LIVE FORENSIC JARAK JAUH PADA RANDOM ACCESS MEMORY (RAM) MENGGUNAKAN FRAMEWORK GRR RAPID RESPONSE

SKRIPSI

disusun oleh

Yerri Bonyu Canno

18.83.0138

PROGRAM SARJANA
PROGRAM STUDI TEKNIK KOMPUTER
FAKULTAS ILMU KOMPUTER
UNIVERSITAS AMIKOM YOGYAKARTA
YOGYAKARTA

2022

LIVE FORENSIC JARAK JAUH PADA RANDOM ACCESS MEMORY (RAM) MENGGUNAKAN FRAMEWORK GRR RAPID RESPONSE

SKRIPSI

untuk memenuhi sebagian persyaratan
mencapai gelar Sarjana
pada Program Studi Teknik Komputer

disusun oleh

Yerri Bonyu Canno

18.83.0138

PROGRAM SARJANA
PROGRAM STUDI TEKNIK KOMPUTER
FAKULTAS ILMU KOMPUTER
UNIVERSITAS AMIKOM YOGYAKARTA
YOGYAKARTA
2022

PERSETUJUAN

SKRIPSI

LIVE FORENSIC JARAK JAUH PADA RANDOM ACCESS MEMORY (RAM) MENGGUNAKAN FRAMEWORK GRR RAPID RESPONSE

yang dipersiapkan dan disusun oleh

Yerri Bonyu Canno

18.83.0138

telah disetujui oleh Dosen Pembimbing Skripsi

pada tanggal 20 Januari 2022

Dosen Pembimbing,

Joko Dwi Santoso, M.Kom.

NIK. 190302181

PENGESAHAN

SKRIPSI

LIVE FORENSIC JARAK JAUH PADA RANDOM ACCESS MEMORY (RAM) MENGGUNAKAN FRAMEWORK GRR RAPID RESPONSE

yang dipersiapkan dan disusun oleh

Yerri Bonyu Canno

18.83.0138

telah dipertahankan di depan Dewan Penguji
pada tanggal 20 Januari 2022

Susunan Dewan Penguji

Nama Penguji	Tanda Tangan
Melwin Syafrizal, S.Kom., M.Eng. **NIK. 190302105**	_____
Muhammad Rudyanto Arief, M.T. **NIK. 190302098**	_____
Joko Dwi Santoso, M.Kom. **NIK. 190302181**	_____

Skripsi ini telah diterima sebagai salah satu persyaratan
untuk memperoleh gelar Sarjana Komputer
Tanggal 20 Januari 2022

DEKAN FAKULTAS ILMU KOMPUTER

Hanif Al Fatta, M.Kom.
NIK. 190302096

PERNYATAAN

Saya yang bertandatangan dibawah ini menyatakan bahwa, skripsi ini merupakan karya saya sendiri (ASLI), dan isi dalam skripsi ini tidak terdapat karya yang pernah diajukan oleh orang lain untuk memperoleh gelar akademis di suatu institusi pendidikan tinggi manapun, dan sepanjang pengetahuan saya juga tidak terdapat karya atau pendapat yang pernah ditulis dan/atau diterbitkan oleh orang lain, kecuali yang secara tertulis diacu dalam naskah ini dan disebutkan dalam daftar pustaka.

Segala sesuatu yang terkait dengan naskah dan karya yang telah dibuat adalah menjadi tanggungjawab saya pribadi.

