



Hak cipta dan penggunaan kembali:

Lisensi ini mengizinkan setiap orang untuk menggubah, 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 FUZZY HASHING UNTUK
MENINGKATKAN JUMLAH DETEKSI MALWARE
DENGAN METODE SIGNATURE BASED DETECTION**

SKRIPSI

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



Aditia Rinaldi

11110110060

**PROGRAM STUDI TEKNIK INFORMATIKA
FAKULTAS TEKNOLOGI INFORMASI DAN KOMUNIKASI
UNIVERSITAS MULTIMEDIA NUSANTARA
TANGERANG**

2015

PERNYATAAN TIDAK MELAKUKAN PLAGIAT

Dengan ini, saya:

Nama : Aditia Rinaldi
NIM : 11110110060
Fakultas : Teknologi Informasi dan Komunikasi
Program Studi : Teknik Informatika

menyatakan bahwa skripsi yang berjudul IMPLEMENTASI FUZZY HASHING UNTUK MENINGKATKAN JUMLAH DETEKSI MALWARE DENGAN METODE SIGNATURE BASED DETECTION ini adalah karya ilmiah saya sendiri, bukan plagiat dari karya ilmiah yang ditulis oleh orang lain atau lembaga lain, dan semua karya ilmiah orang lain atau lembaga lain yang dirujuk dalam skripsi ini telah disebutkan sumbernya serta dicantumkan di 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 tempuh.

Tangerang, 27 April 2015

(Aditia Rinaldi)

LEMBAR PENGESAHAN SKRIPSI

IMPLEMENTASI FUZZY HASHING UNTUK MENINGKATKAN JUMLAH DETEKSI MALWARE DENGAN METODE SIGNATURE BASED DETECTION

Oleh

Nama : Aditia Rinaldi

NIM : 11110110060

Fakultas : Teknologi Informasi dan Komunikasi

Program Studi : Teknik Informatika

Tangerang, 7 Mei 2015

Ketua Sidang

Dosen Penguji

Maria Irmina Prasetiyowati, S.Kom., M.T.

Ranny, S.Kom., M.Kom.

Dosen Pembimbing I

Dosen Pembimbing II

Yustinus Widya Wiratama, S.Kom., M.Sc.

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

Mengetahui,

Ketua Program Studi Teknik Informatika

Maria Irmina Prasetiyowati, S.Kom., M.T.

KATA PENGANTAR

Puji syukur penulis panjatkan ke hadirat Tuhan Yang Maha Sempurna atas berkat, kekuatan, serta limpahan inspirasi-Nya sehingga penulis dapat menyelesaikan skripsi beserta penulisan laporannya yang merupakan salah satu tahap bersejarah dalam perjalanan panjang pendidikan. Laporan ini dipersiapkan untuk diajukan kepada Program Studi Teknik Informatika, Fakultas Teknologi Informasi dan Komunikasi, Universitas Multimedia Nusantara sebagai salah satu syarat kelulusan memperoleh gelar Sarjana Komputer (S.Kom.).

Terselesaikannya skripsi ini tidak lepas dari kerja sama banyak pihak, untuk itu izinkan penulis mengucapkan terima kasih kepada:

1. Dr. Ninok Leksono, Rektor Universitas Multimedia Nusantara,
2. Kanisius Karyono, S.T., M.T., Dekan Fakultas Teknologi Informasi dan Komunikasi Universitas Multimedia Nusantara,
3. Maria Irmina Prasetyowati, S.Kom., M.T., Ketua Program Studi Teknik Informatika Universitas Multimedia Nusantara dan selaku ketua sidang skripsi yang telah memberi masukan dalam menulis skripsi,
4. Yustinus Widya Wiratama, S.Kom., M.Sc. dan Seng Hansun, S.Si., M.Cs. yang membimbing pembuatan skripsi dan yang telah mengajar penulis tata cara menulis karya ilmiah dengan benar,
5. Ranny, S.Kom., M.Kom. selaku penguji dalam sidang skripsi yang telah memberi masukan dalam menulis skripsi,
6. Keluarga penulis yang telah memberikan dukungannya,
7. Segenap dosen, dan teman penulis yang tidak dapat penulis sebutkan satu-persatu.

Semoga skripsi ini bisa bermanfaat untuk memberikan informasi yang berguna dan menjadi inspirasi bagi seluruh pembacanya.

