BAB 1
Pendahuluan

1.1 Latar Belakang

Perkembangan teknologi pada saat ini sudah sangat pesat, terutama *smartphone*. *Smartphone* telah berkembang dan memiliki banyak fitur yang dapat dimanfaatkan sehari-hari oleh pengguna. Secara lambat laun perkembangan *smartphone* dapat menggantikan peran dari komputer, dilihat dengan banyaknya fitur yang dimiliki smartphone pada saat ini diyakini dapat bersaing dengan komputer suatu saat nanti. Salah satu *smartphone* yang memiliki fitur cukup lengkap yaitu smartphone yang dibekali sistem operasi Android.

Android adalah sistem operasi yang paling banyak digunakan di berbagai kalangan untuk saat ini. Selain digunakan untuk berkomukinasi, Android pada saat ini digunakan sebagai sistem untuk mengakses jaringan dan untuk berkomunikasi antar perangkat multimedia. Hampir semua informasi terekam dalam ponsel, mulai dari informasi sosial, gambar dan video, *history* kehidupan, informasi pribadi dan informasi perbankan seseorang dapat terekam di dalamnya [1]. Android telah memperoleh pangsa pasar yang sangat besar karena arsitekturnya, dan popularitas *application programming interface* (APIs) di dalam komunitas pengembang aplikasi. Android telah berhasil memenangkan jumlah pengguna lebih dari 87% dari pangsa pasar, maka dari itu Android meninggalkan para pesaingnya iOS, Windows Phone OS, dan Blackberry [2]. Sistem operasi android memiliki tingkat keamanan yang cukup baik guna menjaga privasi seseorang, dibeberapa merk smartphone yang beredar saat ini terdapat smartphone yang memiliki pengamanan ganda guna menjaga privasi data seseorang tanpa harus menginstall vault aplikasi terlebih dahulu.

Vault aplikasi merupakan sebuah aplikasi Anti forensics (AF) yang terdapat pada smartphone baik itu Android ataupun iOS, menurut [3] AF adalah serangkaian taktik dan tindakan yang diambil oleh seseorang yang ingin menggagalkan proses investigasi. *Icon* pada aplikasi ini dapat terlihat berbeda-beda, ada yang menyerupai sebuah lemari penyimpanan atau loker, ada yang seperti kalkulator, ada yang meneyerupai seperti aplikasi lain, bahkan ada yang seperti *file manager.* Dalam menggunakan aplikasi ini, seorang pengguna harus mengetik kode sandi yang telah dibuatnya untuk mengakses dan melihat data yang disimpan di dalamnya [4]. Dengan adanya aplikasi tersebut semua orang dapat menyembunyikan data mereka, tidak memandang apakah pengguna itu seorang yang baik atau sebaliknya. Dalam *digital*

investigation, aplikasi vault dapat menghambat pekerja forensik dalam menginvestigasi kasus tersebut guna mendapatkan bukti.

1.2 Rumusan Masalah

Adapun perumusan masalah yang didapat berdasarkan latar belakang, yaitu:

1. Bagaimana cara mengetahui semua data yang disembunyikan melalui aplikasi vault pada perangkat Android *unrooted*?
2. Bagaimana melakukan deteksi data pada aplikasi vault perangkat Android *unrooted* agar semua data dapat terlihat?

1.3 Batasan Masalah

Batasan masalah pada TA ini adalah sebagai berikut:

1. Penelitian ini hanya dilakukan pada perangkat Android Unrooted.
2. Fokus mencari aplikasi anti-forensic yang terinstall di perangkat android unrooted.

1.4 Tujuan Penelitian

Tujuan yang diharapkan dari Tugas Akhir (TA) ini adalah membuat aplikasi pendeteksi aplikasi anti forensik (vault) pada Android yang dapat membantu pekerja forensik dalam menginvestigasi perangkat Android unrooted yang telah terinstall aplikasi anti forensik, sehingga para pekerja forensik dapat mengetahui semua file yang ada baik itu yang tersembunyi ataupun tidak, guna investigasi.

1.5 Rencana Kegiatan

Rencana kegiatan yang akan dilakukan pada TA ini adalah sebagai berikut:

1. Studi literatur

   Tahap awal dari TA ini adalah mencari dan membaca referensi-referensi yang berkaitan dengan topik yang di angkat. Yang menjadi acuan dalam TA ini adalah *conference* dengan judul “Detection and Recovery of Anti-Forensic (Vault) Applications on Android Devices” yang ditulis oleh Michaila Duncan dan Umit Karabiyik.
2. Pengumpulan Data

Pengumpulan data didapatkan dari hasil *testing* beberapa aplikasi vault popular yang ada pada Google play store.

3. Analisis dan Alur Pemodelan

   Analisis dan alur pemodelan menggunakan metode *logical acquisition* guna mengakuisisi data pada perangkat yang menjadi bukti.

4. Implementasi Sistem

   Implementasi sistem dibangun dengan menggunakan bahasa pemrograman python, untuk membandingkan aplikasi vault dan non vault dilakukan dengan menggunakan *command* dasar Android Debug Bridge (ADB).

5. Analisis Hasil Implementasi

   Analisis hasil implementasi yaitu dengan melakukan sejauh mana tools dapat mendeteksi *file* yang berada dalam aplikasi vault pada perangkat Android *unrooted.*

6. Penulisan Proposal

   Semua hasil kegiatan dari pengumpulan data hingga implementasi pada tahap ini akan didokumentasikan dalam bentuk laporan tugas akhir.

1.6 Jadwal Kegiatan

Berikut jadwal pengerjaan Tugas Akhir dapat dilihat pada Tabel 1.

Tabel 1 Jadwal Pengerjaan

Kegiatan	**Bulan**					
	1	2	3	4	5	6
Studi Litelatur						
Pengumpulan Data						
Analisis dan Perancangan Sistem						
Implementasi Sistem						
Analisis Hasil Implementasi						
Penulisan Laporan						