Jurnal Coding Sistem Komputer Universitas Tanjungpura
Volume 02 No. 1 (2014), hal 10 – 18

ISSN : 2338-493x

PENGEMBANGAN ANTIVIRUS MENGGUNAKAN METODE *HEURISTIC* GANDA DAN SISTEM *REALTIME PROTECTOR* SERTA PERBANDINGANNYA DENGAN ANTIVIRUS LOKAL

[1]Ardiansyah, [2]Cucu Suhery, [3]Ilhamsyah
[1][2][3]Jurusan Sistem Komputer, Fakultas MIPA Universitas Tanjungpura
Jl. Ahmad Yani, Pontianak
Telp./Fax.: (0561) 577963
e-mail:
[1]ardyprologic@gmail.com, [2]csuhery@gmail.com, [3]ilhamsm99@gmail.com

Abstrak

Pada umumnya antivirus digunakan untuk membersihkan dan melindungi sistem komputer dari infeksi virus komputer. Namun pada saat ini beberapa jenis virus telah berevolusi sehingga dapat lolos dari pendeteksian antivirus, karena antivirus yang digunakan belum menyimpan signature dari virus tersebut. Pada penelitian ini dikembangkan sebuah aplikasi antivirus yang diberi nama Spartan Antivirus yang dapat mendeteksi virus menggunakan signature dan dilengkapi dengan metode pendeteksian heuristic ganda serta sistem realtime protector. Aplikasi antivirus ini juga memiliki process viewer, yaitu sebuah fitur yang memungkinkan user dapat menghentikan sebuah proses yang aktif melalui antivirus tersebut. Hasil dari penelitian ini adalah aplikasi antivirus dapat mendeteksi virus tidak hanya dengan signature saja, tetapi juga dengan metode heuristic ganda dan sistem realtime protector. Antivirus yang dikembangkan dibandingkan dengan antivirus lokal lainnya (Smadav, PC Media Antivirus dan Morphost Antivirus). Kelebihan antivirus ini yaitu memiliki fitur dimana user secara manual dapat menambahkan signature sebuah file yang dicurigai sebagai virus ke database antivirus. Kekurangan antivirus ini adalah waktu yang dibutuhkan dalam proses scanning belum secepat antivirus yang lainnya.

Kata kunci: infeksi, *signature*, *heuristic* ganda, *realtime protector*, *process viewer*, *user*, *scanning*

1. PENDAHULUAN

Pengguna komputer tentunya pernah mengalami masalah yang di-akibatkan oleh virus baik secara langsung maupun tidak langsung. Hal tersebut merupakan masalah yang cukup berat karena harus membersihkan sistem komputernya dari virus secara manual. Virus komputer pada umumnya meng-infeksi sistem komputer, namun lebih buruknya lagi sebagian virus juga dapat menginfeksi file dokumen yang tentunya sangat merugikan bagi pengguna komputer.

Virus komputer merupakan sebuah *software* yang dapat menggandakan atau menyalin dirinya sendiri dan menyebar dengan cara menyisipkan/menginfeksi salinan dirinya ke dalam program lain. Efek yang ditimbulkan oleh virus diantaranya menampilkan pesan yang mengganggu, menginfeksi dan merusak file sistem, menginfeksi dokumen dan lain sebagainya.

Metode *scanning* sebuah antivirus sebaiknya tidak hanya menggunakan pencocokan nilai ceksum CRC32 atau MD5 saja, namun juga menggunakan berbagai teknik lainnya untuk men-deteksi keberadaan virus komputer. Oleh karena itu dibutuhkan sebuah antivirus yang menggunakan metode *heuristic* ganda dan sistem *realtime protector* yang dapat mendeteksi virus dan *malware* lainnya tidak hanya melalui *signature*-nya saja tetapi juga dengan

ISSN : 2338-493x

karakteristik dan tingkah lakunya secara *realtime*.