Tangerang, 27 April 2015

(Aditia Rinaldi)



IMPLEMENTASI FUZZY HASHING UNTUK MENINGKATKAN JUMLAH DETEKSI MALWARE DENGAN METODE SIGNATURE BASED DETECTION

ABSTRAK

Hash tradisional yang umum digunakan adalah MD5, SHA-1, dan SHA256. Dalam penelitian ini, keterbatasan *hash* tradisional dimana nilainya digunakan untuk membandingkan kesamaan *file* (*fingerprinting*), akan digantikan dengan *fuzzy hashing* sebagai salah satu metode *hash* yang berbeda dari *hash* tradisional karena dengan menggunakan *fuzzy hash* dapat mendeteksi kemiripan *file* dengan *output* berupa rentang nilai dari nol (tidak mirip) sampai dengan satu (sangat mirip) sehingga *malware* yang dapat terdeteksi dapat melebihi jumlah *signature* yang telah ada dalam *database* walau *signature malware* sebenarnya belum dibangun ke dalam *database*, terutama *malware* yang masih mirip atau varian dari *malware* yang telah terdapat dalam *database* dengan batas toleransi kemiripan minimal (*threshold*) tertentu. Implementasi *fuzzy hashing* menggunakan gabungan algoritma *spamsum* untuk menghasilkan nilai *hash* dan algoritma *Levenshtein Distance* termodifikasi untuk membandingkan kemiripan antara dua nilai *fuzzy hash*. Dari hasil uji coba, didapati bahwa implementasi *fuzzy hashing* pada *signature malware* dapat meningkatkan jumlah deteksi *malware* rata-rata sebesar 31,84% dan meningkatkan tingkat akurasi rata-rata sebesar 16,63% dari *hash* tradisional SHA256. Peningkatan jumlah deteksi dan akurasi optimal dapat dicapai pada *threshold* 50%.

Kata kunci: *accuracy, detection rate, fuzzy hasing, signature-based detection, signature malware.*

U M N

IMPLEMENTATION OF FUZZY HASHING TO INCREASE THE NUMBER OF MALWARE DETECTION WITH SIGNATURE-BASED DETECTION METHOD

ABSTRACT

Traditional hash that commonly used is MD5, SHA-1, and SHA256. In this research, the limitations of traditional hash where the value is used to compare identical file (fingerprinting), will be replaced by fuzzy hashing as one of the hash method that slightly different from traditional hash because by using fuzzy hash can detect similarity with output value from zero (not similar) to one (very similar), so the number of detected malware can exceed the number of signatures that have been stored in database even though the actual malware signatures have not been built or stored in the database, especially similar malware or variant of malware that have been stored in the database with specific threshold. Implementation of fuzzy hash use a combination spamsum algorithm to generate fuzzy hash value and modified Levenshtein Distance algorithm to compare similarity between two fuzzy hash value. And the result, the implementation of fuzzy hashing on malware signature can increase the number of malware detection on average by 31,84% and increase the accuracy rate on average by 16,63% from SHA256 traditional hash. Optimal enhancement number of malware detection and accuracy rate can be achieved at the threshold 50%.

Keywords: accuracy, detection rate, fuzzy hashing, signature-based detection, signature malware.

UMMN

DAFTAR ISI

PERNYATAAN TIDAK MELAKUKAN PLAGIAT	ii
LEMBAR PENGESAHAN SKRIPSI	iii
KATA PENGANTAR	iv
ABSTRAK	vi
ABSTRACT	vii
DAFTAR ISI.....	viii
DAFTAR TABEL.....	x
DAFTAR GAMBAR	xii
BAB I PENDAHULUAN	1
1.1 Latar Belakang	1
1.2 Rumusan Masalah	4
1.3 Batasan Masalah.....	4
1.4 Tujuan Penelitian	5
1.5 Manfaat Penelitian	5
1.6 Sistematika Penulisan	5
BAB II LANDASAN TEORI.....	7
2.1 Malicious Software	7
2.2 File Signature	8
2.3 Malware Signature	10
2.4 Traditional Hashing.....	11
2.5 Fuzzy Hashing.....	13
2.6 Levenshtein Distance	19
2.7 Signature-Based Detection.....	22
2.8 Tingkat Deteksi dan Akurasi.....	23
BAB III METODE DAN PERANCANGAN SISTEM.....	25
3.1 Metode Penelitian.....	25
3.1.1 Variabel Penelitian	27
3.2 Spesifikasi Perangkat	27
3.2.1 Perangkat Keras	28
3.2.2 Perangkat Lunak.....	28
3.3 Pengumpulan Data dan Pengambilan Sampel Malware	28
3.3.1 Pengumpulan Data	28
3.3.2 Pengambilan Sampel.....	29
3.4 Perancangan Basis Data	32
3.5 Perancangan Library Fuzzy Hash	32
3.5.1 Perancangan Fungsi Penghitungan Fuzzy Hash suatu File.....	33
3.5.2 Perancangan Fungsi Perbandingan Hash	37
3.5.3 Hubungan antar Class dalam Library Fuzzy Hash.....	38
3.6 Perancangan Aplikasi.....	40
3.6.1 Aplikasi Dashboard.....	40
3.6.2 Aplikasi Database Signature Builder	41