Yogyakarta, 2 Januari 2022

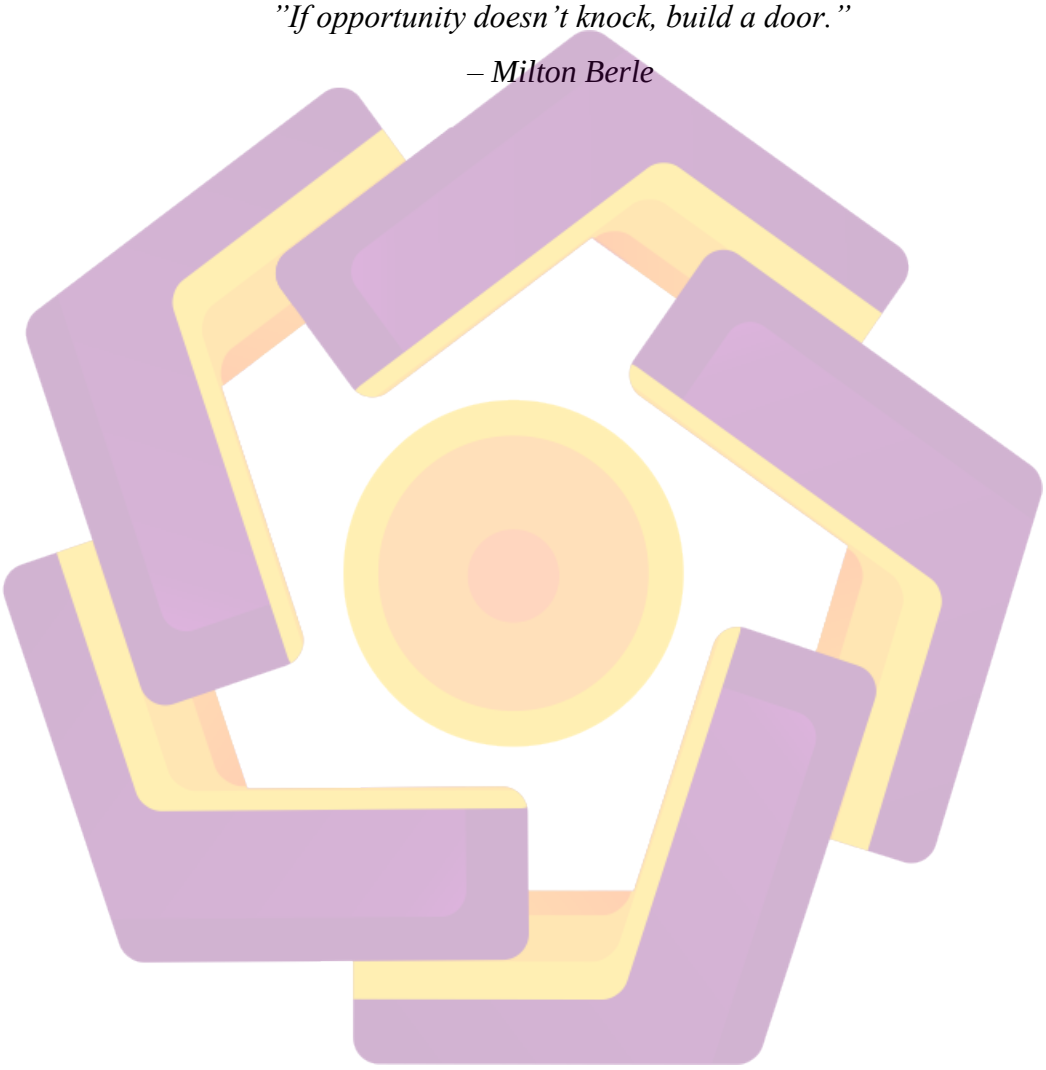
Yerri Bonyu Canno

NIM. 18.83.0138

MOTTO

” If you have faith as small as a mustard seed, you can say to this mountain, ‘Move from here to there,’ and it will move. Nothing will be impossible for you.”
(Matthews 17:20)

”If opportunity doesn’t knock, build a door.”
– Milton Berle



PERSEMBAHAN

Untuk-Dia & mereka yang telah mengasihiku,

They mean the world to me.

KATA PENGANTAR

Puji dan syukur penulis haturkan kepada Allah yang Mahabaik, karena kasih dan kebaikan-Nya, penulis pada akhirnya dapat menyelesaikan skripsi ini. Penulis meyakini bahwa skripsi ini tidak akan berhasil diselesaikan tanpa pertolongan dan kebaikan Allah. Skripsi ini adalah tugas akhir untuk memenuhi persyaratan akademis guna memperoleh gelar Sarjana Strata Satu (S-1) Ilmu Komputer pada Fakultas Ilmu Komputer Universitas Amikom Yogyakarta.

Penulis merasakan kebaikan dan pertolongan Allah melalui banyak pihak yang dengan berbagai cara telah mendukung dan membantu penulis dalam penulisan skripsi ini. Oleh karena itu, penulis menyampaikan ungkapan terima kasih kepada:

