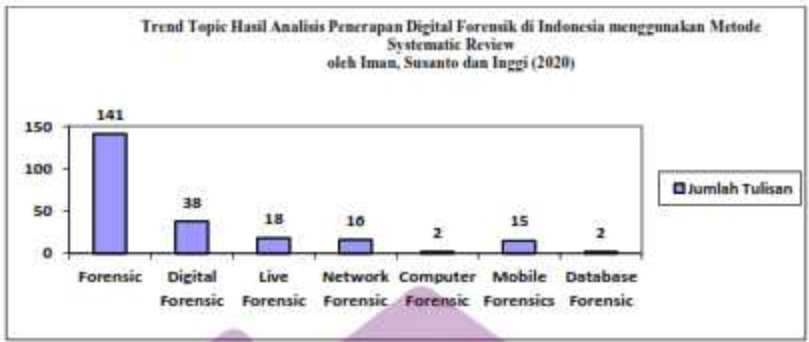
BAB I
PENDAHULUAN

1.1 Latar Belakang

Metode aktivitas kejahatan di dunia maya menjadi semakin berkembang seiring dengan perkembangan teknologi yang ada saat ini sehingga metode pencegahan juga selalu diupayakan agar bisa berguna untuk mendukung proses investigasi hukum yang berlaku[1]. Digital forensik yang juga sering disebut sebagai komputer forensik merupakan salah satu cabang dari ilmu forensik yang menangani bukti-bukti digital legal yang digunakan dalam suatu kejahatan forensik terutama bukti-bukti yang masih melekat pada media penyimpanan komputer maupun media penyimpanan lainnya[2]. Digital forensik dilandasi oleh praktik pengumpulan artefak atau data digital, analisis data digital dan pelaporan hasil investigasi yang pada penerapannya memiliki metode yang sangat beragam. Ilmu digital forensik ini sediri merupakan salah satu cabang dari ilmu forensik yang muncul sebagai respon terhadap perilaku kriminal, perilaku ilegal, dan perilaku tidak pantas[3].

Iman, Susanto dan Inggi (2020), melakukan penelitian analisa pada artikel reviewnya "Analisa Perkembangan Digital Forensik dalam Penyelidikan *Cybercrime* di Indonesia (*Systematic Review)*" berdasarkan pencarian jurnal di tiga sumber yaitu Garba Rujukan Digital (GARUDA), *Science and Technology Index* (SINTA) dan RAMA *Repository* dengan kata kunci "*forensic*", "*digital forensic*", "*live forensic*", "*network forensic*", "*computer forensic*", "*mobile forensic*" dan "*database forensic*" menggunakan sistem *systematic review* menyimpulkan bahwa kejahatan yang paling banyak ditemui dan ditangani dalam penerapan sub digital forensik di Indonesia adalah kejahatan yang berkaitan dengan metode *live forensic*. Hasil analisis bisa dilihat pada gambar 1.1 Grafik *Trend Topic* [1].



Gambar 1. 1 Grafik *Trend Topic*

Live forensic merupakan salah satu metode analisis digital forensik yang muncul sebagai respon terhadap kekurangan yang ada pada metode *static forensic* karena bisa memberikan informasi yang lebih lengkap dalam hal menemukan data-data sementara (data *volatile*) pada *Random Access Memory* (RAM) jika dibandingkan dengan analisis secara statik (*static forensic*) seperti misalnya aktivitas *memory, running processes, network processes*, dan lain-lain, karena dilakukan secara langsung pada sistem yang sedang berjalan[4]. Saat ini *live forensic* sudah bisa juga dilakukan dari jarak jauh yang juga dikenal sebagai *remote live forensic* dengan menggunakan *framework GRR Rapid Response* yang berarsitektur *client-server* agar aktivitas forensik dan investigasi dapat dilakukan dalam waktu yang lebih cepat dan berskala sehingga analisis dan triase terhadap serangan dapat segera dilakukan dari jarak jauh[5].

