BAB I Pendahuluan

1.1. Latar Belakang

Mobile Phone Forensics merupakan cabang dari forensik digital yang sedang diperdebatkan dikarenakan beberapa *smartphone* menjadi perangkat yang umum digunakan baik untuk personal maupun bisnis[1]. Perdebatan tersebut dikarenakan fokus dari *Mobile Device Forensics* ini menjadi berbeda disebabkan oleh disematkannya sebuah sistem operasi pada *mobile device* terkait sehingga fokus ekstraksi dan analisa data menjadi berbeda dengan perangkat yang tidak disematkan sebuah sistem operasi. Dengan adanya sistem operasi yang disematkan di *smartphone* seperti android, ios, windows phone dan lain sebagainya membuat semua pengguna secara tidak langsung menyimpan beberapa data penting mereka kedalam *smartphone* pengguna saat pengguna menggunakan beberapa fitur yang disediakan pada sistem operasi tersebut. Dan tidak mengherankan juga apabila pengguna *smartphone* yang ada adalah seorang kriminal[2]. Disisi investigator dalam bidang ini, data yang disimpan dalam *smartphone* menyimpan bukti yang sangat penting untuk menyelesaikan sebuah kasus kriminal[2].

Sistem operasi Android sampai pada kuartal ketiga pada tahun 2014 lalu masih berada pada tingkat pertama pada pemasaan global dengan total pengiriman perangkat ber-sistem operasi android mencapai 84,4%[3]. Hal ini membuat penggunaan Android sebagai sistem operasi menjadi dominan dan semakin dominan sistem operasi maka semakin tinggi kemumngkinan penjahat untuk melakukan tindak kejahatan dengan perangkat tersebut maupun menggunakan perangkat tersebut sebagai sarana kejahatan[1]. Salah satu fitur isitimewa yang disediakan sistem operasi android adalah aktivitas *Rooting.* Dengan aktivitas *Rooting* ini membuat pengguna bisa memperoleh hak akses tertinggi untuk memodifikasi sistem sesuai dengan kehendak pengguna dengan resiko merusak sistem yang ada[4]. Disisi investigator forensik digital, menganalisa perangkat android yang sudah ada dalam keadaan *Root* lebih menguntungkan dalam akuisisi data karena para investigator dapat memperoleh semua data dari *smartphone* baik data dari *volatile* maupun *non-volatile memory*. Namun sebaliknya apabila investigator mendapatkan perangkat yang belum mendapatkan hak akses *root* (*unrooted device)* membuat para investigator sedikit mengalami kesulitan dalam memilih teknik akuisisi data yang memungkinkan investigator mendapatkan data yang cukup untuk menyelesaikan suatu kasus kriminal

dikarenakan terbatasnya data yang bisa diakses karena tidak memiliki hak akses tertinggi dalam sistem tersebut.

Metode ekstraksi data pada *mobile forensics* sistem operasi android dibagi menjadi 2 yaitu *physical* dan *logical extraction* dimana setiap metode memiliki teknik akuisisi data yang berbeda[5]. Pada *unrooted device* digunakan metode *logical extraction* untuk ekstraksi data sistem pada perangkat andorid disebabkan oleh terbatasnya data yang bisa diambil melalui perangkat ini karena belum memperoleh hak akses tertinggi. Teknik yang digunakan pada *logical extraction* untuk *unrooted device* antara lain *AFLogical, SD card Imaging, Android Backup Analysis,* dan *Commecial Provider*[5]. Setiap Teknik pada *logical extraction* ini memiliki perbedaan pada jumlah data yang dapat diambil dari perangkat android tersebut dan diperlukan pemilihan teknik yang tepat untuk menghindari perubahan data secara besar pada perangkat yang dapat merusak integritas dari barang bukti perangkat tersebut.

Dengan demikian diperlukan perbandingan untuk setiap teknik akusisi data pada metode *Logical Extraction* ini untuk memudahkan investigator dalam memilih teknik yang tepat untuk keperluan investigasi pada barang bukti digital.