2. LANDASAN TEORI

2.1. Virus

Secara umum virus komputer merupakan sebuah *software* berbahaya (*malware*) yang dapat menggandakan atau menyalin dirinya sendiri dan menyebar dengan cara menginfeksi/ menyisipkan salinan dirinya ke dalam program maupun menyebarkan program lain yang dapat dieksekusi. Beberapa kemampuan dasar virus (Hartojo Salim, 1990), diantaranya adalah:

a. Kemampuan memperbanyak diri, yaitu kemampuan dasar sebuah virus untuk menduplikasikan dirinya pada sebuah file maupun pada sistem komputer.

b. Kemampuan menyembunyikan diri, yaitu kemampuan sebuah virus untuk menyembunyikan dirinya ketika sedang aktif (sedang menginfeksi) sehingga user tidak akan mengetahui keberadaan virus tersebut.

c. Kemampuan untuk memanipulasi, yaitu kemampuan sebuah virus dalam melakukan tindakan pada sistem, seperti membuat tampilan yang menggangu, merusak dan menghapus file dokumen atau file sistem, serta mengacaukan kerja alat-alat I/O (keyboard, printer, dan lain-lain).

d. Kemampuan mendapatkan informasi, yaitu kemampuan dasar sebuah virus untuk mendapatkan informasi tentang struktur media penyimpanan, diantaranya letak file sistem, letak suatu file, dan sebagainya.

e. Kemampuan untuk memeriksa keberadaan dirinya, yaitu kemampuan dasar virus untuk mencari ID (tanda pengenal) dirinya pada sebuah file atau sistem. Kemampuan virus ini dapat mencegah virus menginfeksi sebuah file atau sistem yang sama secara berulang kali.

2.2. *Worms*

Secara umum *worms* adalah *software* berbahaya (*malware*) yang dapat menyebar dengan cara menggandakan dirinya ke dalam sistem komputer. Beberapa kemampuan dasar *worms* (Achmad Darmal, 2007), diantaranya adalah:

a. Kemampuan memperbanyak diri, yaitu kemampuan dasar suatu *worms* untuk menggandakan dirinya dan menyebar pada sistem komputer melalui perantara media lain seperti disket, *USB drive*, maupun melalui suatu jaringan komputer.

b. Kemampuan rekayasa sosial, yaitu kemampuan dasar suatu *worms* untuk mengelabuhi *user* dengan cara berpura-pura seperti program biasa. Ketika *user* menjalankan program tersebut maka secara otomatis *worms* tersebut akan aktif.

c. Kemampuan menyembunyikan diri, yaitu kemampuan suatu *worms* untuk menyembunyikan dirinya ketika *worms* sedang aktif sehingga *user* tidak mengetahui keberadaan *worms* tersebut.

d. Kemampuan mendapatkan informasi, yaitu kemampuan dasar sebuah *worms* untuk memperoleh informasi yang ia butuhkan, seperti jenis sistem operasi, direktori *system* windows, memeriksa antivirus dan lain sebagainya.

e. Kemampuan mengadakan manipulasi, yaitu kemampuan suatu *worms* untuk memanipulasi *registry* agar *worms* dapat aktif saat komputer dihidupkan, bahkan *worms* dapat memanipulasi *registry* milik suatu antivirus agar tidak menganggu *worms* tersebut.

2.3. *Trojan Horse*

Secara umum *trojan horse* dapat diartikan sebagai sebuah *software* berbahaya (*malware*) yang memiliki kemampuan dalam pengontrolan atau pengaksesan data antar jaringan.

Beberapa jenis *trojan* berdasarkan fungsi dan kemampuannya (S'to, 2010), yaitu:

ISSN : 2338-493x

a. *Trojan Remote Access*, yaitu jenis *trojan* yang bekerja dengan cara membuka sebuah *port* secara diam-diam sehingga *hacker* bisa mengen-dalikan komputer korban.
b. *Trojan Data-Sending*, yaitu suatu jenis *trojan* yang bertujuan untuk mengirimkan data-data tertentu (*pass-word*, data *credit card*, dan sebagainya) yang berada pada komputer korban ke sebuah *email* khusus yang telah disiapkan.
c. *Trojan Destructive*, yaitu suatu jenis *trojan* yang sangat berbahaya karena jika telah menginfeksi sistem kom-puter maka *trojan* ini akan menghapus semua file sistem pada komputer korban (seperti file .dll, .ini atau .exe).
d. *Trojan DoS Attack*, yaitu suatu jenis *trojan* yang memiliki kemampuan untuk menjalankan *Distributed DoS (DDoS)* melalui komputer korban.
e. *Trojan Proxy*, yaitu suatu jenis *trojan* yang berfungsi untuk membuat kom-puter korban menjadi seperti sebuah komputer perantara/*proxy*, sehingga *hacker* dapat menyembunyikan identitas dirinya ketika melakukan kegiatan ilegal menggunakan komputer tersebut.
f. *Trojan FTP*, yaitu sebuah jenis *trojan* yang paling sederhana karena hanya memiliki sebuah fungsi yaitu membuka *port* 21 di komputer korban.
g. *Trojan Software Detection Killers*, yaitu jenis *trojan* yang memiliki kemampuan untuk mendeteksi dan melumpuhkan fungsi antivirus dan *firewall* pada sistem komputer.

