BAB I PENDAHULUAN

I.1 Latar Belakang

Teknologi antivirus adalah *software* yang digunakan untuk mendeteksi, mencegah, dan menghapus virus komputer. Beberapa produk antivirus populer termasuk Avast, Avira, McAfee, Windows Defender, dan Kaspersky.Teknologi antivirus untuk mendeteksi virus, seperti pemindaian *file*, pemindaian heuristik, dan pemindaian komponen dalam waktu nyata. Teknologi antivirus juga sering menyediakan fitur tambahan seperti perlindungan jaringan, perlindungan email, dan perlindungan privasi (Malin, et al, 2012).

Teknologi *malware* adalah *software* yang dirancang untuk menyebabkan kerusakan, mencuri informasi, atau mengambil alih kontrol komputer tanpa persetujuan. Beberapa jenis *malware* yang umum termasuk *trojan*, *ransomware*, dan *downloader*. Antivirus adalah *software* yang digunakan untuk mendeteksi, mencegah, dan menghapus virus komputer (Malin, et al, 2012).

Potensi antivirus dalam menangani jenis *malware* seperti *trojan*, *ransomware,* dan *downloader* dapat dilihat dari cara menangani konsep *CIA (Confidentiality, Integrity, dan Availability)*. Konsep keamanan *confidentiality* yang diterapkan pada antivirus dapat mendeteksi dan menghapus *trojan*, *ransomware* dan *downloader* yang digunakan untuk mengakses data pribadi yang dienkripsi, sehingga membantu melindungi kerahasiaan informasi (Samonas & Coss, 2014).

Konsep keamanan *integrity* yang diterapkan pada antivirus dapat mendeteksi dan menghapus *ransomware* yang digunakan untuk mengenkripsi *file* pada komputer, sehingga membantu mencegah kerusakan data permanen dan kerusakan sistem.

Konsep keamanan *availability* yang diterapkan pada antivirus dapat mendeteksi dan menghapus *trojan*, *ransomware* dan *downloader* yang digunakan untuk mengambil alih kontrol komputer dan menghentikan akses ke *file* atau aplikasi yang dibutuhkan, sehingga membantu mencegah kesulitan dalam mengakses data dan layanan kritis.

Pada penelitian ini, metode analisis statis digunakan untuk mengetahui aktivitas *malware* dengan cara mengambil informasi pada indikator pendeteksian seperti *string blacklist, section, libraries, file* ratio, dan *function*. Metode ini biasanya digunakan untuk mengidentifikasi apa yang dilakukan oleh *malware* jika dijalankan. Jumlah indikator pendeteksian *malware* akan digunakan untuk mengetahui karakteristik antivirus pada fitur yang akan diuji. Karakteristik antivirus sangat penting untuk diperhatikan. Hal ini dikarenakan jika antivirus memiliki performa yang buruk, menyebabkan kinerja sistem komputer menjadi terhambat dan berpotensi rawan untuk disusupi oleh *malware*. Selain itu, tingkat deteksi antivirus juga menjadi hal utama dalam melindungi perangkat dari serangan *malware*.

I.2 Perumusan Masalah

Merujuk kepada latar belakang yang telah dijelaskan sebelumnya, pada penelitian ini dapat diambil rumusan masalah yang mendasari penelitian ini yaitu:

a. Bagaimana mengenali karakteristik antivirus berdasarkan indikator pendeteksian *malware?*
b. Bagaimana membandingkan karakteristik dari berbagai antivirus dalam mendeteksi *malware?*
c. Bagaimana mengetahui tingkat deteksi antivirus dalam menangani *malware*?

I.3 Tujuan Penelitian

Berdasarkan rumusan masalah yang telah disebutkan sebelumnya, dapat ditentukan tujuan pada penelitian ini, yaitu:

a. Mengetahui karakteristik antivirus berdasarkan indikator pendeteksian *malware*.
b. Mengetahui hasil perbandingan karakteristik antivirus dalam mendeteksi *malware* berdasarkan sumber daya komputasi dan waktu *scan.*
c. Mengetahui tingkat deteksi antivirus dalam menangani *malware* berdasarkan akurasinya.

I.4 Batasan Masalah

Adapun pembatasan penelitian yang dikaji dalam penelitian ini adalah sebagai berikut:

1. Analisis *malware* statis hanya melakukan pengambilan data dari total temuan atau indikator pendeteksian *malware* sebagai pendukung untuk mengenali karakteristik antivirus.
2. Analisis karakteristik antivirus hanya menggunakan metrik penggunaan sumber daya komputasi, tidak membahas metrik lain selain metrik tersebut.
3. Sampel antivirus dan *malware* yang digunakan berjumlah 5 dan 6, *malware* yang digunakan berjenis *trojan, ransomware dan downloader* berekstensi *.exe*

I.5 Manfaat Penelitian

Adapun manfaat yang diharapkan dapat dirasakan setelah melakukan penelitian ini dari segi teoritis dan praktis adalah sebagai berikut:

1. Keilmuan

   Secara keilmuan, Penelitian ini diharapkan dapat menjadi acuan dalam memahami cara kerja *software* antivirus dan bagaimana antivirus dapat digunakan untuk mendeteksi dan mencegah *malware*, mengidentifikasi sumber daya komputer yang berperan penting pada antivirus dalam mendeteksi *malware* serta menambah wawasan tentang bagaimana sumber daya sistem mempengaruhi proses kerja *software* antivirus.

2. Praktis

   Secara praktis, penelitian ini diharapkan dapat dijadikan panduan dalam mengidentifikasi dan mengevaluasi karakteristik antivirus yang efektif dalam menangani *malware*, membantu dalam mengevaluasi kinerja dari antivirus yang diujikan dalam menangani *malware*. Selain itu, penelitian ini juga diharapkan dapat mengenali karakteristik penggunaan sumber daya antivirus ketika melakukan *scanning* hingga *malware* di karantina dan kemampuan tingkat deteksi tiap antivirus.