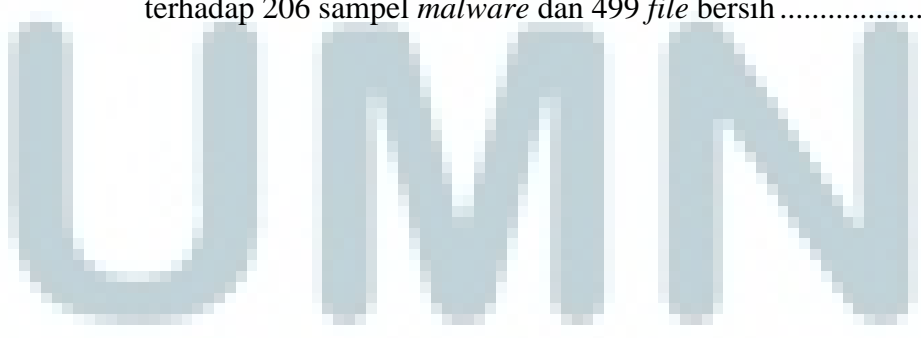
3.6.3 Aplikasi Malware Detector	41
3.6.4 Use Case Diagram.....	42
3.6.5 Activity Diagram.....	43
3.6.6 Class Diagram	57
3.6.7 Perancangan Antarmuka	63
BAB IV IMPLEMENTASI DAN UJI COBA	66
4.1 Spesifikasi Perangkat	66
4.2 Implementasi Program	66
4.2.1 Library Fuzzy Hashing.....	66
4.2.2 Aplikasi Dashboard.....	72
4.2.3 Aplikasi Database Signature Builder	73
4.2.4 Aplikasi Malware Detector	75
4.2.5 Kompilasi Program	78
4.3 Uji Coba Program	78
4.3.1 Persiapan	78
4.3.2 Uji Coba Program Dashboard	81
4.3.3 Uji Coba Program Database Signature Builder	85
4.3.4 Uji Coba Program Malware Detector	92
4.3.5 Analisis Hasil Uji Coba Deteksi	118
BAB V KESIMPULAN DAN SARAN.....	126
5.1 Kesimpulan	126
5.2 Saran.....	127
DAFTAR PUSTAKA	129
LAMPIRAN.....	132
DAFTAR RIWAYAT HIDUP.....	136