2.4. Antivirus

Antivirus adalah sebuah program komputer yang dapat mendeteksi, melumpuhkan (mematikan kinerja virus) serta menghapus virus komputer dan program berbahaya lainnya.

Antivirus dapat dibagi menjadi tiga jenis (Aat Shadewa, 2007), diantaranya:
a. *Fix*, yaitu sebuah *software* yang dapat mendeteksi dan menghapus hanya satu jenis virus.
b. *Antidot*, yaitu sebuah *software* yang dapat mendeteksi dan menghapus beberapa jenis virus.
c. Antivirus, yaitu sebuah *software* yang dapat mendeteksi, melumpuhkan dan menghapus banyak jenis virus, dan umumnya akan langsung aktif ketika komputer dijalankan.

2.5. Perangkat Lunak Pendukung

Perangkat lunak pendukung adalah *software* yang digunakan dalam penelitian, baik dalam menganalisa virus, perancangan antivirus, hingga pengujian antivirus.

Perangkat lunak pendukung yang digunakan adalah:
a. Visual Basic, yaitu sebuah bahasa pemrograman yang merupakan *event driven programing* (pemrograman terkendali kejadian) yang berarti program akan menunggu respon berupa *event* atau kejadian tertentu (tombol diklik, menu dipilih dan lain-lain) dari *user*.
b. Sandboxie, yaitu sebuah *software* yang berfungsi membuat direktori bayangan (*virtual drive*) pada sebuah sistem komputer, sehingga mampu mengamankan sistem komputer dari serangan virus maupun kerusakan *registry*.
c. Process explorer, yaitu sebuah *soft-ware* yang berfungsi untuk melihat dan menghentikan proses yang sedang aktif pada sistem.
d. Deep freeze, yaitu sebuah *software* yang berfungsi untuk melindungi sistem komputer dengan cara membekukan *drive* sehingga walaupun terjadi keru-sakan pada sistem, ketika windows di-*restart* maka sistem akan kembali seperti keadaan awal.
e. UPX atau *Ultimate Packer for eXecutables*, yaitu sebuah *software* yang berfungsi untuk mengkompres ukuran dari suatu file *executable* (exe).

3. METODE PENELITIAN

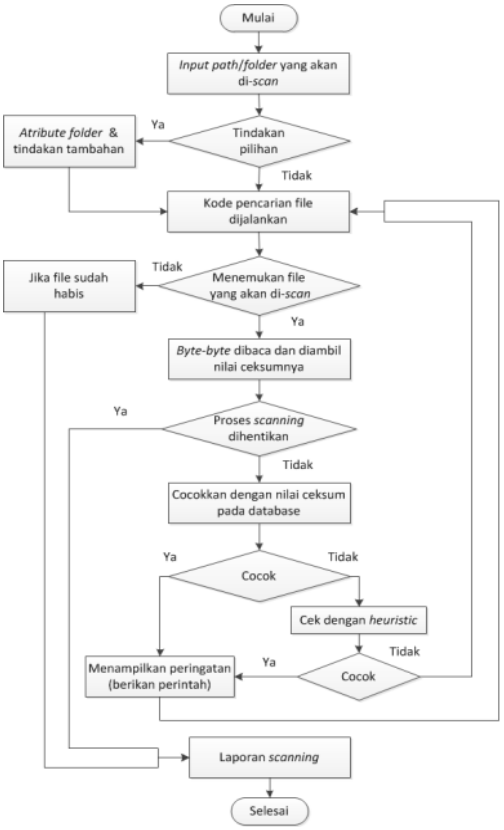
Pada penelitian ini terdapat beberapa tahap yang dilakukan, yaitu

ISSN : 2338-493x

studi pustaka guna mempelajari teori-teori sebagai acuan dalam penelitian ini, proses penelitian (perancangan *flow-chart* antivirus, perancangan desain, metode *heuristic* ganda dan sistem *realtime protector*), analisa kebutuhan, integrasi dan pengujian aplikasi anti-virus dengan sampel virus guna mengetahui rasio atau akurasi pendeteksian antivirus tersebut, setelah itu dilakukan analisa terhadap hasil pengujian dan dibandingkan dengan beberapa antivirus lokal (Smadav, PC Media Antivirus dan Morphost Antivirus) kemudian menarik kesimpulan mengenai kelebihan dan kekurangannya.

