



Hak cipta dan penggunaan kembali:

Lisensi ini mengizinkan setiap orang untuk mengubah, memperbaiki, dan membuat ciptaan turunan bukan untuk kepentingan komersial, selama anda mencantumkan nama penulis dan melisensikan ciptaan turunan dengan syarat yang serupa dengan ciptaan asli.

Copyright and reuse:

This license lets you remix, tweak, and build upon work non-commercially, as long as you credit the origin creator and license it on your new creations under the identical terms.

**IMPLEMENTASI ALGORITMA AHO-CORASICK PADA
APLIKASI PENCARI FILE DALAM FORENSIC IMAGE
UNTUK DIGITAL FORENSIC**

SKRIPSI

**Diajukan sebagai salah satu syarat untuk memperoleh gelar
Sarjana Komputer (S.Kom.)**



Charles Anderson Lim

14110110011

**PROGRAM STUDI INFORMATIKA
FAKULTAS TEKNIK DAN INFORMATIKA
UNIVERSITAS MULTIMEDIA NUSANTARA
TANGERANG
2018**

HALAMAN PENGESAHAN SKRIPSI

IMPLEMENTASI ALGORITMA AHO-CORASICK PADA APLIKASI PENCARI FILE DALAM FORENSIC IMAGE UNTUK DIGITAL FORENSIC

Oleh

Nama : Charles Anderson Lim

NIM : 14110110011

Program Studi : Infomatika

Fakultas : Teknik dan Informatika

Tangerang, 10 Agustus 2018

Ketua Sidang



Seng Hansun, S.Si., M.Cs.

Penguji



Arya Wicaksana, S.Kom.,
M.Eng.Sc., OCA, CEH

Dosen Pembimbing



Dennis Gunawan, S.Kom., M.Sc.

Mengetahui,

Ketua Program Studi

Informatika



Seng Hansun, S.Si., M.Cs.

PERNYATAAN TIDAK MELAKUKAN PLAGIAT

Dengan ini saya,

Nama : Charles Anderson Lim

NIM : 14110110011

Program Studi : Informatika

Fakultas : Teknik dan Informatika

menyatakan bahwa skripsi dengan judul "**IMPLEMENTASI ALGORITMA AHO-CORASICK PADA APLIKASI PENCARI FILE DALAM FORENSIC IMAGE UNTUK DIGITAL FORENSIC**" merupakan karya ilmiah saya sendiri, bukan plagiat dari karya ilmiah milik orang lain atau lembaga lain, dan semua karya ilmiah orang lain atau lembaga lain yang dirujuk dalam skripsi ini telah disebutkan sumber kutipannya dan dicantumkan pada Daftar Pustaka.

Jika di kemudian hari terbukti ditemukan kecurangan/penyimpangan, baik dalam pelaksanaan skripsi maupun dalam penulisan laporan skripsi, saya bersedia menerima konsekuensi dinyatakan TIDAK LULUS untuk mata kuliah Skripsi yang telah saya jalani.

Tangerang, 10 Agustus 2018



Charles Anderson Lim

PERNYATAAN PERSETUJUAN PUBLIKASI KARYA ILMIAH
UNTUK KEPENTINGAN AKADEMIS

Sebagai sivitas akademik Universitas Multimedia Nusantara, saya yang bertanda tangan di bawah ini:

Nama : Charles Anderson Lim
NIM : 14110110011
Program Studi : Informatika
Fakultas : Teknik dan Informatika
Jenis Karya : Skripsi

Demi pengembangan ilmu pengetahuan, menyetujui dan memberikan izin kepada **Universitas Multimedia Nusantara** *hak Bebas Royalti Non-eksklusif (Non-exclusive Royalty-Free Right)* atas karya ilmiah saya yang berjudul: **Implementasi Algoritma Aho-Corasick pada Aplikasi Pencari File dalam Forensic Image untuk Digital Forensic** beserta perangkat yang diperlukan.

Dengan Hak Bebas Royalti Non-eksklusif ini, pihak **Universitas Multimedia Nusantara** berhak menyimpan, mengalihmedia atau *format-kan*, mengelola dalam bentuk pangkalan data (*database*), merawat, dan mendistribusi dan menampilkan atau mempublikasikan karya ilmiah saya di internet atau media lain untuk kepentingan akademis, tanpa perlu meminta izin dari saya maupun memberikan royalty kepada saya, selama tetap mencantumkan nama saya sebagai penulis karya ilmiah tersebut.

