ABSTRAK

Modus operasi kejahatan di dunia siber sudah semakin banyak dan beragam. Teknik yang digunakan oleh pelaku kejahatan semakin lama semakin mutakhir. Salah satunya menggunakan *malware*. *Malware* telah dirancang secanggih mungkin untuk membuat celah pada sistem keamanan. Bahkan saat ini *malware* sudah semakin mudah masuk ke dalam komputer melalui perantara *file* dan juga bisa melalui website yang mengandung *malware*. Untuk mengantisipasi masuknya *malware* ke dalam komputer, perlu adanya proses analisis dengan metode yang tepat dan mudah untuk digunakan. Salah satu metode yang mudah adalah dengan menggunakan metode *reverse engineering* yaitu metode untuk mencari suatu informasi yang disembunyikan. Untuk mendukung metode *reverse engineering* terdapat sistem operasi yang bernama *remnux* yang merupakan distribusi dari linux. Di dalam sistem operasi *remnux* terdapat *tools* yang dapat menanalisis malware yang berada pada *file* berbentuk exe yaitu exescan , ada juga analyze.pdf dan pdf id yang dapat menanalisis malware pada *file* berbentuk pdf, serta juga bisa menanalisis alamat *website* yang berbahaya atau mengandung *malware.* Dengan melakukan analisis *malware* menggunakan metode *reverse engineering* pada *remnux* dapat memudahkan seorang analis untuk melakukan analisis terhadap *malware* dan juga membuat seorang analis mendapatkan informasi tentang *malware* yang berguna untuk dilaporkan kepada *developer antivirus* sebagai bahan acuan untuk ke depannya.

Kata Kunci : *Malware*, *reverse engineering*