4. PERANCANGAN DAN IMPLEMENTASI

4.1. Perancangan *Flowchart* Antivirus



Gambar 1. *Flowchart* Antivirus

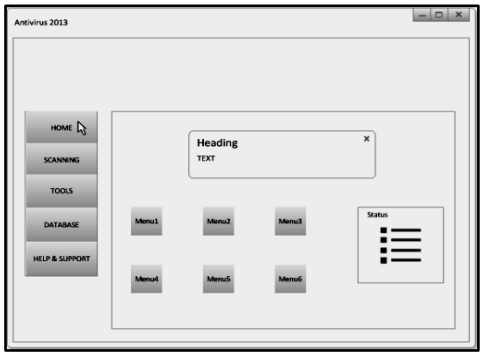
Perancangan *Flowchart* antivirus ini merupakan gambaran umum dimana antivirus membaca sebuah file dan menentukan apakah file tersebut merupakan sebuah virus atau bukan melalui *checksum error* pada database atau melalui metode *heuristic* ganda.

Flowchart antivirus yang digunakan dalam penelitian ini ditunjukkan pada gambar 1.

4.2. Perancangan Desain Antivirus

Pada perancangan desain antivirus terdapat beberapa tombol pilihan menu seperti menu *home*, menu *scanning*, menu *tools*, menu *database* dan menu *help & support*.

Desain antivirus yang digunakan dalam penelitian ini ditunjukkan pada gambar 2.



Gambar 2. Desain Antivirus

Menu-menu pada antivirus tersebut dimaksudkan untuk mempermudah *user* dalam penggunaan antivirus tersebut. Menu *home* antivirus berguna untuk memberikan keterangan tentang antivirus, seperti fitur yang dimiliki, jenis *heuristic*, database virus dan lain-lain. Menu *scanning* antivirus berguna untuk memberikan perintah pada antivirus, di lokasi mana yang akan diperiksa. Menu ini juga berfungsi untuk memulai dan memberhentikan proses *scanning*. Menu *tools* antivirus berguna untuk memberikan pilihan *tools* tambahan jika diperlukan. *Tools* tambahan tersebut berupa program bawaan dari windows, seperi *regedit*, *on-screen keyboard, command prompt, task manager* dan sebagainya. M*enu database* antivirus digunakan untuk menampilkan *database list* serta

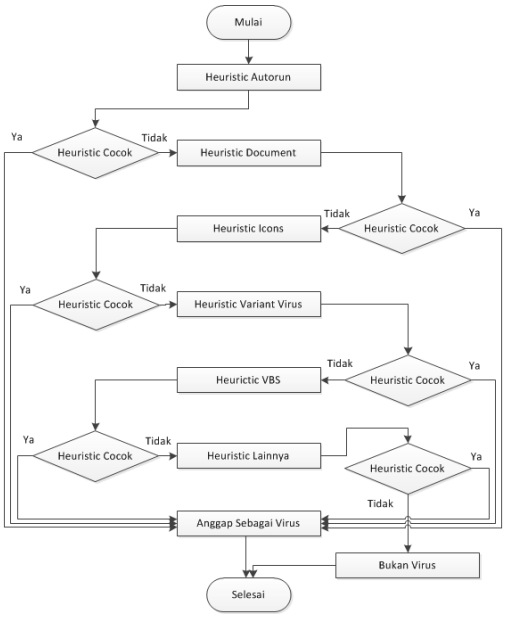
ISSN : 2338-493x

quarantine list. Pada menu tersebut juga terdapat pilihan yang bisa digunakan oleh *user* untuk menambahkan *signature* virus secara manual. M*enu help & support* antivirus berguna untuk memberikan penjelasan bagaimana cara menggunakan antivirus, cara *update* database, dan bantuan lain sebagainya serta menampilkan ucapan terima kasih kepada pihak-pihak yang telah membantu dalam pengembangan antivirus ini.

4.3. Perancangan *Flowchart* Metode *Heuristic* Ganda

Pada perancangan *flowchart* metode *heuristic* ganda, terdapat beberapa metode *heuristic* yang digunakan oleh antivirus untuk mendeteksi keberadaan virus.

