan yang terjadi didalam jaringan, termasuk serangan DoS, tetapi pembacaan log file masih dilakukan secara manual dengan membacanya per baris satu per satu file [1]. Oleh karena itu pada tugas akhir ini penulis akan melakukan analisis file log yang sudah ada. Log yang telah diambil tersebut nantinya akan dianalisis menggunakan metode K-Means Clustering. Analisis yang dilakukan adalah pendeteksian ada tidaknya serangan DoS pada jaringan, pencarian sumber dan sasaran serangannya. Metode K-Means Clustering merupakan salah satu dari metode Clustering yang ada. Metode K-Means Clustering dipilih karena mempunyai kemampuan mengelompokkan data dalam jumlah yang cukup besar dengan waktu yang cepat dan efisien serta dapat menghasilkan kelompok data menjadi ada tidaknya serangan pada jaringan [19].

1.2. Perumusan Masalah

Berdasarkan latar belakang berikut adalah rumusan masalah pada tugas akhir ini yaitu:

1. Bagaimana memproses *log file* dengan metode *K-Means Clustering* agar bisa digunakan untuk keperluan forensik terutama pada serangan *DoS* ?
2. Bagaimana *K-Means Clustering* yang baik agar didapatkan hasil akurasi yang bagus dalam mendeteksi serangan DoS ?

Adapun batasan masalah dari tugas akhir ini adalah :

1. Forensik digital berfokus pada serangan yang terjadi di *controller* SDN.
2. Serangan yang digunakan adalah Denial of Service (DoS).
3. Forensik dilakukan secara offline, sehingga data log yang dianalisis adalah log files yang telah ada bukan dilakukan saat sistem sedang berjalan.
4. *Controller* yang digunakan adalah *Single Controller*.
5. SDN hanya menggunakan OpenFlow.
6. Versi OpenFlow yang digunakan adalah 1.3.
7. Modul berjalan menggunakan RYU Controller 4.2.

1.3. Tujuan

Berdasarkan perumusan masalah, maka tujuan pembuatan tugas akhir ini adalah :

1. Mengetahui cara memproses log files dengan mengimplementasikan metode K-Means Clustering, sehingga bisa digunakan untuk keperluan forensik terutama pada serangan DoS.
2. Mengetahui K-Means Clustering yang baik dalam menghitung akurasi untuk mendeteksi serangan DoS pada analisis log file.

1.4. Rangkaian Kegiatan

Table 1. Rencana Kegiatan

Kegiatan	Bulan									
	Jan	Feb	Mar	Apr	Mei	Sep	Oct	Nov	Dec	Jan
Studi Literatur										
Pengumpulan Data										
Identifikasi Sistem										
Analisis dan Perancangan Sistem										
Tahap Pembuatan Sistem										
Tahap Pengujian Sistem										
Penulisan Laporan										