BAB I
PENDAHULUAN

1.1. Latar Belakang

Teknologi komputer sangat dibutuhkan oleh kehidupan manusia terutama personal maupun kelompok (organisasi). Sebuah kelompok (organisasi) memerlukan adanya komputerisasi dalam berbagai kegiatan yang dilakukannya. Sistem komputerisasi tersebut membuat keamanan data-data asset yang dimiliki oleh kelompok lebih terjaga, terutama informasi-informasi dan data-data penting yang bersifat rahasia. (Pabokory, Astuti, & Kridalaksana, 2015).

Perkembangan perangkat lunak yang menangani keamanan data terutama yang bersifat rahasia semakin canggih, terutama dalam keamanan sistem operasi. Jenis sistem operasi yang menerapkan hal tersebut adalah sistem operasi buatan Microsoft, yaitu Windows 10. Windows 10 memiliki fitur keamanan sistem operasi yaitu *Bitlocker Drive Encryption*. BitLocker adalah sebuah fitur enkipsi *full-disk* yang telah tersedia dalam sistem operasi Microsoft Windows khususnya Windows 10, yang didesain untuk melindungi data dengan melakukan enkripsi terhadap keseluruhan partisi. *BitLocker Drive Encryption* menggunakan algoritma *Advanced Encrypted Standart* (AES) dalam mode *Code Block Chaining* (CBC) dengan panjang kunci 128-bit, yang digabungkan dengan *Elephant diffuser* untuk meningkatkan kemanannya (Hamdani & Dwi, 2015). BitLocker dapat menenkripsi banyak media penyimpanan data untuk mencegah orang lain membuka, merusak, memodifikasi, serta penyebaran data baik disengaja maupun tidak disengaja.

BitLocker menyediakan *Recovery Key* dengan kata sandi numerik 48-digit unik yang bisa digunakan untuk membuka kunci sistem jika *password* BitLocker itu sendiri tidak diketahui. *Recovery key* dapat disimpan pada akun Microsoft, dicetak atau disimpan dalam bentuk file. Permasalahan yang akan terjadi adalah ketika pengguna melupakan atau menghilangkan *password* dan *Recovery Key* BitLocker tersebut.

Algoritma *brute force* merupakan algoritma yang dapat memecahkan masalah dengan sangat sederhana, langsung, dan dengan cara yang jelas. Algoritma *brute force* ini dapat digunakan untuk menemukan kembali password yang lupa atau hilang. Penyelesaian permasalahan *password cracking* dengan menggunakan algoritma *brute force* dilakukan dengan cara menempatkan dan mencari semua kemungkinan *password* yang ada dengan menambahkan karakter dan panjang *password* tertentu, hal ini tentunya akan menciptakan banyak sekali kombinasi *password* (Pramudita K. E., 2011).

Hasil penelitian (Pramudita K. E., 2011) tersebut masih memiliki beberapa kekurangan, diantaranya penelitian tersebut hanya berisi penjelasan-penjelasan teknik *brute force attack* dan tidak disertai dengan pembuktian implementasi penerapan *brute force attack* terhadap studi kasusnya. Berdasarkan deskripsi tersebut di dalam penelitian ini akan dilakukan implementasi serta "Analisis Proses *Recovery Password* BitLocker Penyimpanan Data Menggunakan Teknik *Brute Force* Pada Windows 10" untuk menemukan *password* dan *recovery key* BitLocker yang lupa ataupun hilang.

1.2. Rumusan Masalah

Rumusan masalah pada penelitian ini adalah:

a. Bagaimana menganalisis tingkat keamanan fitur Bitlocker *Drive Encryption* terhadap data pengguna Windows 10?
b. Bagaimana melakukan *recovery password* menggunakan teknik *brute Force*?

1.3. Batasan Masalah

a. Sistem operasi yang digunakan dalam penelitian ini adalah Windows 10.
b. Pembuatan *Virtual Hard Drive* pada penelitian ini menggunakan WinImage**.**
c. Proses *Recovery Password* BitLocker menggunakan Passware Kit Forensic 2021.
d. Metode yang digunakan hanya menggunakan metode *brute force*.

1.4. Tujuan Penelitian

a. Menganalisis tingkat keamanan fitur Bitlocker *Drive Encryption* terhadap data pengguna Windows 10.
b. Melakukan *recovery password* menggunakan teknik *brute Force.*

1.5. Manfaat Penelitian

Manfaat dalam penelitian ini adalah sebagai berikut :

a. Mengetahui tingkat keamanan fitur Bitlocker *Drive Encryption*.
b. Membantu pengguna BitLocker ketika tejadi lupa atau kehilangan *password* sehingga *drive* yang terkunci BitLocker bisa dibuka kembali.

1.6. Metodologi Penelitian

Metode penelitian yang digunakan dalam menyusun tugas akhir ini terdiri dari langkah-langkah berikut :

1.6.1. Pengumpulan Data

Pengumpulan data sangat berpengaruh pada proses *recovery* data

1.6.2. Pengujian

Pengujian dilakukan dengan menjalankan aplikasi/program untuk melakukan *recovery* data.

1.6.3. Analisis

Merupakan tahapan analisis pengaruh data, kapasitas, dan *performance* komputer terhadap kecepatan proses *recovery* data.

1.6.4. Evaluasi

Evaluasi dilakukan untuk mengetahui apa saja kekurangan dan kelebihan yang terdapat dalam proses *recovery* data dan untuk mengetahui apakah manfaat yang dicapai sudah sesuai dengan harapan yang diinginkan.

1.7. Sistematika Penulisan

Sistematika penulisan yang dilakukan dalam pembuatan laporan Tugas Akhir ini yaitu sebagai berikut :

BAB I PENDAHULUAN

Bab ini membahas permasalahan umun yang meliputi tentang latar belakang, rumusan masalah, batasan masalah, tujuan pnelitian, manfaat penelitian dan metode penelitian.

BAB II LANDASAN TEORI

Bab ini membahas tentang teoritis yang berhubungan dengan penelitian. Diantaranya teori tentang : *Bitlocker Drive Encryption, Trusted Platform Module,* Algoritma kriptografi, WinImage dan Passware Kit Forensics.

BAB III METODOLOGI

Bab ini membahas tentang metode yang digunakan dalam perancangan teknik recovery data, sumber dan teknik pengumpulan data, serta tahapan-tahapan yang sesuai dengan metode yang digunakan untuk menyelesaikan penelitian.

BAB IV HASIL DAN PEMBAHASAN

Berisikan penjelasan langkah-langkah yang digunakan pada penelitian ini yang telah dijelaskan pada metodologi penelitian, lalu pemaparan hasil pengujian, serta analisa terhadap hasil pengujian dan perbandingannya.

BAB V KESIMPULAN DAN SARAN

Bab ini membahas tentang kesimpulan dari pembahasan masalah dan saran-saran untuk teknik serupa.