

ANALISIS OVERCLOCKING KARTU GRAFIS KOMPUTER

UNTUK MELAKUKAN CRACKING PASSWORD

SKRIPSI

untuk memenuhi sebagian persyaratan
mencapai derajat Sarjana
pada Program Studi Informatika



disusun oleh

Yudhi Agus Triyono

17.21.1110

**PROGRAM SARJANA
PROGRAM STUDI INFORMATIKA
FAKULTAS ILMU KOMPUTER
UNIVERSITAS AMIKOM YOGYAKARTA
YOGYAKARTA
2019**

ANALISIS OVERCLOCKING KARTU GRAFIS KOMPUTER

UNTUK MELAKUKAN CRACKING PASSWORD

SKRIPSI



disusun oleh

Yudhi Agus Triyono

17.21.1110

**PROGRAM SARJANA
PROGRAM STUDI INFORMATIKA
FAKULTAS ILMU KOMPUTER
UNIVERSITAS AMIKOM YOGYAKARTA
YOGYAKARTA
2019**

PERSETUJUAN

SKRIPSI

ANALISIS OVERCLOCKING KARTU GRAFIS KOMPUTER UNTUK MELAKUKAN CRACKING PASSWORD

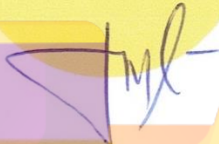
yang dipersiapkan dan disusun oleh

Yudhi Agus Triyono

17.21.1110

telah disetujui oleh Dosen Pembimbing Skripsi
pada tanggal 24 Oktober 2018

Dosen Pembimbing,



Joko Dwi Santoso, M.Kom.

NIK. 190302181

PENGESAHAN

SKRIPSI

ANALISIS OVERCLOCKING KARTU GRAFIS KOMPUTER UNTUK MELAKUKAN CRACKING PASSWORD

yang dipersiapkan dan disusun oleh

Yudhi Agus Triyono

17.21.1110

telah dipertahankan di depan Dewan Penguji
pada tanggal 23 Juli 2019

Susunan Dewan Penguji

Nama Penguji

Tanda Tangan

Heri Sismoro, M.Kom.
NIK. 190302057



Ichsan Wiratama, ST, M.Cs.
NIK. 190302119




Joko Dwi Santoso, M.Kom.
NIK. 190302181



Skripsi ini telah diterima sebagai salah satu persyaratan
untuk memperoleh gelar Sarjana Komputer
Tanggal 29 Juli 2019

DEKAN FAKULTAS ILMU KOMPUTER




Krisnawati, S.Si, M.T.
NIK. 190302038

PERNYATAAN

Saya yang bertanda tangan di bawah 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 tanggung jawab saya pribadi.

Yogyakarta, 26 Juli 2019



Yudhi Agus Triyono
NIM. 17.21.1110

MOTTO

“Keep moving forward”

“Man Jadda Wa Jadda”

“Bukanlah ilmu yang seharusnya mendatangimu, tetapi kamulah yang harus mendatangi ilmu itu.”

“Kebanyakan dari kita tidak mensyukuri apa yang sudah kita miliki, tetapi kita selalu menyesali apa yang belum kita capai.”

“Sesuatu yang belum dikerjakan, seringkali tampak mustahil; kita baru yakin kalau kita telah berhasil melakukannya dengan baik.”



PERSEMBAHAN

Alhamdulillahirobbil'alamin, segala puji bagi Allah SWT dengan segala limpahan rahmat, hidayah, serta karunia-Nya, sehingga saya bisa menyelesaikan skripsi ini dengan baik dan tepat waktu. Skripsi ini saya persembahkan kepada :

1. Allah SWT dan Nabi besar Muhammad SAW yang memberikan segala nikmat, rahmat dan karunia-Nya kepada saya, sehingga skripsi ini dapat terselesaikan.
2. Kedua orang tua yang senantiasa memberi dukungan melalui perkataan dan juga doa-doa
3. Dosen pembimbing, bapak Joko Dwi Santoso, M.Kom. yang telah memberikan bimbingan, masukan, motivasi serta arahan untuk kelancaran dan kemudahan dalam pembuatan skripsi ini.
4. Kakak-kakak sepermainan grup Si Bolang, Mas Cendhika, Mas Ferian, Mas Bhaguz, Mas Khusnun, Mas Ervan, Mas Andi, Mas Purwaji, Mas Arya, Mas Aveef & Kang Candra yang selalu memberikan dukungan untuk terus semangat dalam menyelesaikan studi saya.
5. Teman-teman sekantor di MSI (Micro Star International) Jakarta yang banyak memberikan pengalaman kerja dan dukungan untuk cepat-cepat menyelesaikan studi.
6. Teman-teman organisasi di HMJTI, Fossil dan Amikom OC Team yang banyak memberikan pengetahuan berorganisasi serta dukungan untuk kelancaran skripsi.
7. Teman-teman sekelas di 11-S1TI-01 yang berjuang bersama-sama selama menempuh studi, sukses selalu untuk kalian semua dimanapun berada.
8. Serta seluruh pihak yang telah banyak membantu dan tidak bisa disebutkan satu per satu, saya ucapkan terima kasih banyak.