Flowchart metode *heuristic* ganda yang digunakan dalam penelitian ini ditunjukkan pada gambar 3.



Gambar 3. *Flowchart* Metode *Heuristic* Ganda

Flowchart metode *heuristic* ganda ini merupakan gambaran umum dimana antivirus melakukan pencocokan *string* dengan beberapa metode *heuristic* yang dimilikinya seperti *Heuristic Autorun*, *Heuristic Document*, *Heuristic Icons*, *Heuristic Variant Virus* dan *Heuristic VBS*.

Metode *Heuristic Autorun* digunakan untuk mendeteksi jenis virus yang memanfaatkan file *autorun.inf* agar dapat berjalan secara otomatis. Pada umumnya virus jenis ini sering ditemukan pada *USB drive*. Metode *Heuristic Document* digunakan untuk mendeteksi jenis virus yang menginfeksi suatu file dokumen. Umumnya file dokumen yang terinfeksi tersebut akan menjadi sebuah file *executable* (.exe atau .scr). Metode *Heuristic Icons* digunakan untuk mendeteksi jenis virus berdasarkan *icon* yang digunakan. Umumnya virus yang terdeteksi dengan metode ini menggunakan *icon text*, *icon image*, *icon folder* dan sebagainya. Metode *Heuristic Variants Virus* digunakan untuk mendeteksi jenis virus yang memiliki kemiripan *string* dengan beberapa varian atau jenisnya yang lain. Sedangkan Metode *Heuristic VBS* digunakan untuk mendeteksi jenis virus yang memanfaatkan fasilitas *script* seperti *VBScript*.

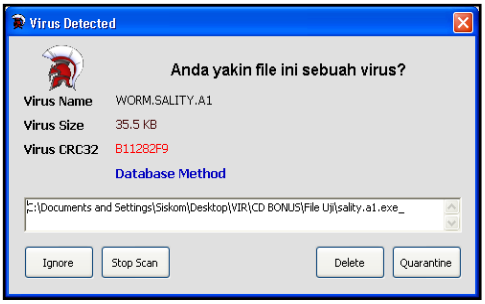
5. HASIL DAN PEMBAHASAN

5.1. Metode *Checksum Error*

Pengujian menggunakan metode *checksum error* dilakukan berdasarkan dengan pencocokan nilai *CRC32* virus dengan database. Jika nilai *CRC32* sebuah file belum terdapat pada database maka file tersebut tidak akan dianggap virus, namun jika nilainya sudah terdapat pada database maka akan dianggap sebagai virus.

Hasil pengujian antivirus menggunakan metode *checksum error* ditunjukkan pada gambar 4.

ISSN : 2338-493x



Gambar 4. Pengujian Menggunakan Metode *Checksum Error*

Pada hasil pengujian ini ditunjukkan oleh gambar 4, sebuah file dengan *virus name* "Worm.Sality.1", *virus size* "35,5 KB" *virus CRC32* "B11282F9" terdeteksi menggunakan metode database atau *checksum error*. Sebelumnya nilai *CRC32* dari file virus ini telah tersimpan pada database sehingga ketika file ini terdeteksi maka akan langsung dianggap sebagai virus.

5.2. Metode *Heuristic* Ganda

5.2.1. Metode *Heuristic Autorun*

Pengujian menggunakan metode *heuristic autorun* dilakukan berdasarkan dengan pendeteksian file "autorun.inf" yang dapat memicu file virus untuk berjalan secara otomatis. Hasil pengujian antivirus menggunakan metode *heuristic autorun* mirip seperti gambar 4, hanya saja *virus name*, *virus size*, *virus CRC32* dan metode pendeteksiannya saja yang berbeda.

Pada hasil pengujian ini, sebuah file "autorun.inf" terdeteksi sebagai sebuah virus dengan *virus name* "Heur. Autorun(2) virus", *virus size* 0,19 KB", *virus CRC32* "17FFF7AB" dan metode pendeteksian "Heuristic Method". File tersebut terdeteksi menggunakan metode *heuristic autorun* karena memiliki *string* sensitif seperti yang digunakan pada metode *heuristic autorun*.

5.2.2. Metode *Heuristic Document*

Pengujian menggunakan metode *heuristic document* dilakukan dengan cara memeriksa apakah sebuah file *executable* mengandung *string* file dokumen atau tidak. Hasil pengujian antivirus menggunakan metode *heuristic document* mirip seperti gambar 4, hanya saja *virus name*, *virus size*, *virus CRC32* dan metode pendeteksiannya saja yang berbeda.