UMMN

DAFTAR TABEL

Tabel 2.1.	Beberapa tipe <i>malware</i> (Oriyano, 2014).....	7
Tabel 2.2.	Beberapa tipe <i>file</i> beserta <i>magic number</i> (Kessler, 2014)	8
Tabel 2.3.	Contoh perubahan nilai <i>hash</i> MD5 dan SHA256	11
Tabel 2.4.	Contoh perubahan nilai <i>fuzzy hash</i> dan SHA256.....	16
Tabel 2.5.	Aturan perbandingan <i>fuzzy hash</i> antara dua <i>signature</i> (Kornblum, 2006).....	22
Tabel 3.1.	Spesifikasi PC yang digunakan dalam pengembangan aplikasi	28
Tabel 3.2.	Rancangan tabel <i>signature</i> yang berisi informasi <i>malware</i> sederhana.....	32
Tabel 3.3.	Daftar <i>function</i> berdasarkan <i>pseudocode</i> pada sub-bab 2.5	33
Tabel 3.4.	Keterangan beberapa <i>method</i> dari <i>class</i> dalam <i>Dashboard</i>	58
Tabel 3.5.	Keterangan beberapa <i>method</i> dari <i>class</i> dalam <i>Database</i> <i>Signature Builder</i>	60
Tabel 3.6.	Keterangan beberapa <i>method</i> dari <i>class</i> dalam <i>Malware Detector</i>	62
Tabel 4.1.	Persiapan pembentukan <i>file database signature</i>	80
Tabel 4.2.	Skenario yang digunakan dalam uji deteksi.....	81
Tabel 4.3.	Perbandingan <i>file database signature</i> yang telah dihasilkan	91
Tabel 4.4.	Hasil deteksi db.sha256 terhadap sampel <i>malware</i> beserta varian	95
Tabel 4.5.	Hasil deteksi db-all.sha256 terhadap sampel <i>malware</i> beserta varian	95
Tabel 4.6.	Hasil deteksi db.sha256 terhadap sampel <i>malware</i> beserta varian dan <i>file</i> lain yang dipilih secara acak	97
Tabel 4.7.	Hasil deteksi db-all.sha256 terhadap sampel <i>malware</i> beserta varian dan <i>file</i> lain yang dipilih secara acak	98
Tabel 4.8.	Hasil deteksi db.fuzzy terhadap sampel <i>malware</i> beserta varian pada batas kemiripan minimal 25%	101
Tabel 4.9.	Hasil deteksi db.fuzzy terhadap sampel <i>malware</i> beserta varian pada batas kemiripan minimal 50%	101
Tabel 4.10.	Hasil deteksi db.fuzzy terhadap sampel <i>malware</i> beserta varian pada batas kemiripan minimal 75%	102
Tabel 4.11.	Hasil deteksi db.fuzzy terhadap sampel <i>malware</i> beserta varian pada tingkat kemiripan minimal 100%	103
Tabel 4.12.	Hasil deteksi db-all.fuzzy terhadap sampel <i>malware</i> beserta varian pada batas kemiripan minimal 25%	106
Tabel 4.13.	Hasil deteksi db-all.fuzzy terhadap sampel <i>malware</i> beserta varian pada batas kemiripan minimal 50%	106
Tabel 4.14.	Hasil deteksi db-all.fuzzy terhadap sampel <i>malware</i> beserta varian pada batas kemiripan minimal 75%	107
Tabel 4.15.	Hasil deteksi db-all.fuzzy terhadap sampel <i>malware</i> beserta varian pada batas kemiripan minimal 100%	107

Tabel 4.16. Hasil deteksi db.fuzzy terhadap sampel <i>malware</i> beserta varian dan <i>file</i> lain yang dipilih secara acak pada batas kemiripan minimal 25%	110
Tabel 4.17. Hasil deteksi db.fuzzy terhadap sampel <i>malware</i> beserta varian dan <i>file</i> lain yang dipilih secara acak pada batas kemiripan minimal 50%	111
Tabel 4.18. Hasil deteksi db.fuzzy terhadap sampel <i>malware</i> beserta varian dan <i>file</i> lain yang dipilih secara acak pada batas kemiripan minimal 75%	111
Tabel 4.19. Hasil deteksi db.fuzzy terhadap sampel <i>malware</i> beserta varian dan <i>file</i> lain yang dipilih secara acak pada batas kemiripan minimal 100%	112
Tabel 4.20. Hasil deteksi db-all.fuzzy terhadap sampel <i>malware</i> beserta varian dan <i>file</i> lain yang dipilih secara acak pada batas kemiripan minimal 25%	115
Tabel 4.21. Hasil deteksi db-all.fuzzy terhadap sampel <i>malware</i> beserta varian dan <i>file</i> lain yang dipilih secara acak pada batas kemiripan minimal 50%	116
Tabel 4.22. Hasil deteksi db-all.fuzzy terhadap sampel <i>malware</i> beserta varian dan <i>file</i> lain yang dipilih secara acak pada batas kemiripan minimal 75%	116
Tabel 4.23. Hasil deteksi db-all.fuzzy terhadap sampel <i>malware</i> beserta varian dan <i>file</i> lain yang dipilih secara acak pada batas kemiripan minimal 100%	117
Tabel 4.24. Penghitungan akurasi dan deteksi db.sha256 dan db.fuzzy terhadap 206 sampel <i>malware</i>	119
Tabel 4.25. Penghitungan akurasi dan deteksi db-all.sha256 dan db-all.fuzzy terhadap 206 sampel <i>malware</i>	121
Tabel 4.26. Penghitungan akurasi dan deteksi db.sha256 dan db.fuzzy terhadap 206 sampel <i>malware</i> dan 499 <i>file</i> bersih	123
Tabel 4.27. Penghitungan akurasi dan deteksi db-all.sha256 dan db-all.fuzzy terhadap 206 sampel <i>malware</i> dan 499 <i>file</i> bersih	124