Demikian pernyataan ini saya buat dengan sebenarnya untuk dipergunakan sebagaimana mestinya.

Tangerang, 10 Agustus 2018



Charles Anderson Lim

KATA PENGANTAR

Puji syukur kepada Tuhan Yang Maha Esa yang selalu menyertai selama masa penggerjaan skripsi dalam laporan skripsi berjudul “Implementasi Algoritma *Aho-Corasick* pada Aplikasi Pencari *File* dalam *Forensic Image* untuk *Digital Forensic*” sehingga dapat diselesaikan dengan baik dan benar. Skripsi ini diajukan kepada Program Studi Teknik Informatika, Fakultas Teknik dan Informatika, Universitas Multimedia Nusantara.

Penyelesaian skripsi ini juga dibantu dan didukung oleh berbagai pihak, seperti teman-teman, dosen pembimbing, dan keluarga. Oleh karena itu, ucapan terima kasih yang sebesar-besarnya diucapkan kepada:

1. Dr. Ninok Leksono, selaku Rektor Universitas Multimedia Nusantara,
2. Hira Meidia, B.Eng., Ph.D., selaku Dekan Fakultas Teknik dan Informatika Universitas Multimedia Nusantara,
3. Seng Hansun, S.Si., M.Cs., selaku Ketua Program Studi Informatika Universitas Multimedia Nusantara,
4. Dennis Gunawan, S.Kom., M.Sc., selaku dosen pembimbing, yang membimbing pembuatan skripsi dan yang telah mengajar tata cara menulis skripsi dengan benar,
5. Keluarga yang selalu mendukung dan memberi semangat selama proses penggerjaan skripsi,
6. Teman-teman seperjuangan Group [DG] Skripsi 2014 yang terdiri dari Bryan, David, Dhaniya, Edwin, Hansen, Hendricksen, Hendro, Ivan, Kenny,

Rudiyanto, Sintya, Thomas, William, Willy, dan Yudha yang saling menyemangati dan berbagi ilmu demi kelulusan bersama,

7. Teman dan sahabat yang telah mendukung dan membantu selama proses penggerjaan skripsi, dan
8. Seluruh pihak yang telah memberikan bantuan dalam penulisan skripsi ini.

Semoga skripsi ini dapat bermanfaat, baik sebagai sumber informasi maupun sumber inspirasi, terutama untuk yang ingin belajar dan mengembangkan teknologi informasi dan komunikasi dalam bidang *Digital Forensic*.

Tangerang, 10 Agustus 2018



Charles Anderson Lim

IMPLEMENTASI ALGORTIMA AHO-CORASICK PADA APLIKASI PENCARI FILE DALAM FORENSIC IMAGE UNTUK DIGITAL FORENSIC

ABSTRAK

Era digital dikarakteristikkan sebagai penerapan dari teknologi komputer. Penggunaan komputer sebagai alat kriminal untuk melakukan penyembunyian data digital meningkat. Seperti beberapa kasus kriminal, bukti digital berupa *file* dihapus dari *file system*. Bukti digital masih bisa di-recover selama ruang alokasi untuk *file* tersebut belum ditimpas dengan data yang lain atau melalui penghapusan atau pembersihan *hard disk*. Dalam *digital forensic*, dibuat duplikasi ruang penyimpanan bukti digital yang disebut juga *forensic image*. Bukti digital yang sudah bisa dihapus bisa di-recover dengan mencari kata kunci tertentu yang cocok dengan bukti digital dalam *forensic image* dan *recover file* yang ditemukan. Oleh karena itu dibuatlah aplikasi pencari *file* dalam *forensic image* dengan mengimplementasikan algoritma *aho-corasick* untuk melakukan pencarian *file*. Hasil percobaan dengan *forensic image* yang tidak di-overwrite menunjukkan rata-rata waktu pencarian *file* yang dilakukan adalah 0,002387 detik, dan rata-rata waktu untuk melakukan *recover* adalah 33,48114 detik. Kemudian didapat juga nilai rata-rata *precision* sebesar 0,970173, rata-rata *recall* sebesar 0,741920, dan rata-rata *f-measure* sebesar 0,837072. Jumlah data yang dapat di-recover dengan baik bergantung pada urutan *file* yang dimasukkan ke dalam *forensic image* dan ukuran data yang digunakan untuk *overwrite* data *forensic image*. Jika *file* pada *forensic image* dimasukkan berurut berdasarkan ukuran *file* dari terkecil hingga terbesar, maka jumlah *file* yang bisa di-recover sangat sedikit ketika di-overwrite dengan data berukuran besar.