Pada hasil pengujian ini, sebuah file terdeteksi sebagai sebuah virus dengan *virus name* "Worms.Infeks.2", *virus size* "201,5 KB", *virus CRC32* "9295999A" dan metode pendeteksian yaitu "Doc Heuristic". File tersebut terdeteksi sebagai sebuah virus karena memiliki *string* sensitif yang digunakan pada metode *heuristic document*.

5.2.3. Metode *Heuristic Icons*

Pengujian menggunakan metode *heuristic icon* dilakukan berdasarkan dengan pencocokan nilai *byte icon* yang digunakan sebuah file dengan nilai *byte icon* yang dijadikan *string* pada *heuristic icons.* Hasil pengujian antivirus menggunakan metode *heuristic icons* mirip seperti gambar 4, hanya saja *virus name*, *virus size*, *virus CRC32* dan metode pendeteksiannya saja yang berbeda.

Pada hasil pengujian ini,sebuah file *executable* terdeteksi sebagai sebuah virus dengan *virus name* "Stration. Variant", virus size "64 KB", *virus CRC32* "92542815" dan metode pendeteksian yaitu "Icon Heuristic". File *executable* tersebut menggunakan *icon text* yang sebenarnya hanya digunakan oleh file bertipe *text*, sehingga terdeteksi sebagai virus dengan metode *heuristic icons.*

5.2.4. Metode *Heuristic Variant Virus*

Pengujian menggunakan metode *heuristic variant virus* dilakukan berdasarkan dengan pencocokan *string* yang terdapat pada antivirus dengan *string* yang terdapat pada sebuah file. Hasil pengujian antivirus meng-gunakan metode *heuristic variant virus* mirip seperti gambar 4, hanya saja *virus name*, *virus size*, *virus CRC32* dan metode pendeteksiannya saja yang berbeda.

Jurnal Coding Sistem Komputer Universitas Tanjungpura
Volume 02 No. 1 (2014), hal 10 – 18

ISSN : 2338-493x

Pada hasil pengujian ini,sebuah file *executable* terdeteksi sebagai sebuah file terinfeksi dengan *virus name* "Win. Almanahe.A", virus size "148 KB", *virus CRC32* "6CF7E7D8" dan metode pendeteksian yaitu "Smart Heuristic". File tersebut telah terinfeksi oleh sebuah virus sehingga memiliki *string* sensitif yang sama dengan *string* pada *metode heuristic variant virus.*

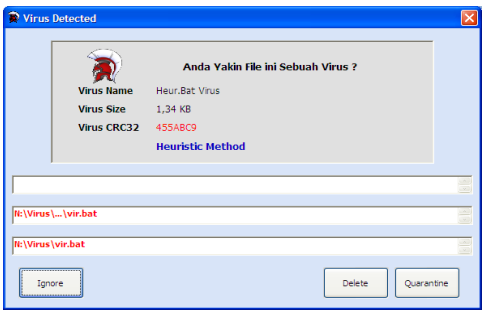
5.2.5. Metode *Heuristic VBS*

Pengujian menggunakan metode *heuristic VBS* dilakukan berdasarkan dengan pencocokan *string* sensitif pada antivirus dengan *string* yang terdapat pada sebuah file *VBS*. Hasil pengujian antivirus menggunakan metode *heuristic VBS* mirip seperti gambar 4, hanya saja *virus name*, *virus size*, *virus CRC32* dan metode pendeteksiannya saja yang berbeda.

Pada hasil pengujian ini,sebuah file *VBS* terdeteksi sebagai sebuah virus dengan *virus name* "Heur.VBS Virus", virus size "4.15 KB", *virus CRC32* "1D8C1FDD" dan metode pendeteksian "Heuristic Method". File tersebut memiliki *string* sensitif yang sama dengan *string* pada metode *heuristic VBS.*

5.3. Sistem *Realtime Protector*

Pengujian sistem *realtime protector* dilakukan dengan cara membuka sebuah *path/folder* yang berisi virus. Jika *realtime protector* mendeteksi adanya keberadaan sebuah virus, maka *realtime protector* telah berjalan dengan baik.



Gambar 5. Pengujian Sistem *Realtime Protector*

Hasil pengujian sistem *realtime protector* antivirus ditunjukkan pada gambar 5.