1. **Bapak Prof. Dr. Suyanto, MM.** selaku Rektor Universitas Amikom Yogyakarta yang telah memberikan kesempatan kepada penulis untuk menempuh pendidikan di Universitas Amikom Yogyakarta.
2. **Bapak Joko Dwi Santoso, M.Kom.** selaku dosen pembimbing yang telah memberikan dukungan, arahan dan bimbingan untuk penulis sehingga penulis dapat segera menyelesaikan skripsi ini.
3. **Bapak Hanif Al Fatta, M.Kom.** selaku Dekan Fakultas Ilmu Komputer Universitas Amikom Yogyakarta.
4. **Bapak Dony Ariyus, S.S.,M.Kom.** selaku Ketua Program Studi Teknik Komputer Universitas Yogyakarta yang telah mendukung penulis beserta para mahasiswa prodi Teknik Komputer lainnya selama belajar di Prodi ini.
5. **Para Dosen** di Fakultas Ilmu Komputer Universitas Amikom Yogyakarta, yang telah mendidik dan membekali penulis dengan berbagai disiplin ilmu selama belajar di Fakultas ini.
6. **Para Staff dan Student Staff DAAK bagian Pengajaran** di Universitas Amikom Yogyakarta yang telah mendukung dan memberikan inspirasi kepada penulis selama menjadi Student Staff sehingga penulis bisa segera menyelesaikan skripsi ini.

7. **Orang tua, adik, sepupu, seluruh keluarga, pacar serta sahabat** yang senantiasa mendukung penulis melalui doa, nasihat dan perhatian.

Akhirnya, penulis menyadari bahwa skripsi ini belumlah sempurna. Oleh karena itu, penulis dengan rendah hati menerima segala koreksi, kritik dan saran yang membangun dari pembaca sekalian.

Yogyakarta, 1 Januari 2022

Penulis

Yerri Bonyu Canno

DAFTAR ISI

DAFTAR TABEL

DAFTAR GAMBAR

INTISARI

Random Access Memory (RAM) pada dasarnya menyimpan data yang menggambarkan semua aktivitas yang sedang berjalan pada sistem. Data *volatile* merupakan data sementara yang akan terhapus secara permanen ketika sistem dimatikan, sehingga untuk memperoleh bukti digital forensik yang berupa data *volatile* hanya bisa dilakukan dengan menggunakan teknik *live forensic*. Namun, teknik *live forensic* sendiri memiliki kondisi tertentu agar investigasi dapat segera dijalankan, yaitu investigasi harus dijalankan langsung pada komputer target dalam keadaan hidup, sedangkan tidak semua kondisi memungkinkan hal ini terjadi. Oleh karena itu untuk menjawab permasalahan yang disebabkan oleh batasan jarak dan waktu, maka perlu dilakukan *live forensic* jarak jauh sehingga investigasi dapat segera dilakukan.

GRR Rapid Response merupakan kerangka kerja yang akan digunakan dalam memberikan tanggapan terhadap insiden yang difokuskan pada forensik jarak jauh dan dilakukan secara langsung pada sistem komputer yang sedang berjalan. Metode *National Institute of Standards and Technology* (NIST) akan digunakan untuk menjelaskan bagaimana tahapan-tahapan forensik yang akan dilakukan sehingga dapat diketahui alur penelitian secara sistematis, dan dapat dijadikan acuan dalam menyelesaikan permasalahan yang ada.

Hasil penelitian ini menunjukkan persentase tingkat keberhasilan *Framework GRR Rapid Response* dalam menemukan data *volatile* pada RAM dari jarak jauh secara *live forensic* sebesar 100% pada *client Windows* dan 85,7% pada *client Linux.*

Kata Kunci: *Live Forensic, GRR Rapid Response*, *Random Access Memory*, Data *Volatile*, NIST

ABSTRACT

Random Access Memory (RAM) basically is saving data that describes all activities currently running on the system. Volatile data is temporary data that will be permanently deleted when the system is turned off, so that obtaining digital forensic evidences in the form of volatile data can only be done using live forensic techniques. However, the live forensic technique itself has certain conditions so that the investigation can be carried out immediately, namely the investigation must be carried out directly on the target computer in a live state, while not all conditions allow this to happen. Therefore, to answer the problems caused by distance and time constraints, it is necessary to conduct remote live forensic so that investigations can be carried out immediately.

GRR Rapid Response is a framework that will be used in providing incident response that is focused on remote forensic and carried out directly on a live computer system. The National Institute of Standards and Technology (NIST) method will be used to explain how the forensic stages will be carried out so that the research flow can be systematically identified, and can be used as a reference in solving existing problems.

The results of this study indicate the percentage success rate of the GRR Rapid Response Framework in finding volatile data in RAM remotely using live forensic are 100% on Windows client and 85,7% on Linux client.

Keyword: *Live Forensic, GRR Rapid Response, Random Access Memory, Volatile Data, NIST*