DAFTAR GAMBAR

Gambar 1.1.	Laporan Kaspersky Lab tentang pertumbuhan <i>malware</i> tahun 2013 (Kaspersky, 2013).....	2
Gambar 2.1.	<i>Checksum</i> kumpulan <i>file</i> yang menggunakan CRC, MD5, dan SHA-1 (ALTAP, 2014)	10
Gambar 2.2.	Ilustrasi <i>Piecewise Hash</i> (Kornblum, 2007)	13
Gambar 2.3.	Ilustrasi <i>rolling hash</i> dengan ukuran $n = 3$ (FRRI Inc, 2014).....	14
Gambar 2.4.	Ilustrasi lain <i>rolling hash</i> dengan ukuran $n = 6$ (Kornblum, 2007).....	14
Gambar 2.5.	<i>Pseudocode</i> algoritma <i>spamsum</i> dalam <i>fuzzy hashing</i>	17
Gambar 2.6.	Lanjutan <i>pseudocode</i> algoritma <i>spamsum</i> dalam <i>fuzzy hashing</i>	18
Gambar 2.7.	<i>Levenshtein Distance</i> dengan pendekatan <i>dynamic programming</i> (Fischer dan Robert, 1974)	20
Gambar 2.8.	<i>Levenshtein Distance</i> termodifikasi dengan perubahan nilai <i>cost</i> dan penambahan operasi <i>swap</i> (Breitinger, 2011; Rutenberg, 2008)	21
Gambar 3.1.	Alur proses pengiriman <i>file</i> yang dicurigai <i>malware</i> oleh partisipan melalui DropItToMe	30
Gambar 3.2.	Alur proses pemeriksaan <i>file</i> yang telah dikirim partisipan	31
Gambar 3.3.	Rancangan <i>class RollingState</i>	34
Gambar 3.4.	Rancangan <i>class Signature</i>	34
Gambar 3.5.	Rancangan <i>class SignatureInfo</i>	35
Gambar 3.6.	Rancangan <i>class FuzzyHashing</i>	36
Gambar 3.7.	Contoh implementasi cara menghasilkan <i>fuzzy hash</i> dari suatu <i>file</i>	36
Gambar 3.8.	Rancangan <i>class LevenshteinDistance</i>	37
Gambar 3.9.	<i>Class Diagram</i> dalam <i>library fuzzy hash</i>	38
Gambar 3.10.	Contoh penggunaan <i>library fuzzy hash</i> pada <i>console application</i>	39
Gambar 3.11.	<i>Use case diagram</i> keseluruhan aplikasi	43
Gambar 3.12.	<i>Activity Diagram</i> ketika mengeksekusi <i>Database Signature Builder</i>	44
Gambar 3.13.	<i>Activity Diagram</i> ketika mengeksekusi <i>Malware Detector</i>	44
Gambar 3.14.	<i>Activity Diagram</i> ketika mengatur konfigurasi <i>file executable</i> aplikasi.....	45
Gambar 3.15.	<i>Activity Diagram</i> ketika mengatur konfigurasi <i>file database signature default</i>	45
Gambar 3.16.	<i>Activity Diagram</i> ketika melakukan <i>update identified_name malware</i> pada <i>database signature default</i>	46
Gambar 3.17.	<i>Activity Diagram</i> ketika melakukan hapus <i>record</i> informasi <i>malware</i> pada <i>database signature default</i>	46

