1. PENDAHULUAN

1.1. Latar Belakang

Penemuan sejumlah *malware* diketahui meningkat seiring waktu, berbagai teknik analisis *malware* dalam kegiatan forensik digital telah diusulkan untuk pertahanan dan mitigasi serangan yang disebabkan oleh serangan *malware*[1]. Perangkat lunak berbahaya atau yang biasa disebut *malicious software* (*malware)* adalah program yang dirancang untuk membahayakan individu, perusahaan, atau pemerintah[2], sehingga memaksa peneliti untuk melakukan berbagai cara mitigasi dan pencegahan. Disisi lain pengembang *malware* juga ingin melindungi aset mereka dengan berbagai cara salah satunya menggunakan teknik anti-forensik[3].

Anti-forensik adalah teknik yang bertujuan untuk menyembunyikan, memanipulasi, dan bahkan menghapus data dengan menargetkan pada kredibilitas barang bukti digital tindak pidana yang diperoleh. Beberapa kategori yang dimiliki oleh anti-forensik sesuai dengan tujuan dan jenis serangannya yaitu: *artifact wiping, data hiding, obfuscation,* dan *attack against forensicss tools and processes*[4]. Dalam penerapannya pengembang malware sering memanfaatkan *obfuscation* dan *data hiding* berupa *program packers* untuk melindungi kode asli dari *malware* yang mereka buat. *Program packers* adalah perangkat lunak kategori *obfuscation* dan *data hiding* yang dapat mengemas *malware*[5]*,* lebih dari itu *program packers* adalah alat yang dapat mengompres dan mengenkripsi konten *malware* dengan memperkecil dan mengaburkan binernya kedalam konten *malware* baru untuk menyulitkan proses investigasi forensik digital[6]. Mengompresi *malware* tidak hanya mengurangi ukuran tetapi juga mengubah tampilan luar *malware*, mengaburkan isi *malware*, menyembunyikan kode dan data aslinya. Oleh karena itu menggunakan *program packers* pada *malware* memberikan keuntungan ganda untuk mengurangi ukuran serta mengaburkan kode asli, data, dan tujuan[4].

Dengan adanya keinginan pengembang *malware* yang ingin melindungi asetnya menggunakan *program packers*, timbul kesalah pahaman bahwa *program packers* identik hanya digunakan untuk pengemasan *malware*, padahal pada praktiknya baik program bersih maupun malware keduanya dapat dilakukan pengemasan menggunakan *program packers*[7]karena secara umum *program packers* bermanfaat untuk mengecilkan ukuran file,

mencegah analisis *reverse engineering,* dan meningkatkan performa penggunaan memori[8].

Berdasarkan penjabaran diatas analisis dampak *program packers* dalam kegiatan forensik digital ini dilakukan untuk memberikan pemahaman mengenai cara kerja *program packers* dalam menyulitkan investigasi forensik digital serta penanganan terhadap metode *obfuscation* dan *data hiding* yang disebabkan oleh *program packers*. Metode yang digunakan dalam penelitian ini meliputi analisis *portable executable* (PE File) sebagai bagian dari analisis statis[9], dimana analisis statis merupakan metode analisis yang tidak perlu melakukan eksekusi terhadap *malware* untuk pengamatannya. Serta analisis jaringan komunikasi sebagai bagian dari analisis dinamis, yang mana analisis ini perlu melakukan eksekusi *malware* untuk kemudian dapat dilakukan analisis[10]. Dengan membandingkan hasil temuan dari *malware* yang sudah dikemas atau belum dikemas, nantinya akan dapat menjadi bahan rujukan dalam membantu kegiatan forensik digital yang melibatkan pengemasan *malware*.

1.2. Rumusan Masalah

Rumusan masalah pada penelitian ini adalah sebagai berikut:

1. Bagaimana membangun sebuah lingkungan pengujian untuk eksekusi file dnegan program packers?
2. Bagaimana dampak penggunaan program packers terhadap kemampuan deteksi dan analisis forensik digital?

1.3. Tujuan

Tujuan yang ingin dicapai dalam pengerjaan TA ini adalah:

1. Membangun lingkungan pengujian untuk eksekusi file dengan program packers.
2. Menganalisis dampak eksekusi file dengan program packers terhadap pertanyaan dalam kegiatan forensik digital.

1.4. Batasan Masalah

Batasan yang diterapkan pada penelitian ini terbatas pada*:*

1. Penelitian dilakukan pada lingkungan virtual mechine dengan spesifikasi OS Windows 10, *virtual size* 160.00 GB, *actual size* 50 GB
2. *Sandbox* yang digunakan adalah FlareVM v 3.0.1.

3. Objek penelitian ini adalah *malware*
4. Penelitian dilakukan dengan *malware* yang belum terkemas dan dilakukan pengemasan dengan sengaja
5. Pengemasan menggunakan *program packers ultimate packers for executable* (UPX)

Landasan Teori