

ABSTRAK

ANALISIS KARAKTERISTIK ANTIVIRUS BERDASARKAN METRIK SUMBER DAYA KOMPUTASI DAN INDIKATOR PENDETEKSIAN

Oleh

Ramiz Qudamah

1202190065

Malware, kependekan dari "*malicious software*", proses nya 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 *string blacklist*, *file ratio*, *section*, *libraries*, *function*. 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 15.50% pada *CPU*, dan 22.5 Megabyte pada *memory*. Pada kecepatan waktu *scan* paling rendah dimiliki oleh McAfee dengan waktu 9.17 detik. Antivirus McAfee relatif paling tinggi dalam mendeteksi sampel *malware* dengan tingkat deteksi 100%. Hasil penelitian menunjukkan 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*, *Real-time Protection*, *Testing*, Tingkat Deteksi