ABSTRAK

Malware merupakan program ataupun perangkat lunak yang bertujuan untuk masuk ke dalam sistem komputer tanpa sepengetahuan penggunanya dan dapat mengganggu bahkan merusak merusak sistem komputer tersebut. Seiring berjalannya waktu, jenis dan ancaman *malware* kian canggih dan meluas. Penyebaran *malware* dapat melalui berbagai cara dan salah satu caranya ialah pembuat *malware* menyisipkan program *malware* tersebut kedalam berbagai jenis *file* kemudian mengemasnya agar dapat mengelabuhi antivirus sehingga program *malware* tersebut tidak terdeteksi, kemudian ketika pengguna menjalankan atau membuka *file* yang tersisipi *malware* maka otomatis program *malware* akan aktif dan menginfeksi komputer penggunanya.

Oleh sebab itu penelitian ini dilakukan guna mendeteksi dan menganalisis sampel *file* yang terdapat *malware* di dalamnya. Penelitian ini dijalankan di dalam sebuah mesin virtual yang bersistem operasi remnux yang di dalam sistem operasi tersebut telah tersedia sampel *malware* serta *tools* untuk dapat melakukan pembedahan pada sampel *file* yang nantinya akan dideteksi dan dianalisis. Dalam penelitian ini penulis menggunakan metode anomali dengan teknik statis untuk mencari kejanggalan dari sampel *file* yang nantinya akan diteliti. Teknik statis ini tidak menjalankan ataupun mengeksekusi sampel *malware*, tetapi hanya membedahnya. Sampel *File* yang akan diteliti berupa *file* .exe dan *file* pdf. Dalam masing-masing jenis ekstensi *file* tersebut nantinya akan terdapat dua buah sampel *file* yang berbeda yaitu yang bersih dari *malware* dan yang tersisipi *malware* untuk kemudian dibandingkan anomali apa yang ada didalam kedua *file* tersebut.

Pada penelitian ini, tahap-tahap metode anomali yang akan dilakukan adalah fase *training*, learning, dan analisis. Hasil keluaran dari penelitian ini ialah berupa tabel *fileprint* dari anomali pada sampel *file* yang telah diteliti, dan diharapkan dapat membantu pemahaman tentang *malware* serta dalam mengurangi dan mencegah kejahatan siber di dunia maya.

Kata Kunci: *malware*, analisis *malware*, metode anomali, analisis statis, remnux.