Dalam pemilihan metode tahapan-tahapan forensik perlu mempertimbangkan beberapa kriteria diantaranya harus memenuhi *individuality, repeatability, reliability, performance, testability, scalability,* dan *quality standards*[6]. Metode analisis yang digunakan pada penelitian ini adalah metode *National Institute of Standards and Technology* (NIST) yang memiliki empat tahapan yaitu *Collection, Examination, Analysis,* dan *Reporting*[7]. Penelitian dilakukan menggunakan skenario kasus *remote live forensic* yang akan disimulasikan untuk menemukan dan menganalisis artefak data *volatile* pada *Random Access Memory* (RAM) dari jarak jauh dengan menggunakan *framework GRR Rapid Response* dengan menerapkan metode NIST.

1.2 Rumusan Masalah

Berdasarkan latar belakang yang telah disampaikan, maka dirumuskanlah suatu permasalah penelitian yang akan dipecahkan/diselesaikan pada penelitian ini yaitu :

1. Bagaimana proses *live forensic* jarak jauh dilakukan pada *Random Access Memory* (RAM) menggunakan *framework GRR Rapid Response*?
2. Bagaimana performa atau tingkat keberhasilan *framework GRR Rapid Response* dalam menemukan dan menganalisa data *volatile* pada *Random Access Memory* (RAM)?

1.3 Batasan Masalah

Berdasarkan identifikasi masalah yang telah diuraikan, agar pembahasan tidak meluas dan menyimpang dari pokok bahasan, maka diperlukan batasan masalah penelitian ini sebagai berikut:

1. Metode analisis yang digunakan untuk menjelaskan tahapan-tahapan forensik yang akan dilakukan adalah *National Institute of Standards and Technology* (NIST).
2. *Framework live forensic* jarak jauh yang digunakan adalah *framework GRR Rapid Response* pada *server Linux Ubuntu 18.04* dengan *client Windows 10 Pro* dan *Linux Ubuntu 18.04*.
3. Penelitian dilakukan pada skenario kasus *dummy* terkait pelanggaran *standards operation procedure* (SOP) penggunaan komputer oleh karyawan dari suatu perusahaan yang dibuat dan disimulasikan untuk menemukan dan menganalisis data *volatile* pada *Random Access Memory* (RAM) dari jarak jauh.
4. *Live forensic* dilakukan dari jarak jauh dengan skenario bahwa perusahaan memang sudah menggunakan layanan *framework GRR Rapid Response* sejak awal untuk memantau kinerja para karyawan, sehingga aplikasi *client* dan *server* sejak awal sudah terinstal dan berjalan pada latar belakang perangkat terkait.

5. Tujuan dari penelitian ini adalah untuk melakukan percobaan *live forensic* jarak jauh dan menentukan persentase tingkat keberhasilan *framework GRR Rapid Response* untuk menemukan data *volatile* pada *Random Access Memory* (RAM) dengan sistem operasi *Windows 10 Pro* dan *Linux Ubuntu 18.04*.
6. Persentase tingkat keberhasilan *framework GRR Rapid Response* dalam menemukan data *volatile* pada skenario kasus *live forensic* jarak jauh ditentukan dengan menghitung persentase tingkat keberhasilan rata-rata dengan metode persamaan indeks tidak tertimbang.

1.4 Maksud dan Tujuan Penelitian

Berdasarkan rumusan masalah yang telah diuraikan, maksud dan tujuan yang hendak dicapai dari penelitian ini yaitu:

1. Melakukan percobaan *live forensic* jarak jauh menggunakan *framework GRR Rapid Response* untuk menemukan dan menganalisis data *volatile* pada *Random Access Memory* (RAM).
2. Menentukan performa atau tingkat keberhasilan *framework GRR Rapid Response* dalam menemukan data *volatile* pada *Random Access Memory* (RAM) berdasarkan hasil analisis *live forensic* jarak jauh.

