BAB I
PENDAHULUAN

1.1 Latar Belakang

Teknologi informasi dan komunikasi memiliki peranan penting dalam kehidupan saat ini, kemajuan teknologi informasi seperti pisau bermata dua, yang memiliki dampak positif pada penggunanya seperti menigkatkan produktivitas, efisiensi, dan efektifitas kerja. Kemudian disisi lain penggunaan teknologi informasi juga bisa memberikan fasilitas tindak kejahatan didunia maya, maka dari itu diperlukan suatu alat untuk memberikan analisa serta pembuktian kasus kejahatan tersebut.

Pada data *ID-Cert* tahun 2010 – 2016, berbagai macam kasus pelanggaran *UU ITE* yang berhubungan dengan *cyber crime* dan *cyber security* pada saat ini semakin banyak bermunculan, dari pencemaran nama baik perusahaan maupun perorangan serta penghinaan dimedia sosial, dan ada juga kasus pembunuhan berencana yang dibuktikan dengan memanfaatkan mobile forensics (ID-Cert. 2016).

Penanganan kasus *cyber crime* tidak lepas dari pendekatan terkordinasi dan terstruktur dari seorang *Investigator* atau lebih sering disebut dengan *incident response* yang meliputi kegiatan seperti konfirmasi insiden apa yang terjadi, memberikan penangan serta deteksi cepat, menentukan dan mendokumentasikan sampai dengan memungkinkan tindak pindana atau perdata terhadap pelaku atau saksi ahli (Mandia K, 2014).

Salah satu metode investigasi yang digunakan saat ini adalah dengan menggunakan pendekatan metode *remote forensics*, yaitu dengan cara pengambilan data atau akuisisi dilakukan secara remote melalui media jaringan kabel atau nirkabel dengan sistem kerja yaitu menyisipkan *backdooring* (agent) kepada *client* atau *corporate* yang dijalakan secara remote agar tercipta suatu *flow*

(aliran) yang sudah dikonfigurasi dengan infrastruktur server yaitu dengan menggunakan *GRR Rapid Repsonse.*

GRR merupakan singkatan dari *Google Rapid Response* merupakan sebuah *Framework Multi-platform* yang dibangun dan *dideploy* oleh *staff incident response (IR) Google,* serta mendapatkan popularitas sebesar 20% sampai dengan sepenuhnya didukung oleh komunitas *opensource*. Motivasi utama dalam membangun *GRR* adalah untuk meningkatkan kesiapan analisa serta investigasi, dengan menurunkan biaya investigasi dan menigkatkan kualitas bukti digital yang diperoleh, dengan fitur utama yaitu melakukan *collecting data* terhadap *system agent* yang akan dianalisa melalui media remote, serta memiliki fitur detail monitoring dari *CPU Client,* memori, penggunaan I/O dan lain-lain (Moser, A., & Cohen, M. I. 2013)

1.2 Rumusan Masalah

Dari latar belakang tersebut, maka dapat ditentukan beberapa rumusan masalah, diataranya sebagai berikut:

1. Bagaimana menganalisa karakteristik fitur yang terdapat pada *GRR Rapid Response* ?
2. Bagaimana merancang *GRR Server* agar bisa melakukan akuisisi data browser pada agent /client melalui metode *Remote Live Forensics* ?
3. Bagaimana mengimplementasi *GRR Server* untuk keperluan investigasi ?

1.3 Batasan Masalah

Batasan masalah yang digunakan dalam tugas akhir ini adalah :

1. *Framework GRR Server* dibangun dan dikonfigurasi pada Sistem Operasi Ubuntu 16.04 LTS (64-bit)
2. Server dan Agent diinstall pada *Vmware Workstation*.

3. Client (Agent) meliputi Sistem Operasi : Windows 7 (64-bit), Windows Server 2008 (32-bit), Ubuntu 12.04 (32-bit), OpenSUSE (32-bit), Redhat (32-bit), Centos (32-bit), dan Kali linux (32-bit).
4. Tidak melakukan simulasi pada mode *private browser*
5. Fokus Pengembangan *GRR Server* ini hanya dalam ruang lingkup Browser, yaitu dengan melakukan pengembangan modul *YAML* pada *Artifact manager* yang disediakan oleh *GRR Server*.
6. Browser yang digunakan meliputi *Google Chrome, Mozilla Firefox, Safari dan Internet Explorer.*

1.4 Tujuan Penelitian

Berdasarkan rumusan masalah yang telah dibuat sebelumnya, berikut dikemukakan beberapa tujuan yang ingin dicapai pada penelitian ini sebagai berikut:

a. Mempelajari serta mengenali karakteristik fitur yang terdapat pada *GRR Server.*
b. Merancang *Framework GRR server* dengan menggunakan metode *Remote Live Forensics.*
c. Mengimplementasikan *Framework GRR Server* untuk keperluan Investigasi khususnya akuisisi data pada browser.

