A**bstrak**

Malware atau *Malicious Software* adalah program yang dibuat secara khusus untuk menyusup sehingga bisa tetap berada di dalam sebuah sistem untuk periode waktu tertentu tanpa sepengetahuan oleh pemilik sistem tersebut. Menurut penelitian terbaru, *malware* sudah meningkat pada fase yang mengkhawatirkan dan beberapa jenis *malware* bersembunyi di sistem dengan menggunakan teknik yang berbeda. Penelitian ini melakukan deteksi malware menggunakan *system call (syscall)* pada sistem operasi Android. Analisis *Malware Remote Access Trojan* pada sistem operasi Android menggunakan *Metode Reverse Engineering* yang berguna untuk menemukan prinsip teknologi dari perangkat, objek, atau sistem dari analisis struktur, fungsi dan operasinya. Analisis pada metode ini, menggunakan analisis dinamis yaitu dengan menjalankan setiap *malware* pada sistem operasi Android untuk mendapatkan informasi *system call* (*syscall*) yang sedang berjalan. Hasil informasi *system call* (*syscall*) tersebut akan diseleksi menggunakan fitur selection *Machine Learning* menggunakan metode *Random Forest.* Tujuan dari penelitian ini adalah mengetahui ciri-ciri berdasarkan *system call (syscall)* dan akurasi dari sistem deteksi ciri-ciri *adanya malware Remote Access Trojan* pada sistem operasi Android. Hasil rata-rata akurasi pada penelitian ini dengan 4 skenario menggunakan metode *Random Forest* adalah 96% dan nilai f1-score adalah 94%. Nilai akurasi ini cukup baik dan dapat diterapkan dalam deteksi ciri-ciri adanya *malware Remote Access Trojan* berdasarkan *system call (syscall)* pada Sistem Operasi Android.

Kata kunci : ***Malicious Software, Remote Access Trojan, Sistem Operasi Android, System Call (Syscall), Random Forest, Reverse Engineering***