ABSTRAK

Setiap tahun laporan serangan *malware* terus meningkat hal ini memaksa para peneliti untuk terus berkembang dan berinovasi dalam melakukan mitigasi, pencegahan, dan pemberantasan serangan *malware*. Disisi lain pihak pengembang *malware* juga tidak ingin kalah, mereka terus berkembang dan berinovasi dengan memanfaatkan alat anti-forensik kategori *data hiding* berupa *program packers*. Meskipun *program packers* termasuk dalam kategori alat anti-forensik, *program packers* juga dapat bermanfaat untuk menjaga integritas dan validitas kode program menggunakan fungsi pengemasan sehingga menyulitkan proses *reverse engineering*. Oleh karena itu pada tugas akhir (TA) ini dilakukan penelitian terkait *program packers* sebagai alat anti-forensik pada kasus serangan *malware*. Penelitian ini bertujuan untuk Mengetahui dampak penggunaan program packers terhadap kemampuan deteksi dan analisis forensik digital dan Mengetahui langkah apa yang harus dilakukan untuk menangani dampak yang dihasilkan oleh *program packers.* Metode yang digunakan pada penelitian ini adalah analisis statis dan analisis dinamis, analisis statis menggunakan metode *reverse engineering* sebagai bagian dari cara mendapatkan informasi program penyusun *malware*, sementara analisis dinamis menggunakan metode eksekusi *malware* pada lingkungan aman untuk mengamati perilakunya secara langsung. Penelitian ini diharapkan bisa memberikan wawasan baru pada analisis *malware* terkait pentingnya memahami *program packers* sebagai anti-forensik pada forensik digital *sample malware*.

Kata Kunci: *malware, program packers, anti-forensics,* forensik digital.