KATA PENGANTAR

Puji dan syukur penulis persembahkan kepada Allah SWT yang telah memberikan rahmat, hidayah dan kekuatan sehingga penulis dapat menyelesaikan skripsi yang berjudul Analisis Overclocking Kartu Grafis untuk Melakukan Cracking Password. Tidak lupa shalawat beserta salam penulis panjatkan kepada junjungan alam Nabi Besar Muhammad SAW.

Laporan skripsi ini dibuat untuk melengkapi tugas akhir kuliah dan memenuhi syarat kelulusan program Pendidikan S1 Teknik Informatika di Universitas Amikom Yogyakarta.

Dalam penyusunan laporan skripsi ini, penulis banyak mendapatkan bantuan dan bimbingan dari berbagai pihak, maka penulis mengucapkan terimakasih kepada :

1. Kedua orang tua, serta adik-adik yang selalu memberi dukungan, doa dan nasehat.
2. Prof. Dr. M. Suyanto, MM. selaku Rektor Universitas AMIKOM Yogyakarta.
3. Drs. Sudarmawan, MT, selaku ketua jurusan S1 Teknik Informatika Universitas AMIKOM Yogyakarta.
4. Joko Dwi Santoso, M.Kom. selaku dosen pembimbing yang telah banyak memberikan pengarahan bagi penulis dalam pembuatan skripsi.
5. Bapak dan Ibu dosen Universitas AMIKOM Yogyakarta yang telah banyak memberikan ilmunya selama penulis berkuliah.
6. Teman-teman seperjuangan S1-TI-01 dalam menempuh studi di AMIKOM.
7. Teman-teman Fossil yang telah memberikan banyak pengalaman dan pengetahuan berorganisasi selama studi.
8. Semua pihak yang telah membantu baik dukungan moril maupun materil, pikiran, dan tenaga dalam penyelesaian skripsi ini.

Penyusun tentunya menyadari bahwa pembuatan skripsi ini masih banyak sekali kekurangannya. Oleh karena itu penyusun berharap kepada semua pihak agar dapat menyampaikan kritik dan saran yang membangun untuk menambah kesempurnaan skripsi ini. Namun penyusun tetap berharap skripsi ini akan bermanfaat bagi semua pihak yang membacanya.

Yogyakarta, 26 Juli 2019

Penulis



Yudhi Agus Triyono



DAFTAR ISI

HALAMAN JUDUL.....	i
PERSETUJUAN	ii
PENGESAHAN	iii
PERNYATAAN.....	iv
MOTTO.....	v
PERSEMBAHAN	vi
KATA PENGANTAR	vii
DAFTAR ISI.....	ix
DAFTAR TABEL.....	xii
DAFTAR GAMBAR	xiii
INTISARI.....	xv
ABSTRACT.....	xvi
BAB 1 PENDAHULUAN	1
1.1 Latar Belakang.....	1
1.2 Rumusan Masalah.....	2
1.3 Batasan Masalah	2
1.4 Maksud dan Tujuan Penelitian.....	3
1.5 Metode Penelitian	3
1.6 Sistematika Penulisan	5
BAB II LANDASAN TEORI	7
2.1 Tinjauan Pustaka.....	7
2.2 Dasar Teori.....	9
2.2.1 Konsep Keamanan Informasi.....	9

2.2.1.1	<i>Confidentiality</i>	10
2.2.1.2	<i>Integrity</i>	10
2.2.1.3	<i>Availability</i>	11
2.2.2	Jenis-Jenis Serangan	11
2.2.2.1	<i>Virus</i>	12
2.2.2.2	<i>Phising</i>	13
2.2.2.3	<i>DoS</i> atau <i>DDoS</i>	14
2.2.2.4	<i>Password Attack</i>	14
2.2.2.4.1	Brute Force Attack	15
2.2.2.4.2	Dictionary Attack	15
2.2.2.4.3	Keylogger Attack	15
2.2.2.5	<i>Social Engineering Attack</i>	16
2.2.3	<i>Hashing</i>	17
2.2.4	Mengenal GPU.....	18
2.2.5	<i>Nvidia Pascal</i>	21
2.2.5.1	Battery Boost	21
2.2.5.2	Gameworks	22
2.2.5.3	GSync.....	23
2.2.5.4	GPU Boost 3.0	23
2.2.5.5	GameStream.....	24
BAB III	ANALISIS DAN PERANCANGAN	26
3.1	Gambaran Umum.....	26
3.2	Analisis Masalah.....	27
3.3	Alur Penelitian	29
3.4	Analisis Kebutuhan.....	31
3.4.1	Analisis Kebutuhan Fungsional	31
3.4.2	Analisis Kebutuhan Non-Fungsional.....	31
3.4.2.1	Analisis Kebutuhan Perangkat Keras (<i>Hardware</i>)	32
3.4.2.2	Analisis Kebutuhan Perangkat Lunak (<i>Software</i>)	34
3.4.3	Skenario Pengujian	39