Kata Kunci: *aho-corasick*, *digital forensic*, *file recovery*, *file searching*, *forensic image*.

**UNIVERSITAS
MULTIMEDIA
NUSANTARA**

**IMPLEMENTATION OF AHO-CORASICK ALGORITHM
ON FILE CARVING ON FORENSIC IMAGE
FOR DIGITAL FORENSIC**

ABSTRACT

The digital age is characterized as the application of computer technology. The use of computers as a criminal tool for digital data hiding increases. Like some criminal cases, digital evidence of files is deleted from the file system. Digital evidence can still be recovered as long as the allocation space for the file has not been overwritten with other data or through the removal or cleaning of the hard disk. In digital forensics, duplicate digital evidence storage space is called forensic image. Deleted digital evidence can be recovered by search for certain keywords that match the digital evidence in the forensic image and recover the files found. Therefore, a file carving for forensic image application is created by implementing an aho-corasick algorithm to perform file search. The experiment result with non-overwrite forensic images shows the average time to search files is 0.002387s, and the average time to recover is 33.48114s. Based on examination result, the average precision 0.970173, the average recall of 0.741920, and the average value of f-measure 0.837072. The amount of data that can be recovered depends on the order of file inserted on the forensic image and the size of the data used to overwrite forensic image data. If the file in the forensic image is sorted by the size of the file from the smallest to the largest, then the number of file that can be recovered is very small when overwritten with large data.

Keywords: aho-corasick, digital forensic, file recovery, file searching, forensic image.

**UNIVERSITAS
MULTIMEDIA
NUSANTARA**

DAFTAR ISI

HALAMAN PENGESAHAN SKRIPSI.....	ii
PERNYATAAN TIDAK MELAKUKAN PLAGIAT	iii
PERNYATAAN PERSETUJUAN PUBLIKASI	iv
KATA PENGANTAR	v
ABSTRAK	vii
ABSTRACT	viii
DAFTAR ISI.....	ix
DAFTAR GAMBAR	x
DAFTAR TABEL	xii
DAFTAR RUMUS.....	xiii
BAB I PENDAHULUAN	1
1.1 Latar Belakang Masalah	1
1.2 Rumusan Masalah	3
1.3 Batasan Masalah.....	4
1.4 Tujuan Penelitian.....	4
1.5 Manfaat penelitian	4
1.6 Sistematika Penulisan.....	5
BAB II LANDASAN TEORI.....	7
2.1 Digital Forensik	7
2.2 New Technology File System (NTFS)	7
2.3 Master File Table (MFT).....	8
2.4 Forensic Image	14
2.5 File Signature.....	14
2.6 Aho-Corasick.....	15
2.7 FTK Imager	19
2.8 HashMyFiles.....	20
2.9 Architecture of File Undelete with Aho-Corasick Algorithm.....	21
2.10 F-measure	23
BAB III METODOLOGI DAN PERANCANGAN APLIKASI	25
3.1 Metodologi Penelitian	25
3.2 Perancangan Aplikasi	26
3.3 Perancangan Antarmuka.....	38
BAB IV IMPLEMENTASI DAN HASIL UJI COBA	40
4.1 Spesifikasi Perangkat.....	40
4.2 Implementasi	40
4.2.1 Tampilan Aplikasi.....	41
4.2.2 Implementasi Algoritma dan Skenario Uji Coba	41
4.3 Uji Coba.....	61
4.3.1 Uji Coba Aplikasi.....	61
4.3.2 Analisis Hasil Uji Coba.....	72
BAB V KESIMPULAN DAN SARAN	77
5.1 Kesimpulan.....	77
5.2 Saran.....	77
DAFTAR PUSTAKA	79
LAMPIRAN	81