Pada gambar 5 menunjukkan sistem *realtime protector* mendeteksi sebuah file sebagai virus. Pada hasil pengujian ini, sebuah file terdeteksi sebagai virus dengan *virus name* "Heur.Bat Virus", *virus size* "1,34 KB", *virus CRC32* "455ABC9" dan metode pendeteksian yaitu "Heuristic Method"

Sistem *realtime protector* ini telah terintegrasi dengan metode *checksum error* dan metode *heuristic ganda*, sehingga akurasi pendeteksiannya sama dengan ketika antivirus melakukan proses *scanning.*

5.4. Perbandingan Fitur Beberapa Antivirus Lokal

Pada tabel 1 dapat dilihat perbandingan fitur antivirus yang dikembangkan (Spartan Antivirus) dengan beberapa antivirus lokal yang ada di Indonesia yaitu Smadav, PC Media Antivirus dan Morphost Antivirus.

Tabel 1. Perbandingan Fitur Antivirus Lokal

NO	PERBANDINGAN	ANTIVIRUS			
		SMADAV	PCMAV	MORPHOST AV	SPARTAN AV
1	Realtime Protector	Ada	Ada	Ada	Ada
2	Process Viewer	Ada	Tidak	Tidak	Ada
3	Updated	Ada	Ada	Tidak	Ada
4	Add Virus Sign Manually	Tidak	Tidak	Tidak	Ya
5	Website resmi	smadav.net	pcmav.net	morphostlab.com/ morphost-antivirus	~

Beberapa parameter yang menjadi acuan dalam perbandingan antivirus ini diantaranya adalah *realtime protector*, *process viewer*, *updated*, *add virus sign manually*, serta *website* resmi sebagai sarana publikasi antivirus.

Pada parameter pertama yaitu *realtime protector*, keempat antivirus memiliki fitur ini. Pada parameter kedua yaitu *process viewer*, hanya Smadav dan Spartan Antivirus yang memiliki fitur ini. Pada parameter ketiga yaitu fitur

ISSN : 2338-493x

updated, Smadav, PC Media Antivirus dan Spartan Antivirus memiliki fitur ini. Pada parameter keempat *yaitu add virus sign manually*, hanya Spartan Antivirus yang memiliki fitur ini. Pada parameter kelima yaitu *website* resmi, Smadav, PC Media Antivirus dan Morphost memiliki *website* resmi sedangkan Spartan Antivirus belum memiliki *website* resminya

5.5. Perbandingan *Scanning* Beberapa Antivirus Lokal

Pada tabel 2 dapat dilihat perbandingan *scanning* antivirus yang dikembangkan (Spartan Antivirus) dengan beberapa antivirus lokal yang ada di Indonesia yaitu Smadav, PC Media Antivirus dan Morphost Antivirus.

Tabel 2. Perbandingan *Scanning* Antivirus Lokal

NO	PERBANDINGAN	ANTIVIRUS			
		SMADAV	PCMAV	MORPHOST AV	SPARTAN AV
	Version	9.5	9.3	8	2.0
	Heuristic Engine	Ada	Ada	Ada	Ada
	Signatures + Heuristic	4153 +	7222	813 +	1327 +
1	Virus Sample	50	50	50	50
2	Scanning Time (m:s)	00:11	00:16	00:14	00:23
3	Virus Detected	49	23	43	47
4	Virus Quarantine/Delete	49	23	43	47
5	Error Quarantine/Delete	0	0	0	0
6	Detected Ratio (%)	98%	46%	86%	94%

$$\text{rasio (\%)} = \left(\frac{\text{virus detected}}{\text{virus sample}}\right).100$$

Beberapa parameter yang menjadi acuan dalam perbandingan *scanning* antivirus ini diantaranya adalah jumlah *virus sample*, *scanning time(m:s)*, *virus detected*, *virus quarantine/delete*, *error quarantine/delete* dan *detected ratio(%)*.