3.4.3.1	<i>Step-by-Step Overclocking</i> Kartu Grafis	39
3.4.3.2	Rentang Frekuensi Uji Coba	39
3.4.3.3	<i>Password</i> Uji Coba.....	40
3.4.3.4	<i>Hash</i> Uji Coba	41
3.4.4	Rancangan Lab Uji Coba	42
3.4.4.1	Instalasi hashcat.....	42
3.4.4.2	Persiapan File Target dan Output	44
BAB IV	IMPLEMENTASI DAN PEMBAHASAN	46
4.1	<i>Cracking Password</i> Menggunakan <i>Hashcat</i>	46
4.2	Pengujian.....	49
4.2.1	Pengujian <i>Benchmark Hashcat</i>	50
4.2.2	Pengujian <i>Cracking Password</i>	62
4.3	Hasil Pengujian	88
4.4	Analisis Hasil Pengujian	89
BAB V	PENUTUP	93
5.1	Kesimpulan	93
5.2	Saran	94
DAFTAR PUSTAKA	xvii

DAFTAR TABEL

Tabel 3.4.2.1.1 Spesifikasi laptop uji coba	32
Tabel 3.4.2.1.2 Spesifikasi GPU uji coba	33
Tabel 3.4.3.2.1 Tabel rentang frekuensi uji coba <i>overclocking</i>	40
Tabel 3.4.3.3.1 Tabel daftar <i>password</i> uji coba	41
Tabel 3.4.3.4.1 Tabel konversi <i>password</i> ke <i>hash MD5</i>	42
Tabel 4.3.1 Hasil pengujian <i>benchmark hashcat</i>	88
Tabel 4.3.2 Hasil pengujian <i>cracking password hashcat</i>	89
Tabel 4.4.1 Analisis selisih kecepatan <i>benchmark hashcat</i>	90
Tabel 4.4.2 Analisis hasil kecepatan <i>benchmark hashcat</i>	91
Tabel 4.4.3 Analisis perbandingan kenaikan <i>benchmark</i> dan kecepatan <i>cracking</i>	92

DAFTAR GAMBAR

Gambar 2.2.1.1 Segitiga keamanan informasi	10
Gambar 2.2.3.1 Logika fungsi <i>hashing</i>	18
Gambar 2.2.4.1 Jenis-jenis kartu grafis komputer	20
Gambar 2.2.5.1 Logo Nvidia.....	21
Gambar 3.3.1 Alur kerja penelitian.....	30
Gambar 3.4.2.1.1 Laptop MSI GS43VR Phantom Pro	33
Gambar 3.4.2.2.1.1 CPU-Z	34
Gambar 3.4.2.2.2.1 GPU-Z	35
Gambar 3.4.2.2.3.1 Cmder	36
Gambar 3.4.2.2.4.1 MSI Afterburner	37
Gambar 3.4.2.2.5.1 Logo <i>Hashcat</i>	38
Gambar 3.4.4.1.1 Halaman download tool hashcat	43
Gambar 3.4.4.1.2 Hasil extract tool hashcat	43
Gambar 3.4.4.1.3 Perintah menampilkan help hashcat	44
Gambar 3.4.4.2.1 Isi file target cracking.....	45
Gambar 3.4.4.2.2 Isi file output hasil cracking	45
Gambar 4.1.1 Contoh penggunaan <i>hashcat</i>	46
Gambar 4.1.2 Perintah <i>hashcat</i> untuk <i>benchmark</i> MD5.....	48
Gambar 4.1.3 Perintah <i>hashcat</i> untuk <i>cracking password</i> penelitian.....	48
Gambar 4.2.1.1 Hasil <i>benchmark</i> pada GPU Clock 1405 MHz	50
Gambar 4.2.1.2 Hasil <i>benchmark</i> pada GPU Clock 1430 MHz	51
Gambar 4.2.1.3 Hasil <i>benchmark</i> pada GPU Clock 1455 MHz	52
Gambar 4.2.1.4 Hasil <i>benchmark</i> pada GPU Clock 1480 MHz	53
Gambar 4.2.1.5 Hasil <i>benchmark</i> pada GPU Clock 1505 MHz	54

