

# BAB I

## PENDAHULUAN

### 1.1 Latar Belakang

Kehidupan manusia telah dimudahkan dengan hadirnya sebuah alat yang disebut dengan komputer. Komputer adalah sekelompok alat elektronik yang menerima perintah kemudian diproses dengan perhitungan yang akan menghasilkan informasi. Dengan kemajuan teknologi, komputer yang ada saling terhubung membentuk suatu jaringan komputer. Jaringan komputer bertujuan untuk mempermudah dalam bertukar informasi antar komputer. Dalam kasus tersebut, terdapat sebuah komputer yang akan memberikan informasi atau layanan yang disebut dengan server. Server adalah suatu unit komputer yang berfungsi untuk menyimpan informasi dalam suatu jaringan komputer. Server tersebut akan melayani seluruh *client* atau *workstation* yang terhubung ke jaringannya dan merupakan perangkat utama dalam sebuah sistem komunikasi jaringan yang berfungsi sebagai penyedia layanan atau *service* (Sembiring, 2010).

Badan Sistem Informasi Universitas Islam Indonesia (BSI UII) adalah sebuah badan di UII yang memberikan layanan sistem dan teknologi informasi. Dalam memberikan layanan tersebut, BSI UII dibantu dengan adanya beberapa server yang bekerja sesuai dengan ketentuannya. Server yang bekerja melayani *client* atau *workstation* akan menghasilkan sebuah catatan data yang disebut dengan *log*. *Log* adalah sebuah *file* yang berisi daftar tindakan, kejadian (aktivitas) yang telah terjadi di dalam suatu sistem komputer (Tarigan, Engel, & Angela, 2018). Awalnya, *log* digunakan untuk memecahkan masalah, tetapi sekarang *log* banyak berperan dalam kemajuan suatu organisasi. *Log* telah berevolusi mengandung banyak informasi terkait dengan suatu jaringan komputer. Saat ini, *log* mampu membantu mengoptimalkan suatu sistem dan kinerja suatu jaringan komputer (Sahoo, Chottray, Jena, & Pattnaiak, 2012). *Log* dari sebuah server berisi banyak data yang akan mencatat kegiatan server tersebut, contohnya mengenai sistem, *user*, dan lain-lain. Selain itu, *log* pada suatu server juga akan berisi sesuai dengan aplikasi yang dipasang pada server tersebut, contohnya sebuah web server akan memiliki data *log* berbeda dengan dns server. Berdasarkan dari masing-masing kegiatan, maka akan terbentuk sebuah *log* yang memberikan informasi berupa teks. Oleh sebab itu, sebuah server akan berisi informasi dari berbagai macam *log* sesuai aktivitas yang terjadi pada server tersebut. *Log* sangat diperlukan untuk membantu administrator dalam mengatasi hal-hal yang berpotensi menimbulkan masalah, ataupun melacak masalah yang sudah atau

sedang terjadi, baik itu masalah keamanan maupun yang lainnya (Tarigan et al., 2018). Selain *log* terdapat sebuah protokol khusus yang bisa memberikan informasi mengenai status server yaitu *Simple Network Management Protocol* (SNMP). Dalam SNMP, terdapat dua buah perangkat yang disebut dengan *SNMP Agent* dan *SNMP Manager*. *SNMP Agent* adalah perangkat yang akan memberikan informasi sedangkan *SNMP Manager* adalah yang menerima informasi. Dalam melakukan komunikasi antara *SNMP Agent* dan *SNMP Manager*, SNMP akan menggunakan lima buah pesan sederhana yaitu *GET*, *GET-NEXT*, *GET-RESPONSE*, *SET*, and *TRAP*. Pada dasarnya, *SNMP Manager* akan memberikan pesan *GET*, *GET-NEXT*, dan *SET* untuk meminta informasi yang ada pada *SNMP Agent*. Kemudian, *SNMP Agent* baru akan membalas dengan pesan *GET-RESPONSE* untuk memberikan informasinya kepada *SNMP Manager*. Selain itu, *SNMP Agent* juga dapat memberikan pesan *TRAP* yaitu pesan notifikasi yang dipicu oleh suatu kejadian di *SNMP Agent*. Dikarenakan proses kerja SNMP yaitu meminta data untuk mendapatkan informasi, maka *log* merupakan solusi yang mudah bagi seorang administrator dikarenakan *log* sudah menyediakan berbagai informasi yang sedang atau sudah terjadi. Selain itu, SNMP dengan pesan *TRAP* juga memiliki kelemahan yaitu ia hanya mengirim notifikasi ketika terjadi sesuatu pada server. Dengan demikian, seorang administrator akan sulit mengetahui apakah server yang memberikan informasi masih hidup ataupun mati. Berdasarkan situs (Cisco, 2009), mereka mengklaim bahwa salah satu produk mereka hanya memiliki 90 *SNMP Traps*, namun memiliki 6000 *syslog event messages*. Dari keterangan berikut dapat disimpulkan bahwa *log* akan memberikan lebih banyak informasi mengenai kejadian pada sebuah server. Dengan banyaknya informasi maka dapat membantu seorang administrator contohnya saja *troubleshooting*.