Gambar 3.18. <i>Activity Diagram</i> ketika mengaktifkan/menonaktifkan <i>context-menu file explorer</i>	47
Gambar 3.19. <i>Activity Diagram</i> ketika mengaktifkan/menonaktifkan <i>removable drive detector</i>	48
Gambar 3.20. <i>Activity Diagram</i> ketika me-load file sampel.....	49
Gambar 3.21. <i>Activity Diagram</i> ketika melakukan <i>generate</i> nilai <i>hash</i> dari file sampel yang telah di-load.....	49
Gambar 3.22. <i>Activity Diagram</i> ketika melakukan ekspor ke dalam <i>database</i> baru	50
Gambar 3.23. <i>Activity Diagram</i> ketika melakukan ekspor ke dalam <i>database</i> yang sudah ada	50
Gambar 3.24. <i>Activity Diagram</i> ketika dilakukan penghitungan <i>fuzzy hash</i>	51
Gambar 3.25. Contoh isi <i>database signature</i> menggunakan <i>fuzzy hash</i>	52
Gambar 3.26. Contoh isi <i>database signature</i> menggunakan SHA256	52
Gambar 3.27. <i>Activity Diagram</i> ketika melakukan <i>load file database signature</i>	53
Gambar 3.28. <i>Activity Diagram</i> melihat isi <i>file database signature</i>	53
Gambar 3.29. <i>Activity Diagram</i> ketika melakukan <i>load file</i> yang akan di- <i>scan</i>	53
Gambar 3.30. <i>Activity Diagram</i> ketika melakukan deteksi menggunakan <i>database signature</i> SHA256.....	54
Gambar 3.31. <i>Activity Diagram</i> ketika melakukan deteksi menggunakan <i>database signature fuzzy</i>	55
Gambar 3.32. <i>Activity Diagram</i> ketika dilakukan penghitungan <i>similarity</i>	56
Gambar 3.33. <i>Activity Diagram</i> ketika penentuan nilai <i>similarity threshold</i>	56
Gambar 3.34. <i>Class MainForm</i> pada <i>Dashboard</i>	57
Gambar 3.35. <i>Class ViewSignaturesForm</i> pada <i>Dashboard</i>	58
Gambar 3.36. <i>Class MainForm</i> pada <i>Database Signature Builder</i> beserta relasinya dengan <i>library fuzzy hash</i>	59
Gambar 3.37. <i>Class MainForm</i> pada <i>Malware Detector</i> beserta relasinya dengan <i>library fuzzy hash</i> dan <i>form ViewSignatures</i>	61
Gambar 3.38. <i>Class ViewSignatures</i> pada <i>Malware Detector</i> beserta relasinya dengan <i>library fuzzy hash</i> dan <i>MainForm</i>	62
Gambar 3.39. Rancangan antarmuka <i>form</i> utama pada <i>Dashboard</i>	63
Gambar 3.40. Rancangan antarmuka <i>form view signatures</i> pada <i>Dashboard</i>	64
Gambar 3.41. Rancangan antarmuka aplikasi <i>Database Signature Builder</i>	64
Gambar 3.42. Rancangan antarmuka aplikasi <i>Malware Detector</i>	65
Gambar 3.43. Rancangan antarmuka aplikasi <i>Malware Detector</i> pada <i>form View Signatures</i>	65
Gambar 4.1. Nilai-nilai konstanta yang digunakan dalam <i>class FuzzyHashing</i>	67
Gambar 4.2. Inisialisasi dalam algoritma <i>spamsun</i> sebelum melakukan penghitungan <i>fuzzy hash</i>	67
Gambar 4.3. Proses inisialisasi <i>blocksize</i> , inisialisasi dan <i>update traditional hash</i>	68