Gambar 4.2.1.6 Hasil <i>benchmark</i> pada GPU Clock 1530 MHz	55
Gambar 4.2.1.7 Hasil <i>benchmark</i> pada GPU Clock 1555 MHz	56
Gambar 4.2.1.8 Hasil <i>benchmark</i> pada GPU Clock 1580 MHz	57
Gambar 4.2.1.9 Hasil <i>benchmark</i> pada GPU Clock 1605 MHz	58
Gambar 4.2.1.10 Hasil <i>benchmark</i> pada GPU Clock 1630 MHz	59
Gambar 4.2.1.11 Hasil <i>benchmark</i> pada GPU Clock 1655 MHz	60
Gambar 4.2.1.12 Hasil <i>benchmark</i> pada GPU Clock 1680 MHz	61
Gambar 4.2.2.1 Hasil pengujian <i>cracking</i> pada GPU Clock 1405 MHz	65
Gambar 4.2.2.2 Hasil pengujian <i>cracking</i> pada GPU Clock 1430 MHz	67
Gambar 4.2.2.3 Hasil pengujian <i>cracking</i> pada GPU Clock 1455 MHz	69
Gambar 4.2.2.4 Hasil pengujian <i>cracking</i> pada GPU Clock 1480 MHz	71
Gambar 4.2.2.5 Hasil pengujian <i>cracking</i> pada GPU Clock 1505 MHz	73
Gambar 4.2.2.6 Hasil pengujian <i>cracking</i> pada GPU Clock 1530 MHz	75
Gambar 4.2.2.7 Hasil pengujian <i>cracking</i> pada GPU Clock 1555 MHz	77
Gambar 4.2.2.8 Hasil pengujian <i>cracking</i> pada GPU Clock 1580 MHz	79
Gambar 4.2.2.9 Hasil pengujian <i>cracking</i> pada GPU Clock 1605 MHz	81
Gambar 4.2.2.10 Hasil pengujian <i>cracking</i> pada GPU Clock 1630 MHz	83
Gambar 4.2.2.11 Hasil pengujian <i>cracking</i> pada GPU Clock 1655 MHz	85
Gambar 4.2.2.12 Hasil pengujian <i>cracking</i> pada GPU Clock 1680 MHz	87

INTISARI

Keamanan data adalah salah satu hal yang tidak akan hilang sejalan dengan makin berkembangnya teknologi digital. Salah satu metode pengamanan data yang paling sederhana adalah pemberian *password* atau kata kunci pada data yang ingin kita amankan dari tangan orang yang tidak bertanggung jawab. Walau begitu metode ini tidak menjamin sepenuhnya data kita tidak akan bisa diretas oleh *hacker* karena mereka sudah memiliki banyak teknik untuk menembus pengamanan ini. Salah satunya adalah dengan menggunakan teknik *brute force*.

Teknik *brute force* adalah cara untuk meretas *password* dengan cara mencoba semua kemungkinan kombinasi yang ada pada sebuah *wordlist*. Teknik ini membutuhkan kinerja komputer yang sangat tinggi terutama komponen kartu grafis atau *GPU* untuk bisa efektif, karena semakin panjang dan rumit kombinasi huruf, angka dan simbol yang digunakan akan semakin lama juga kata kunci yang benar bisa ditemukan. Salah satu cara untuk meningkatkan kecepatan *brute force* adalah dengan melakukan *overclocking* pada kartu grafis.

Dalam tulisan ini, peneliti melakukan observasi terhadap seberapa besar pengaruh *overclocking* kartu grafis komputer ketika digunakan untuk melakukan *password cracking*. Hasil dari analisis nantinya berguna untuk mengoptimalkan kartu grafis komputer untuk keperluan *password cracking*. Serta analisis ini diharapkan dapat dijadikan referensi untuk mempelajari sistem *hardware* komputer serta keamanan data lebih lanjut.

Kata kunci : *overclocking, gpu, nvidia, password, security*

ABSTRACT

Data security is one of the many things that unreplacable along with the continous development of digital technology. One of the simplest data security methods is giving password to the data that we want to secure from the hands of the irresponsible people. Even so, this method does not fully guarantee that our data will not be hacked by hackers because they already have many techniques to penetrate this form of security. One of them is 'Brute Force' techniques.

Brute Force is a technique to hack passwords by trying all possible combination from a wordlist. This technique requires very high computing speeds especially from the graphics card or GPU to be effective, because the longer and complex the password is used, the longer it can be found. One way to increase the brute force speed is to overclock the graphics card.

In this paper, the researcher aim to observe how much is the influence of computer graphics card overclocking when used to do password cracking. The results of the analysis will be useful for optimizing computer graphics card for password cracking purposes. And also this analysis is expected to be used as a future reference for studying computer hardware systems and data security further.

keyword : overclocking, gpu, nvidia, password, security