BAB 1
PENDAHULUAN

1.1 Latar Belakang

Dalam kurun waktu yang baru-baru ini, angka pertumbuhan program-program yang dihasilkan untuk tujuan kriminal dan ilegal telah menunjukkan perkembangan yang pesat. Program – program ini, yang dikenal sebagai *malware*, diciptakan untuk mendukung perkembangan organisasi kejahatan di ranah komputer. Secara khusus, *malware* bertujuan untuk mengambil alih kendali komputer korban dan merampas data pribadi, informasi rahasia, serta data yang memiliki nilai ekonomi. Pertumbuhan yang signifikan dalam prevalensi *malware* yang digunakan untuk aktivitas kriminal ini telah mendorong upaya intensif dalam bidang investigasi forensik digital dan riset keamanan. Pendekatan terhadap analisis *malware* menjadi semakin penting dan memerlukan penggunaan alat – alat analisis yang dapat diandalkan, selain mengandalkan solusi antivirus[1].

Saat ini, ranah forensik *malware* telah menjadi bagian integral dari disiplin forensik komputer. Tujuan yang mendasari bidang forensik *malware* adalah mengenali serta menganalisis jenis-jenis *malware* yang masih belum dikenal. Banyak di antara jenis *malware* ini didesain dengan canggih untuk menghindari deteksi yang dilakukan oleh perangkat lunak antivirus. Oleh karena itu, untuk dapat mengungkapkan dampak serta metode serangan yang diterapkan oleh *malware*, diperlukan kemampuan yang mampu menganalisis dengan mendalam[2].

Perlindungan terhadap kerahasiaan, integritas, dan ketersediaan dalam sistem komputer secara inheren merupakan tugas yang kompleks. Pertambahan jumlah objek sistem dan interaksi yang rumit antara *malware* dan objek sistem semakin mengukuhkan fakta bahwa menciptakan perlindungan yang efektif dan akurat memerlukan investasi waktu yang signifikan dan mampu meminimalkan potensi kesalahan[3].

Dalam konteks penggunaan komputasi sebagai alat penyimpanan data *on-demand*, kompleksitas semakin meningkat seiring dengan risiko yang diakibatkannya, seperti masalah keamanan, perlindungan privasi, kendali akses, dan kerahasiaan data. Upaya penelitian saat ini memiliki fokus dalam mengumpulkan informasi berkenaan dengan teknik-teknik dalam bidang forensik *malware*, dimana hal ini memiliki tujuan untuk menjaga keamanan informasi yang bersifat sensitif. Identifikasi masalah yang muncul terkait dengan aspek keamanan dan privasi dalam *malware* menarik perhatian yang signifikan, dan studi mengenai teknik forensik *malware* membawa dampak positif dalam upaya menjaga keamanan informasi sensitif, permasalahan yang hingga kini masih diperdebatkan[3].

Penting untuk mencatat bahwa, walaupun kemampuan analisis *malware* terhadap solusi antivirus telah mencapai tingkat yang baik, terdapat kecenderungan untuk lebih memusatkan perhatian pada pengembangan alat analisis yang berfokus pada deteksi dari pada pada pelacakan teknik penghindaran yang diterapkan oleh *malware.* Disiplin analisis *malware* sendiri merupakan bagian yang krusial dalam bidang keamanan komputer, yang bertujuan untuk memahami komponen dan perilaku dari jenis *malware*. Terdapat dua metode yang digunakan dalam analisis *malware*, yakni metode analisis statis yang tidak melibatkan eksekusi program dan metode analisis dinamis yang melibatkan eksekusi program *malware*[4].

1.2 Rumusan Masalah

Berdasarkan deskripsi latar belakang, maka dapat dirumuskan beberapa masalah dalam proyek akhir ini yaitu.

1. Bagaimana menganalisis jenis *malware webc2-div* menggunakan forensik?
2. Bagaimana implementasi *reverse engineering* dalam analisa *malware webc2-div*?

1.3 Tujuan

Berdasarkan rumusan masalah, maka tujuan dari proyek akhir ini sebagai berikut.

1. Mengintegrasi data atau keaslian data setelah teridentifikasi *malware webc2-div* dan di *reverse engineering*.
2. Melakukan analisa pada aplikasi apakah teridentifikasi *malware* atau tidak.
3. Melakukan *reverse engineering* untuk mengetahui aktivitas apa saja yang bisa dilakukan *malware* tersebut.

1.4 Batasan Masalah

Adapun yang menjadi batasan dari permasalahan pada proyek akhir ini adalah sebagai berikut.

1. Banyak *malware* yang diciptakan dengan kemampuan menghindari deteksi antivirus.
2. Analisis *malware* lengkap mengenai kemampuan *malware*.
3. Menggunakan *tools* distro *kali linux*, *has generator, ftk imager, software cutter.*
4. Metode yang digunakan adalah analisis statis, metode yang dilakukan tanpa menjalankan *malware*.
5. Identifikasi masalah keamanan dan privasi pada *malware*.