BAB I
PENDAHULUAN

1.1. Latar Belakang

Dalam era *digital* yang semakin maju, pengunaan aplikasi *mobile* telah menjadi bagian penting dalam kehidupan sehari-hari. *Play Store*, sebagai *platform* distribusi aplikasi *Android* yang populer, menyediakan akses mudah ke berbagai aplikasi yang dapat diunduh oleh pengguna. Namun, dengan popularitas dan ketersediaan yang luas ini, ada resiko adanya aplikasi yang mengandung *malware*, yaitu perangkat lunak berbahaya yang dirancang untuk merusak perangkat, mencuri data pribadi, ataupun mengganggu sistem[1].

Aplikasi pengunduh atau *downloader* adalah salah satu jenis aplikasi yang banyak digunakan pengguna *smarthphone* untuk mengunduh berbagai konten seperti *video, musik,* dan *dokumen(Mila Rosyida,n.d.).* Namun, dalam beberapa tahun terakhir, telah terjadi peningkatan kasus *malware* yang terkait dengan aplikasi pengunduh di *Play Store*. *Malware* pada aplikasi pengunduh dapat mencakup fitur berbahaya seperti virus komputer (*Trojan Horse),* perangkat pengintai *(spyware),* perangkat iklan *(adware)* yang tidak jujur, perangkat jahat *(crimeware), Ransomware* dan perangkat lunak lainnya yang berniat jahat dan tidak diinginkan yang dapat mengancam privasi dan keamanan pengguna[3]. Berkembangnya teknologi ini pun dapat memicu dikembangkannya jenis *malware-malware* baru.

Sistem *Android* merupakan sebuah sistem operasi yang berbasis *Linux* untuk telepon seluler seperti *smarthphone* dan *tablet PC.* Sistem *Android* ini memiliki keunggulan, seperti sistem operasi yang bersifat *open source*, *multitasking*, kemudahan dalam hal *notifikasi* hingga banyaknya aplikasi atau *software* yang dapat dinikmati dengan menggunakan sistem *Android*[4]. Akan tetapi, salah satu keunggulan sistem *Android* menjadi salah satunya kelemahan. Keunggulan sistem operasi yang bersifat *open access*, dimana disediakan *platform* terbuka bagi para pengembang (*user*) yang dimaksudkan agar *user* dapat menciptakan dan mengembangkan aplikasi mereka sendiri sehingga dapat digunakan bermacam

perangkat *seluler.* Akan tetapi, hal ini malah menimbulkan kemudahan oleh pihak yang tidak bertanggung jawab untuk membangun dan mengembangkan *malware* menjadi aplikasi yang dapat masuk ke sistem operasi *Android*[5].

Analisis *forensik malware* memungkinkan identifikasi, analisis, dan pemahaman mendalam tentang jenis-jenis malware yang ada, sumber asalnnya, dan dampak yang mungkin ditimbulkannya. Dengan pemahaman yang lebih baik tentang ancaman ini, pengguna dapat mengambil langkah-langkah yang diperlukan untuk melindungi perangkat dan menjaga keamanan informasi pribadi[5]. Pada penelitian sebelumnya telah dilakukan dalam bidang analisis *forensik aplikasi*, namun penelitian khusus tentang analisis *forensik* untuk perangkat terindikasi *malware* masih terbatas.

Oleh karena itu, penelitian ini akan mengisi kesenjangan pengetahuan tersebut dan memberikan wawasan yang lebih baik tentang jenis-jenis *malware* yang ada pada aplikasi hasil *unduhan* dari *Play Store*. Dengan pemahaman yang lebih baik tentang *malware* pada aplikasi hasil *unduhan* dari *Play Store*, Langkah-langkah keamanan yang lebih efektif dapat diambil untuk mencegah, dan mengatasi ancaman malware. Melalui penelitian ini diharapkan dapat meminimalisir dampak mengenai keamanan data, serta mengurangi dampak *negatif* yang ditimbulkan oleh *malware* pada aplikasi hasil *unduhan* dari *Play Store* terhadap perangkat *mobile.*

1.2. Rumusan Masalah

Berdasarkan latar belakang di atas, maka dapat diambil sebuah rumusan masalah yaitu:

a. Apa saja jenis *Malware* yang umum ditemukan pada aplikasi hasil unduh di *Google Play Store*?
b. Bagaimana cara melakukan deteksi *Malware* pada aplikasi hasil unduh di *Google Play Store* yang mendukung kegiatan *Forensik*?

1.3. Batasan Masalah

Batasan permasalahan pada penelitian ini adalah sebagai berikut:

a. Analisis *Malware* untuk kegiatan *Forensik* menfokuskan penelitian pada hasil unduh aplikasi di *Google Play Store*.
b. Analisis *Malware* untuk mendukung kegiatan *Forensik* akan dilakukan berdasarkan sampel aplikasi pengunduh yang telah dikumpulkan dan tidak melibatkan uji coba pada pengguna.
c. Pembuatan visualisasi data pada hasil analisis menggunakan library *Jupyter Netbook* yang berbasis *Pyhton.*

1.4. Tujuan Penelitian

Adapun tujuan penelitian ini antara lain sebagai berikut:

a. Menganalisa jenis-jenis *Malware* yang umum ditemukan dalam aplikasi pengunduh di *Google Play Store*.
b. Mengembangun metode analisis *Forensik* untuk mendeteksi dan memvisualisasikan dari hasil analisis *Forensik* terhadap *Malware*

1.5. Manfaat Penelitian

Adapun manfaat yang didapat dari penelitian ini, ialah: Informasi yang dihasilkan dari visualisasi data dapat digunakan untuk membantu dalam mendeteksi pola dan perilaku *Malware* pada aplikasi pengunduh dengan lebih efektif mengenai ancaman keamanan yang belum terdeteksi sebelumnya.

Dengan manfaat tersebut, penelitian ini diharapkan dapat memberikan pemahaman yang lebih baik tentang ancaman malware pada aplikasi pengunduh di *Google Play Store* dan berkontribusi pada peningkatan keamanan serta perlindungan pengguna dalam menghadapi ancaman-ancaman tersebut.