ABSTRAK

ANALISIS KARAKTERISTIK ANTIVIRUS BERDASARKAN AKTIVITAS *MALWARE* MENGGUNAKAN ANALISIS DINAMIS

Oleh

MAARIJ HARITSAH

1202194192

Malware, kependekan dari *"malicious software"*, prosesnya dapat dicegah, dicari, dideteksi dan dihapus menggunakan *software* antivirus. Penelitian ini bertujuan untuk mengenali karakteristik antivirus berdasarkan analisis *malware* dan analisis antivirus. Analisis *malware* mencakup jumlah *registry changes,* total *DLL* yang digunakan dan total *API call* yang dipanggil. Analisis antivirus mencakup sumber daya komputasi seperti penggunaan *CPU, memory, disk,* serta waktu *scan* dan tingkat deteksi. Penelitian ini tidak membahas sistem internal pada antivirus dan tidak membahas *source code*. Sampel *malware* berjumlah 6 yang berjenis *trojan, ransomware,* dan *downloader*. *Platform* percobaan berupa virtualisasi *scanning malware* pada antivirus pada skala laboratorium. Percobaan dilakukan dengan menjalankan *malware* pada lingkungan Windows 8.1 *desktop* dalam *virtual machine*. Kemudian dilakukan *scanning* oleh antivirus dengan monitoring pada sumber daya komputasi menggunakan aplikasi *Task Manager* dan *Personal User Activity*. Hasil percobaan yang diukur pada sumber daya komputasi seperti penggunaan *CPU, memory, disk,* dan waktu *scan*. Pada fitur antivirus yang diuji, antivirus Avast relatif lebih rendah penggunaan sumber daya komputasinya, yaitu sekitar 15.38% pada *CPU,* dan 20.95 *Megabyte* pada *memory*. Pada kecepatan waktu *scan* paling rendah dimiliki oleh McAfee dengan waktu 4.27 detik. Antivirus Kaspersky relatif paling tinggi dalam mendeteksi sampel *malware* dengan tingkat deteksi 100%. Hasil penelitian menunjukan bahwa semakin tinggi nilai metrik pendeteksian pada *malware*, maka semakin tinggi pula nilai metrik yang diuji pada antivirus. Kelanjutan penelitian ini dapat berupa penambahan sampel *malware,* variasi jenis *malware* dan penambahan metrik pada antivirus.

Kata kunci: Karakteristik*, Profiling, Removable Drive Protection, Testing,* Tingkat Deteksi.