Gambar 4.4.	Implementasi proses penghitungan <i>hash</i> hingga menjadi <i>Signature</i> akhir. Lanjutan <i>method Calculate</i> pada gambar 4.2	69
Gambar 4.5.	Implementasi proses yang dilakukan saat menjalankan <i>method Compare</i>	70
Gambar 4.6.	Implementasi proses inisialisasi dalam <i>class LevenshteinDistance</i>	71
Gambar 4.7.	Implementasi proses menghitung <i>distance</i>	71
Gambar 4.8.	Implementasi proses menghitung nilai <i>similarity</i> setelah <i>distance</i> didapat	72
Gambar 4.9.	Antarmuka aplikasi <i>Dashboard</i> . <i>Icon</i> yang digunakan berasal dari <i>IconArchive.com</i>	72
Gambar 4.10.	Implementasi proses eksekusi <i>Database Signature Builder</i> dan <i>Malware Detector</i> dari <i>Dashboard</i>	73
Gambar 4.11.	Antarmuka aplikasi <i>Database Signature Builder</i> setelah dilakukan penghitungan <i>hash fuzzy</i>	73
Gambar 4.12.	Proses ekspor ke dalam <i>file database</i>	74
Gambar 4.13.	Penggunaan <i>class FuzzyHashing</i> pada <i>method CalculateFuzzy</i>	75
Gambar 4.14.	Antarmuka aplikasi <i>Malware Detector</i>	75
Gambar 4.15.	Implementasi proses deteksi <i>malware</i> berdasarkan <i>fuzzy hash</i>	76
Gambar 4.16.	Implementasi proses deteksi <i>malware</i> berdasarkan <i>hash SHA256</i>	77
Gambar 4.17.	Kumpulan <i>file</i> hasil kompilasi <i>library</i> dan aplikasi yang dibangun	78
Gambar 4.18.	Garis besar proses uji coba program	78
Gambar 4.19.	Ilustrasi proses yang dilakukan untuk menghasilkan dua buah <i>file database signature</i> tanpa varian	79
Gambar 4.20.	Ilustrasi proses yang dilakukan untuk menghasilkan dua buah <i>file database signature</i> beserta varian	80
Gambar 4.21.	Antarmuka aplikasi <i>Dashboard</i> . Label di atas <i>status bar</i> menunjukkan lokasi aplikasi dan <i>database</i>	82
Gambar 4.22.	<i>Context-menu</i> yang tampil pada <i>system tray</i>	82
Gambar 4.23.	<i>Message box</i> yang tampil ketika <i>removable drive</i> baru terdeteksi	83
Gambar 4.24.	Aplikasi <i>Malware Detector</i> yang dieksekusi setelah <i>removable drive</i> terdeteksi	83
Gambar 4.25.	<i>Message box</i> yang tampil ketika lokasi <i>Malware Detector</i> dan <i>database signature default</i> belum terkonfigurasi secara benar	84
Gambar 4.26.	Opsi <i>launcher context-menu file explorer</i>	84
Gambar 4.27.	<i>Context-menu</i> baru pada <i>file explorer</i>	84
Gambar 4.28.	Tampilan awal aplikasi <i>Database Signature Builder</i>	85
Gambar 4.29.	<i>Browse folder</i> yang berisi sampel <i>malware</i>	86
Gambar 4.30.	Tampilan aplikasi setelah proses <i>load</i> sampel <i>malware</i>	86
Gambar 4.31.	Pembangunan <i>database signature</i> dengan <i>SHA256</i>	87
Gambar 4.32.	Penyimpanan <i>database signature</i> ke dalam <i>file db.sha256</i>	87
Gambar 4.33.	Pembangunan <i>database signature</i> dengan <i>fuzzy hash</i>	88