Sebagai penyedia layanan, sistem yang berjalan pada server harus mampu berjalan selama 24 jam penuh. Oleh sebab itu, untuk memantau jalannya layanan pada server diperlukan pencatatan dalam bentuk *log management system* yang bersifat *realtime* untuk mencatat aktivitas layanan yang berjalan pada server (Arifin, Sugiartowo, & Susilowati, 2018). *Log management* adalah proses untuk menghasilkan, mentransmisikan, menyimpan, menganalisis, dan mengatur keamanan data pada komputer (Chuvakin, Schmidt, & Phillips, 2013). Untuk membantu administrator BSI UII dalam mengelola *log* tersebut, maka penulis akan mengembangkan sistem dengan bantuan *log management system*. Penulis menggunakan *open source log management system* yaitu Elasticsearch, Logstash, Kibana, dan Filebeat (ELK Stack) dalam penerapannya. Dengan ELK Stack penulis dapat memvisualisasikan *log* secara terpusat. Visualisasi merupakan sarana untuk menyampaikan informasi sesuatu tanpa

membutuhkan banyak waktu. Dengan visualisasi, analisis akan lebih efisien dibandingkan harus membaca teks dalam jumlah yang banyak. Visualisasi yang baik akan memberikan informasi penting terkait kebutuhan, namun tidak menutup kemungkinan detail informasi juga harus tersedia. Dengan visualisasi tersebut membantu administrator mendapatkan informasi dan memungkinkan untuk melakukan tugas yang lain pada saat yang bersamaan (Lodde, 2009).

## 1.2 Rumusan Masalah

Adapun rumusan masalah dalam penelitian ini yang sesuai dengan masalah yang dipaparkan di atas yaitu:

- a. Bagaimana memvisualisasikan *log* server di BSI UII secara terpusat?

## 1.3 Batasan Masalah

Adapun batasan masalah pada penelitian ini, yaitu:

- a. *Log* berasal dari server BSI UII yang bersistem operasi Linux.

## 1.4 Tujuan Penelitian

Adapun tujuan dari dilakukannya penelitian ini yaitu:

- a. Dapat membantu administrator BSI UII *monitoring* server.

## 1.5 Manfaat Penelitian

Manfaat yang didapat pada penelitian ini berupa:

- a. Mempermudah administrator dalam proses analisis server.

## 1.6 Metodologi Penelitian

Adapun tahapan metodologi penelitian yang diterapkan dalam penulisan laporan tugas akhir ini adalah sebagai berikut:

- a. Studi literatur

Pada tahap awal penelitian, penulis melakukan studi literatur baik dari buku, jurnal, forum, artikel, tugas akhir, dan sebagainya yang berkaitan dengan topik tugas akhir penulis.

- b. Pengumpulan data

Pada tahap ini dilakukan wawancara kepada pihak-pihak BSI UII yang terlibat dalam pengembangan sistem.

c. Pengembangan

Pada tahap ini dilakukan pengembangan sistem dengan melakukan analisis kebutuhan serta perancangan sistem.

d. Implementasi

Pada tahap ini dilakukan implementasi pada server BSI UII.

e. Pengujian

Pada tahap ini dilakukan dengan menguji fungsionalitas sistem yang telah diimplementasikan pada server BSI UII.

### 1.7 Sistematika Penulisan

Sistematika penulisan disusun untuk memudahkan dalam melakukan pembahasan tugas akhir ini. Sistematika penulisan tugas akhir ini terbagi menjadi lima bab. Dari lima bab tersebut, masih terbagi menjadi beberapa subbab. Adapun uraian dari masing-masing bab tersebut yaitu:

**Bab I Pendahuluan**, bab ini membahas tentang pengantar permasalahan yang akan akan diselesaikan. Bab ini berisi latar belakang masalah, batasan masalah, rumusan masalah, tujuan penelitian, manfaat penelitian, metodologi penelitian, dan sistematika penulisan.

**Bab II Landasan Teori**, bab ini berisi teori-teori yang berkaitan dan menjadi landasan dalam penelitian tugas akhir ini. Adapun teori-teori tersebut yaitu yang berhubungan dengan manajemen *log* pada sistem operasi Linux.

**Bab III Metodologi**, bab ini berisi uraian tentang langkah penyelesaian tugas akhir penulis. Pada bab ini penulis akan membahas mengenai data yang penulis butuhkan, analisis kebutuhan, dan lain-lain.

**Bab IV Hasil dan Pembahasan**, bab ini berisi pembahasan hasil akhir dari implementasi sistem yang telah dibuat.

**Bab V Kesimpulan dan Saran**, bab ini berisi kesimpulan yang merupakan rangkuman dari keseluruhan hasil penelitian tugas akhir. Selain itu, juga terdapat saran untuk mengembangkan lebih lanjut sistem tersebut.