1.5 Manfaat Penelitian

Berdasarkan maksud dan tujuan penelitian yang telah diuraikan, maka manfaat penelitian yang hendak dicapai dari penelitian ini sebagai berikut:

1. Memberikan pemahaman dan pengenalan akan penggunaan *framework GRR Rapid Response* dalam menemukan dan menganalisis data *volatile* dari jarak jauh secara *live forensic* pada *Random Access Memory* (RAM) menggunakan metode analisis *National Institute of Standards and Technology* (NIST).
2. Memberikan rekomendasi solusi dalam meningkatkan kecepatan dan efisiensi proses investigasi berdasarkan hasil pengujian tingkat keberhasilan *framework GRR Rapid Response* dalam menemukan data

volatile dari jarak jauh secara *live forensic* yang berpotensi menjadi bukti digital pada *Random Access Memory* (RAM).

1.6 Metode Penelitian

Metode-metode yang digunakan untuk mendukung jalannya penelitian ini sebagai berikut:

1.6.1 Metode Pengumpulan Data

Metode pengumpulan data yang dilakukan untuk mendukung proses penyusunan skripsi ini sebagai berikut:

1. Metode uji coba/eksperimen, yaitu melakukan percobaan analisis *live forensic* jarak jauh dengan *framework GRR Rapid Response* untuk memperoleh data faktual berupa persentase tingkat keberhasilan dalam menemukan data *volatile* pada *Random Access Memory* (RAM) yang berpotensi menjadi bukti digital.

2. Metode studi pustaka, yaitu melakukan kajian pustaka pada sumber-sumber informasi terpercaya antara lain buku, artikel ilmiah/paper jurnal, dan internet yang digunakan untuk mendukung proses penelitian dan penyusunan laporan penelitian ini.

1.6.2 Metode Analisis

Metode analisis yang digunakan dalam menyusun skripsi ini adalah *National Institute of Standards and Technology* (NIST) yang memiliki empat tahapan, yaitu *Collection* (pengumpulan), *Examination* (pengujian), *Analysis* (penganalisisan) dan *Reporting* (pelaporan) [7] yang selanjutnya akan divalidasi menggunakan teknik validasi *repeatability* dan validasi *reproducibility*[8].

Hasil akhir analisis akan disajikan dalam bentuk persentase tingkat keberhasilan rata-rata dengan metode persamaan indeks tidak tertimbang[9].

1.7 Sistematika Penulisan

Adapun sistematika penulisan yang memuat uraian secara garis besar isi penelitian ini untuk tiap-tiap bab sebagai berikut:

BAB I PENDAHULUAN

Bab ini berisi tentang pendahuluan dari penelitian yang disusun berupa latar belakang masalah, rumusan masalah, batasan masalah, maksud dan tujuan penelitian, manfaat penelitian, metode penelitian, beserta sistematika penulisan.

BAB II LANDASAN TEORI

Bab ini menguraikan teori-teori yang berkaitan langsung dengan ilmu atau masalah yang diteliti yang dapat membantu pengolahan data serta penyusunan laporan penelitian berupa kajian pustaka dan dasar teori.

BAB III METODOLOGI PENELITIAN

Bab ini membahas tentang proses pelaksanaan penelitian ilmiah yang dilakukan, terdiri dari langkah-langkah yang juga menerapkan prinsip metode ilmiah, kebutuhan perangkat lunak dan perangkat keras, bahan penelitian yang digunakan, serta desain antarmuka *tools* yang digunakan.

BAB IV HASIL DAN PEMBAHASAN

Bab ini berisi inti dari sebuah penelitian ilmiah, pada langkah ini hipotesis yang diajukan akan dinyatakan diterima atau ditolak serta pembahasan alasannya untuk menentukan hasil analisis dan evaluasi yang permasalahan yang diteliti.

BAB V PENUTUP

Bab ini berisi kesimpulan akhri dari semua proses penelitian terhadap hasil penerapan metode dan saran yang harus diperhatikan selama penelitian karena adanya berbagai keterbatasan pada penelitian dan rekomendasi untuk pengembangan penelitian selanjutnya.