Bab I Pendahuluan

I.1.1 Latar Belakang

Perkembangan teknologi saat ini mempermudah manusia untuk saling terhubung menggunakan komputer yang terhubung dengan internet. Dibalik itu terdapat dampak negatif dari perkembangan teknologi ini, salah satunya adalah *cyber crime*. *Cyber crime* adalah perbuatan melawan hukum yang dilakukan dengan menggunakan komputer untuk memperoleh keuntungan ataupun tidak dengan merugikan pihak lain (Wisnubroto, 1999). *Cyber crime* yang marak dilakukan salah satunya adalah memanfaatkan kelemahan sistem jaringan komputer dengan menyusupkan program yang digunakan sebagai media untuk mencuri informasi dari sebuah sistem komputer, program ini disebut sebagai *malware*(Marthur, 2013).

Malware singkatan dari *malicious software* adalah *software* yang digunakan untuk melakukan aktivitas yang sifatnya merusak dan mengganggu (Zeltser, 2014). Pada umumnya penyebaran *malware* menggunakan berbagai cara, seperti *social engineering attack, email phising,* dan *downloader*. Tujuan penyebaran *malware* adalah untuk pencurian data rahasia, mencari username dan password, dan spam email (Zeltser, 2014). Selain itu, perangkat lunak yang dianggap sebagai perangkat perusak berdasarkan yang terlihat dan bukan berdasarkan ciri-ciri tertentu, mencakup *Virus Computer, Trojan Horse, spyware, adware crimeware* dan lainnya yang berniat jahat dan tidak diinginkan (G.Kaur, B. Nagpal, 2012).

Berkembangnya teknologi memicu berkembangnya *malware* baru, sehingga semakin banyak pihak yang dirugikan. Bahkan saat ini, *malware* dapat menjangkit hampir seluruh jenis sistem operasi, salah satunya yaitu sistem operasi android. Sistem operasi android adalah sistem operasi seluler *open source* berfitur lengkap pertama yang diciptakan untuk melayani pasar konsumen (Shaerpour, K dan Dehghantanha, A, 2013). *Malware* yang menyerang android disebut android *malware.* Android *malware* menyerang dengan berbagai cara dan salah satunya dengan menggunakan fitur *permission* yang ada pada aplikasi android. Banyak pengguna yang tidak mengerti apa arti dari setiap *permission* dan memberikan *permission* tersebut tanpa memikirkan resiko yang memungkinkan aplikasi tersebut mengakses informasi sensitif pengguna (Franklin, 2014).

Malware analysis adalah suatu aktivitas yang dilakukan untuk mendeteksi ada atau tidaknya *software* yang bertujuan jahat. Karena adanya perkembangan *malware* pada sistem operasi android sehingga *malware analysis* ini akan menjadi solusi untuk mendeteksi adanya *malware*, salah satunya dengan menggunakan *reverse engineering*. *Reverse engineering* dalam analisis *malware* berguna untuk ekstraksi data yang memuat informasi yang ada pada *malware.* Data yang diambil dari hasil *reverse engineering* untuk penelitian ini adalah *permission.* Keuntungan menggunakan *permission-based* ini adalah agar mengetahui kejanggalan dalam sebuah *software* saat meminta akses untuk menggunakan sesuatu didalam *smartphone* yang dimiliki. Pada penelitian ini akan mendapatkan hasil berupa jenis *permission* apa yang paling sering digunakan oleh *malware* agar pengguna android dapat mengetahui dan waspada terhadap jenis *permission* tersebut.

I.1.2 Perumusan Masalah

Pada tugas akhir ini, rumusan masalah yang akan dibahas adalah sebagai berikut:

1. Bagaimana melakukan analisis *malware* pada sistem operasi android pada fitur *permission-based*
2. Bagaimana mengetahui *permission* yang digunakan pada sebuah *malware*
3. Bagaimana mengetahui *permission* yang sering digunakan pada *malware*

I.1.3 Tujuan Penelitian

Pada tugas akhir ini, tujuan yang ingin dicapai adalah sebagai berikut:

1. Melakukan analisis *malware* pada sistem operasi android pada fitur *permission-based*
2. Dapat mengetahui *permission* yang digunakan pada sebuah *malware*
3. Dapat mengetahui *permission* yang sering digunakan pada *malware*

I.1.4 Manfaat Penelitian

Manfaat dari tugas akhir ini adalah sebagai berikut:

1. Dapat mengetahui analisis *malware* pada sistem operasi android pada fitur *permission-based*
2. Dapat mengetahui *permission* yang digunakan pada sebuah *malware*

3. Dapat mengetahui jenis *permission* yang sering digunakan oleh *malware*

I.1.5 Batasan Masalah

Ruang lingkup dari tugas akhir ini adalah sebagai berikut :

1. Menggunakan *reverse engineering*
2. Menggunakan lima puluh sample *malware* dengan API level 19 kebawah
3. Hanya mengacu dan membahas *permission* yang ada pada android manifest
4. Tidak menjalankan *malware*

I.1.6 Sistematika Penulisan

Penulisan ini akan dijabarkan dengan sistematika penulisan sebagai berikut:

BAB I PENDAHULUAN

Bab ini meliputi latar belakang, perumusan masalah, tujuan penelitian, manfaat penelitian, batasan masalah dan sistematika penulisan

BAB II LANDASAN TEORI

Bab ini menjelaskan literatur yang relevan dengan permasalahan yang dihadapi. Menjelaskan setiap teori yang digunakan berdasarkan referensi yang telah didapatkan.

BAB III METODOLOGI PENELITIAN

Bab ini menjelaskan langkah-langkkah penelitian secara rinci, mulai dari tahap awal, tahap hipotesis, tahap simulasi, tahap analisis dan tahap akhir dari penelitian.

BAB IV PERANCANGAN SISTEM DAN SKENARIO DETEKSI

Bab ini menjelaskan rancangan sistem yang digunakan, beserta dengan skenario dan pengerjaan penelitian ini.

BAB V HASIL ANALISIS

Bab ini menjelaskan hasil dari analisis pengerjaan penelitian ini.

BAB VI PENUTUPAN

Bab ini menjelaskan kesimpulan dan saran dari penelitian ini berdasarkan data yang didapatkan.