1.5 Manfaat Penelitian

Adapun manfaat yang diperoleh dari penelitian ini adalah sebagai berikut:

a) Bagi Perguruan Tinggi

1. Menambah referensi terkait dengan pengetahuan *Digital Forensics*.
2. Menambah referensi terkait metode *Remote live forensics.*

3. Menambah wawasan bagi pembaca, khususnya yang berminat untuk mengembangkan tools dan *Framework* Forensik Insident Respon.

b) Bagi Penulis

Dengan adanya penelitian ini penulis mendapatkan kesempatan untuk memahami lebih dalam tentang metode akuisisi data dalam dunia *Digital Forensics.*

1.6 Metodologi Penelitian

Metode penelitian yang digunakan dalam penelitian ini sebagai berikut:

1. Studi Literatur

Studi Literatur dilakukan dengan cara mempelajari buku, jurnal, halaman web yang berkaitan dengan teknologi dan metode yang digunakan, dan panduan manual perangkat lunak yang digunakan. Hal ini bertujuan untuk mencari referensi dan memperluas wawasan terkait dengan tugas akhir yang dikerjakan.

2. Analisis Masalah

Pada tahap ini pekerjaan yang dilakukan adalah menganalisis masalah dan menentukan solusi yang dapat digunakan dalam menyelesaikan masalah yang dihadapi.

3. Perancangan Sistem

Pada tahap ini penulis melakukan perancangan sistem yang diperlukan dengan membuat suatu topologi jaringan yang dapat memenuhi proses jalanya solusi yang telah ditentukan.

4. Pembuatan Artifact

Pada tahap ini penulis melakukan penambahan modul artifact yang disupport dalam format *GRR* yaitu *YAML*, fokus pengembangan *Artifact* yaitu pada modul akusisi browser seperti Program browser *Internet Explorer, Safari, Chrome cache, Opera* dan *Mozilla firefox*.

5. Implementasi Sistem

Tahapan ini merupakan proses pengerjaan dari peracangan sistem yaitu melakukan proses akuisisi (*Hunting*) dengan memanfaatkan modul *Artifact YAML* yang sudah ditambahkan kedalam sistem *GRR*.

6. Penarikan Kesimpulan

Dari hasil implementasi sistem dan metode yang digunakan, maka dilakukan penarikan kesimpulan untuk menunjukkan hasil akhir yang didapat dari proses akuisisi secara keseluruhan dalam tugas akhir ini.

7. Penulisan Laporan

Tahapan ini merupakan tahapan akhir dimana semua hasil dari implementasi sistem dan metode yang digunakan serta hasil dari penarikan kesimpulan dikumpulkan dalam bentuk laporan.

1.7 Sistematika Penulisan Laporan

Dalam penyusunan tugas akhir ini, sistematika penulisan dibagi menjadi beberapa bab sebagai berikut:

BAB I PENDAHULUAN

Bab ini berisi tentang gambaran umum penelitian yang terdiri dari latar belakang masalah, maksud dan tujuan, batasan masalah, metode, dan sistematika penulisan tugas akhir.

BAB II LANDASAN TEORI

Bab ini membahas dasar teori yang digunakan berdasarkan permasalahan yang berkaitan dengan dengan penelitian, meliputi konsep dasar dan definisi dari komputer forensik, *digital evidance,* akuisisi data, metode akuisisi data, pengantar *GRR Server*, arsitektur *GRR* dan pengantar dasar *artifact* serta materi-materi yang yang berhubungan dengan sistem yang digunakan.

BAB III METODOLOGI

Bab ini membahas tentang uraian metode analisis yang digunakan untuk penyelesaian penelitian tentang kebutuhan perangkat lunak yang diperlukan untuk menjalankan sistem *Google Rapid Response*, perancangan sistem, dan perancangan artifact.

BAB IV HASIL DAN PEMBAHASAN

Pada bagian ini membahas tentang pengujian implementasi dari perancangan sistem dan perancangan artifact serta membahas kinerja untuk mendapatkan hasil pengujian sistem.

BAB V PENUTUP

Pada bab ini terdapat beberapa kesimpulan yang didapatkan dari bab-bab sebelumnya. Bab ini juga berisi saran-saran yang diperlukan yang nantinya dapat digunakan dalam pengembangan *Google Rapid Response* sebagai *Framework* Insiden Respon pada akuisisi data *Remote Live Forensics.*