DAFTAR GAMBAR

Gambar 2.1 Struktur <i>volume</i> NTFS	8
Gambar 2.2 Struktur MFT entry	9
Gambar 2.3 Automata	16
Gambar 2.4 Transisi Fungsi Failure	18
Gambar 2.5 Transisi Fungsi Output	18
Gambar 2.6 Tampilan aplikasi FTK Imager	20
Gambar 2.7 Tampilan aplikasi HashMyFiles.....	21
Gambar 2.8 Architecture of File Undelete with Aho-Corasick Algorithm.....	22
Gambar 3.1 Rancangan Aplikasi.....	27
Gambar 3.2 Flowchart Main Display.....	28
Gambar 3.3 Flowchart Search File.....	29
Gambar 3.4 Flowchart Get File Record List.....	30
Gambar 3.5 Flowchart bootRecord	31
Gambar 3.6 Flowchart GetMFT	31
Gambar 3.7 Flowchart getMFTAttribute	34
Gambar 3.8 Flowchart Generate Automata	35
Gambar 3.9 Flowchart Search Word.....	36
Gambar 3.10 Flowchart Find Next State.....	37
Gambar 3.11 Flowchart Recover file	37
Gambar 3.12 Rancangan Tampilan Antarmuka	38
Gambar 3.13 Tampilan Open File Dialog	39
Gambar 3.14 Tampilan Choose Directory Dialog	39
Gambar 4.1 Tampilan Aplikasi	41
Gambar 4.2 Checksum Forensic Image (Skenario)	42
Gambar 4.3 Potongan kode membaca Atribut Boot Record	42
Gambar 4.4 Nilai Atribut Boot Record	43
Gambar 4.5 Potongan Kode get FileRecordList	43
Gambar 4.6 Potongan Kode Get MFT Entry Header.....	44
Gambar 4.7 Nilai MFT Entry Header	44
Gambar 4.8 Potongan kode get MFTAttribute	45
Gambar 4.9 Nilai Attribute Header \$STANDARD_INFORMATION	45
Gambar 4.10 Potongan Kode Get Resident Attribute	46
Gambar 4.11 Nilai \$STANDARD_INFORMATION Resident Attribute	46
Gambar 4.12 Potongan Kode Get \$STANDARD_INFORMATION Attribute ...	46
Gambar 4.13 Informasi \$STANDARD_INFORMATION.....	47
Gambar 4.14 Nilai Attribute Header \$FILENAME.....	47
Gambar 4.15 Nilai \$FILENAME Resident Attribute	47
Gambar 4.16 Potongan Kode Get \$FILENAME	47
Gambar 4.17 Informasi \$FILENAME	48
Gambar 4.18 Nilai Attribute Header \$DATA.....	48
Gambar 4.19 Potongan Kode Get Non Resident Attribute	48
Gambar 4.20 Nilai \$DATA Resident Attribute	49
Gambar 4.21 Informasi \$DATA	49
Gambar 4.22 Potongan kode Get Signature	49

Gambar 4.23 Implementasi Kode Generate Automata	51
Gambar 4.24 Langkah 1 membuat trie.....	52
Gambar 4.25 langkah 2 membuat trie	52
Gambar 4.26 Langkah 3 membuat trie.....	52
Gambar 4.27 Function goto.....	53
Gambar 4.28 Function failure trie	55
Gambar 4.29 Function output	56
Gambar 4.30 Potongan Kode Search Word	57
Gambar 4.31 Potongan kode fungsi findNextState.....	57
Gambar 4.32 Potongan Kode Recover File.....	59
Gambar 4.33 Screenshot Recover File.....	60
Gambar 4.34 Grafik perbandingan jumlah file yang berhasil di-recovery	72
Gambar 4.35 Grafik perbandingan Precision.....	73
Gambar 4.36 Grafik perbandingan Recall	74
Gambar 4.37 Grafik perbandingan f-measure.....	75
Gambar 4.38 Grafik perbandingan waktu pencarian file	75
Gambar 4.39 Grafik perbandingan waktu recover file.....	76