Gambar 4.34. Penyimpanan <i>database signature</i> ke dalam <i>file db.fuzzy</i>	88
Gambar 4.35. Pembangunan <i>database signature</i> terhadap 206 sampel <i>malware</i> dengan SHA256.....	89
Gambar 4.36. Penyimpanan <i>database signature</i> ke dalam <i>file db-all.sha256</i>	89
Gambar 4.37. Pembangunan <i>database signature</i> terhadap 206 sampel <i>malware</i> dengan <i>fuzzy hash</i>	90
Gambar 4.38. Penyimpanan <i>database signature</i> ke dalam <i>file db-all.fuzzy</i>	90
Gambar 4.39. <i>Collision hash</i> terjadi dalam proses penyimpanan <i>database signature db-all.fuzzy</i>	91
Gambar 4.40. Tampilan awal aplikasi <i>Malware Detector</i>	92
Gambar 4.41. Tampilan <i>open dialog</i> saat membuka <i>database signature</i>	92
Gambar 4.42. <i>Browse folder</i> yang berisi <i>file</i> atau sampel <i>malware</i> yang ingin dideteksi.....	93
Gambar 4.43. <i>Input</i> batas bawah <i>similarity</i> aktif jika menggunakan <i>database signature fuzzy hash</i>	93
Gambar 4.44. Hasil deteksi db.sha256 terhadap <i>malware</i> beserta varian.....	94
Gambar 4.45. Hasil deteksi db.sha256 terhadap sampel <i>malware</i> beserta varian dan <i>file</i> lain yang dipilih secara acak.....	96
Gambar 4.46. Hasil deteksi db-all.sha256 terhadap sampel <i>malware</i> beserta varian dan <i>file</i> lain yang dipilih secara acak.....	98
Gambar 4.47. Hasil deteksi db.fuzzy terhadap <i>malware</i> beserta varian pada batas kemiripan minimal 25%	99
Gambar 4.48. Hasil deteksi db.fuzzy terhadap <i>malware</i> beserta varian pada batas kemiripan minimal 50%	100
Gambar 4.49. Hasil deteksi db.fuzzy terhadap <i>malware</i> beserta varian pada batas kemiripan minimal 75%	100
Gambar 4.50. Hasil deteksi db.fuzzy terhadap <i>malware</i> beserta varian pada batas kemiripan minimal 100%	101
Gambar 4.51. Hasil deteksi db-all.fuzzy terhadap <i>malware</i> beserta varian pada batas kemiripan minimal 25%	104
Gambar 4.52. Hasil deteksi db-all.fuzzy terhadap <i>malware</i> beserta varian pada batas kemiripan minimal 50%	104
Gambar 4.53. Hasil deteksi db-all.fuzzy terhadap <i>malware</i> beserta varian pada batas kemiripan minimal 75%	105
Gambar 4.54. Hasil deteksi db-all.fuzzy terhadap <i>malware</i> beserta varian pada batas kemiripan minimal 100%	105
Gambar 4.55. Hasil deteksi db.fuzzy terhadap sampel <i>malware</i> beserta varian dan <i>file</i> lain yang dipilih secara acak pada batas kemiripan minimal 25%	108
Gambar 4.56. Hasil deteksi db.fuzzy terhadap sampel <i>malware</i> beserta varian dan <i>file</i> lain yang dipilih secara acak pada batas kemiripan minimal 50%	109
Gambar 4.57. Hasil deteksi db.fuzzy terhadap sampel <i>malware</i> beserta varian dan <i>file</i> lain yang dipilih secara acak pada batas kemiripan minimal 75%	109

Gambar 4.58. Hasil deteksi db.fuzzy terhadap sampel <i>malware</i> beserta varian dan <i>file</i> lain yang dipilih secara acak pada batas kemiripan minimal 100%	110
Gambar 4.59. Hasil deteksi db-all.fuzzy terhadap sampel <i>malware</i> beserta varian dan <i>file</i> lain yang dipilih secara acak pada batas kemiripan minimal 25%	113
Gambar 4.60. Hasil deteksi db-all.fuzzy terhadap sampel <i>malware</i> beserta varian dan <i>file</i> lain yang dipilih secara acak pada batas kemiripan minimal 50%	114
Gambar 4.61. Hasil deteksi db-all.fuzzy terhadap sampel <i>malware</i> beserta varian dan <i>file</i> lain yang dipilih secara acak pada batas kemiripan minimal 75%	114
Gambar 4.62. Hasil deteksi db-all.fuzzy terhadap sampel <i>malware</i> beserta varian dan <i>file</i> lain yang dipilih secara acak pada batas kemiripan minimal 100%	115
Gambar 4.63. Grafik rata-rata waktu yang dibutuhkan untuk menyelesaikan deteksi <i>file</i> dalam ujicoba	118
Gambar 4.64. Grafik perbandingan tingkat deteksi <i>fuzzy hash</i> dan SHA256 dengan 104 <i>hash signature</i> pada masing-masing <i>database</i> terhadap 206 sampel <i>malware</i>	119
Gambar 4.65. Grafik perbandingan tingkat deteksi <i>fuzzy hash</i> dan SHA256 dengan 206 <i>hash signature</i> (205 <i>hash</i> pada <i>database fuzzy</i>) terhadap 206 sampel <i>malware</i>	121
Gambar 4.66. Grafik perbandingan tingkat deteksi <i>fuzzy hash</i> dan SHA256 dengan 104 <i>hash signature</i> pada masing-masing <i>database</i> terhadap 206 sampel <i>malware</i> dan 499 <i>file</i> bersih	122
Gambar 4.67. Grafik perbandingan tingkat deteksi <i>fuzzy hash</i> dan SHA256 dengan 206 <i>hash signature</i> (205 <i>hash</i> pada <i>database fuzzy</i>) pada masing-masing <i>database</i> terhadap 206 sampel <i>malware</i> dan 499 <i>file</i> bersih	124