1.2. Perumusan masalah

Dalam Tugas Akhir ini dirumuskan masalah berdasarkan latar belakang diatas, yaitu sebagai berikut :

a. Teknik akuisisi data apa yang tepat (tanpa melakukan *rooting* dan sebisa mungkin tidak melakukan instalasi aplikasi dengan data yang diambil cukup untuk dijadikan barang bukti) digunakan untuk aktivitas *mobile forensics* pada *unrooted android device.*
b. Data dan *artifacts* aplikasi apa saja yang bisa diambil untuk setiap teknik akuisisi data yang dipakai pada *unrooted android device.*

1.3. Batasan Masalah

Adapun batasan masalah yang muncul pada tugas akhir ini yaitu :

a. Perangkat yang digunakan untuk aktivitas *mobile forensics* adalah perangkat android dengan hak akses terbatas(*unrooted device).*
b. Perangkat android yang akan dianalisa tidak dienkripsi.

c. Studi kasus aplikasi yang akan dilakukan aktivitas *mobile forensics* adalah aplikasi *Steam mobile* dengan fokus studi kasus log komunikasi pada aplikasi tersebut.
d. Teknik akusisi yang akan dibandingkan adalah teknik *AFLogical, SDcard imaging, Android backup analysis,* dan *Commercial Provider* dengan aplikasi *Oxygen-Forensics.*
e. Pada Tugas Akhir ini akan difokuskan untuk melakukan perbandingan data yang dapat diambil dan jumlah aktivitas yang dilakukan pada barang bukti perangkat untuk menentukan teknik yang tepat untuk dilakukan aktivitas *mobile forensics* pada perangkat android.

1.4. Tujuan

Adapun tujuan yang ingin dicapai pada tugas akhir ini yaitu :

a. Menentukan teknik akuisisi data yang tepat (tanpa melakukan *rooting* dan sebisa mungkin tidak melakukan instalasi aplikasi data yang diambil cukup untuk dijadikan barang bukti) digunakan untuk aktivitas *mobile forensics* pada *unrooted android device.*
b. Mengetahui data *artifacts* aplikasi apa saja yang dapat diambil untuk setiap teknik akuisisi data yang diapakai pada *unrooted android device.*

1.5. Hipotesa

Hipotesa : Akuisisi data dengan metode *logical extraction* dengan teknik *Android Backup Analysis* adalah teknik yang paling aman dan tepat untuk aktivitas *mobile device forensics* sesuai studi kasus yang ada dimana dengan teknik ini *artifacts* aplikasi yang dibutuhkan didapatkan dan merupakan teknik dimana aktivitas yang dilakukan pada *device* yang paling minimal.

1.6. Metode Penelitian

Metode penelitian yang dilakukan untuk implementasi pada tugas akhir ini adalah :

a. Studi Literatur

   Pada tahap ini dilakukan pendalaman teori dan konsep yang dibutuhkan dalam melakukan tugas akhir ini. Diantaranya mempelajari literatur-literatur yang relevan dengan permasalahan meliputi :

   1) *Mobile device Forensics*
   2) *Logical Extraction*
   3) *Steam*

b. Analisis dan Perancangan Sistem

   Pada Tahap ini dilakukan perancangan untuk membuat lingkungan kerja *mobile device forensics* yang kemudian melakukan analisa perbandingan teknik akuisisi data pada *Unrooted Android Device* dengan metode *Logical Extraction* dengan studi kasus aplikasi *Steam Mobile*.

c. Implementasi

   Tahap ini merupakan tahap implementasi dari perancangan sistem dimana akan dilakukan instalasi aplikasi *Steam Mobile* pada perangkat yang akan dianalisa dan kemudian akan dilakukan akuisisi data dengan menggunakan teknik *AFLogical, SDcard Imaging, Android Backup Analysis, dan Commercial Provider* dengan aplikasi *Oxygen-forensics.*

d. Pengujian dan Analisis Hasil Implementasi

   Dalam tahap ini pengujian dilakukan dengan mencatat *artifacts* aplikasi *Steam Mobile* apa saja yang dapat diambil dan aktivitas yang dilakukan pada perangkat pada setiap teknik yang dilakukan. Analisis pada tahap ini dilakukan dengan membandingkan *artifacts* aplikasi yang dapat diambil dan aktivitas yang dilakukan pada perangkat dari hasil pengujian dan diambil sebuah kesimpulan mengenai teknik yang tepat untuk digunakan pada aktivitas *mobile device forensics*.

e. Penyusunan Laporan Tugas Akhir

   Pada Tahap ini dilakukan penarikan kesimpulan dari hasil analisis dan pengujian yang dilakukan. Kemudian dilakukan dokumentasi semua tahapan proses diatas berupa laporan yang berisi tentang dasar teori dan hasil Tugas Akhir ini kedalam sebuah buku tugas akhir.

1.7. Jadwal Kegiatan

Tabel 1.1 Jadwal Kegiatan

Kegiatan	Bulan 1	Bulan 2	Bulan 3	Bulan 4
Studi Literatur dan Pengumpulan data				
Perancangan Sistem				
Implementasi				
Pengujian dan Analisis hasil				
Penyusunan Laporan Tugas Akhir				