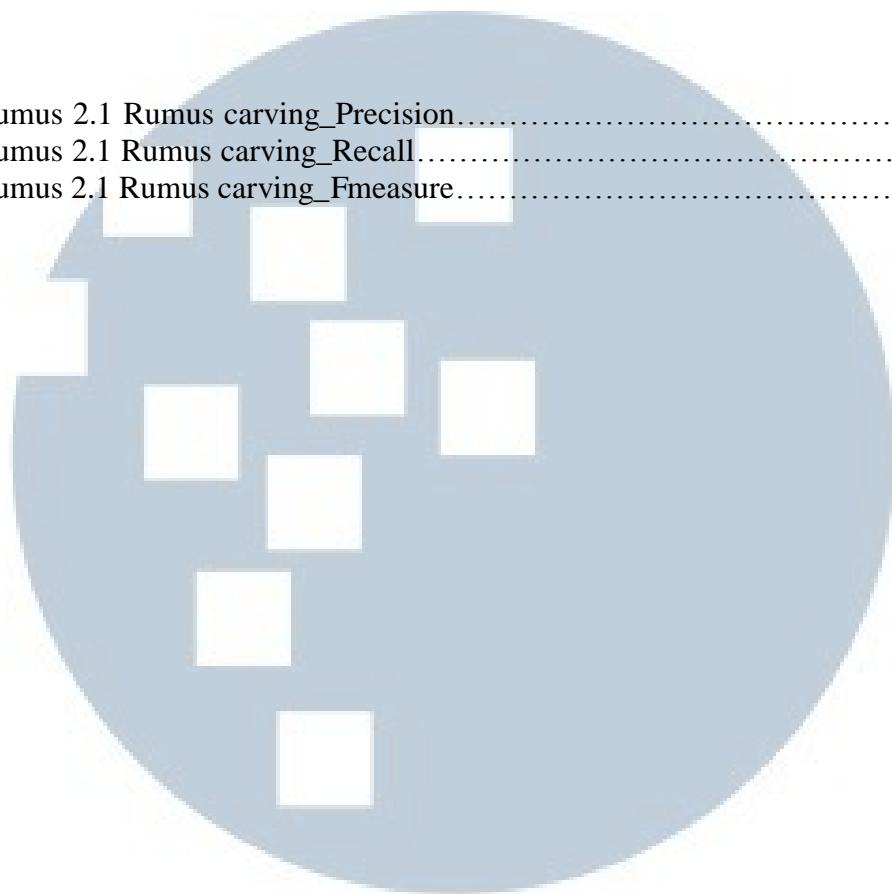
DAFTAR TABEL

Tabel 2.1 Tabel MFT Entry Attribute dengan masing-masing Tipe Identifier.....	9
Tabel 2.2 NTFS File System Metadata Files	10
Tabel 2.3 MFT Entry Header Details.....	10
Tabel 2.4 Common attribute header structure.....	11
Tabel 2.5 Resident attribute header structure.....	12
Tabel 2.6 Non-resident attribute header structure.....	12
Tabel 2.7 \$STANDARD_INFORMATION attribute structure.....	13
Tabel 2.8 \$FILENAME attribute structure	13
Tabel 2.9 File Signature	14-15
Tabel 2.10 Tabel Transisi Automata.....	17
Tabel 2.11 Tabel Transisi Failure	18
Tabel 2.12 Tabek Fungsi Output.....	18
Tabel 2.13 Tabel Transisi Pencarian.....	19
Tabel 4.1 Tabel Transisi Automata.....	54
Tabel 4.2 Tabel Transisi Failure	55
Tabel 4.3 Tabel Fungsi Output.....	56
Tabel 4.4 Hash Value File Skenario	60
Tabel 4.5 Tabel Skenario1 Percobaan 1.....	63
Tabel 4.6 Tabel Skenario 1 Percobaan 2.....	63-64
Tabel 4.7 Tabel Skenario 1 Percobaan 3.....	64
Tabel 4.8 Tabel Skenario 1 Percobaan 4.....	65
Tabel 4.9 Tabel Skenario 1 Percobaan 5.....	65
Tabel 4.10 Tabel Skenario 2 Percobaan 1.....	66
Tabel 4.11 Tabel Skenario 2 Percobaan 2.....	66-67
Tabel 4.12 Tabel Skenario 2 Percobaan 3.....	67
Tabel 4.13 Tabel Skenario 2 Percobaan 4.....	68
Tabel 4.14 Tabel Skenario 2 Percobaan 5.....	68
Tabel 4.15 Tabel Skenario 3 Percobaan 1.....	69
Tabel 4.16 Tabel Skenario 3 Percobaan 2.....	69-70
Tabel 4.17 Tabel Skenario 3 Percobaan 3.....	70
Tabel 4.18 Tabel Skenario 3 Percobaan 4.....	71
Tabel 4.19 Tabel Skenario 3 Percobaan 5.....	71

**UNIVERSITAS
MULTIMEDIA
NUSANTARA**

DAFTAR RUMUS

Rumus 2.1 Rumus carving_Precision.....	23
Rumus 2.1 Rumus carving_Recall.....	23
Rumus 2.1 Rumus carving_Fmeasure.....	23



UMN
UNIVERSITAS
MULTIMEDIA
NUSANTARA