ABSTRAK

Pada generasi milenial seperti sekarang sudah banyak terjadi kejahatan siber, dan itu semakin berkembang dengan pesat. Salah satu kejahatan siber yang menghawatirkan adalah dengan menggunakan *malware*. Saat ini *malware* sudah mulai masuk ke *smartphone* dengan perantara aplikasi. Untuk mengantisipasi masuknya *malware* kedalam *smartphone,* perlu adanya proses analisis dengan metode yang tepat dan mudah digunakan. Salah satu metode yang digunakan adalah dengan meggunakan metode *reverse engineering* atau rekayasa balik yaitu metode untuk mencari suatu informasi adanya malware yang disembunyikan. Untuk mendukung metode *reverse engineering* terdapat sistem operasi yang bernama Remnux yang merupakan salah satu distro dari linux. Di dalam sistem operasi Remnux terdapat tools yang dapat menganalisis malware dalam bentuk apk, xml dan dex yaitu *androguard*. Dari hasil pengujian yang telah dilakukan bahwa sistem analisis aplikasi android ini dapat melakukan analisa terhadap izin aplikasi, nama paket, aktivitas utama dan kode program dari setiap *class*. Terdapat 3 sampel aplikasi versi palsu yang dianalisa dan selanjutnya dibandingkan dengan 3 sampel aplikasi yang didapatkan dari Google Play Store. Hasil akhir yang didapat dari pengujian ini adalah terdeteksinya *malware* pada kode program dari 3 aplikasi versi palsu dan mengetahui cara kerja *malware* tersebut.

Kata Kunci: *Malware, Remnux , Analisis, Reverse Engineering*