Pada parameter pertama semua antivirus diuji dengan *virus sample* sebanyak 50 virus. Pada parameter kedua yaitu *scanning time*, Smadav melakukan proses *scanning* dengan waktu 11 detik, Morphost Antivirus dengan waktu 14 detik, PC Media Antivirus dengan waktu 16 detik dan Spartan Antivirus dengan waktu 25 detik. Pada parameter ketiga yaitu *virus detected*, smadav mampu mendeteksi virus sebanyak 49 virus, Spartan Antivirus sebanyak 47 virus, Morphost Antivirus sebanyak 43 virus dan PC Media Antivirus sebanyak 23 virus. Pada parameter keempat yaitu *virus quarantine/delete*, semua antivirus dapat mengkarantina/menghapus semua virus yang dideteksinya. Pada parameter kelima yaitu *error quarantine/delete*, semua antivirus tidak mengalami error saat mengkarantina/menghapus virus yang dideteksinya. Pada parameter keenam yaitu *detected ratio*, Smadav memiliki rasio 98%, Spartan Antivirus memiliki rasio 94%, Morphost Antivirus memiliki rasio 86% dan PC Media Antivirus memiliki rasio 46%.

6. KESIMPULAN DAN SARAN

6.1. Kesimpulan

Setelah dilakukan pengujian dan analisis terhadap antivirus yang dikembangkan (Spartan Antivirus), maka dapat ditarik kesimpulan sebagai berikut:

1. Cara untuk mendeteksi, melumpuhkan (mematikan kinerja virus) dan menghapus virus komputer dengan metode *heuristic* ganda adalah dengan menguji dan menganalisa sampel virus, kemudian membuat metode *heuristic*-nya berdasarkan ciri-ciri maupun tingkah laku dari virus tersebut.
2. Sistem *realtime protector* sangat efektif dalam melindungi sistem komputer dari serangan virus, karena sistem ini mampu mendeteksi keberadaan virus walaupun antivirus tidak sedang melakukan proses *scanning*. Sistem *realtime protector* telah diuji sebanyak 10 kali dengan sampel *malware* (virus, *worms* dan *trojan*) dan didapat rasio 100% dalam peng-ujian tersebut.
3. Pada perbandingan fitur beberapa antivirus lokal, antivirus yang dikembangkan memiliki kelebihan dari antivirus lokal lain (Smadav, PC Media Antivirus dan Morphost Anti-virus) yaitu memiliki sebuah fitur dimana *user*

ISSN : 2338-493x

dapat menambahkan secara manual signature sebuah file yang dicurigai sebagai virus ke database antivirus. Kekurangan dari antivirus ini adalah belum memiliki *website* resmi sebagai sarana untuk publikasinya.

4. Pada perbandingan *scanning* beberapa antivirus lokal, antivirus yang dikembangkan memiliki rasio atau akurasi pendeteksian sebesar 94%. Kelebihan dari antivirus ini adalah akurasi pendeteksiannya sudah cukup tinggi, bahkan untuk virus yang sebelumnya masih luput dari pendeteksiannya, akan bisa dideteksi dengan cara menambahkan *signature* virus tersebut secara manual ke database antivirus menggunakan fitur *add sign virus manually*. Kekurangan antivirus ini adalah waktu yang diperlukan dalam proses *scanning* belum secepat antivirus lainnya.

6.2. Saran

Metode *heuristic* yang digunakan dalam pengembangan antivirus ini hanyalah beberapa jenis dari metode pendekatan yang dapat digunakan sebagai metode untuk mendeteksi virus. Ada beberapa metode yang dapat digunakan dalam pendeteksian sebuah virus seperti metode ceksum MD5, *PE Header*, *dropper virus* dan lain-lain.

Antivirus yang dikembangkan menggunakan file *text* sebagai database eksternalnya. Ada beberapa pilihan database lain yang dapat digunakan pada antivirus, yaitu dengan database .MDB, .SQL, maupun .XLS. Namun akan lebih baik jika database antivirus menggunakan ekstensi sendiri dan terenkripsi sehingga file database akan lebih aman.

Maka dari itu penulis berharap agar antivirus ini nantinya dapat dikembangkan lebih lanjut dengan optimasi algoritma dan penambahan lebih banyak *heuristic* maupun database virus agar kualitas antivirus ini menjadi semakin baik dan dapat bersaing dengan antivirus lokal yang ada sebagai salah satu aplikasi proteksi tambahan yang dapat melindungi komputer dari serangan virus.

DAFTAR PUSTAKA

[1] Darmal, Achmad. 2006. *Computer Worm 1 - Secret of Underground Coding*. Jasakom.

[2] Salim, Hartojo. 1990. *Virus Komputer*. Andi Offset: Yogyakarta.

[3] Shadewa, Aat. 2007. *Rahasia Membuat Antivirus Menggunakan Visual Basic*. DSI Publishing: Yogyakarta.

[4] S'to. 2010. *CEH (Certified Ethical Hacker):300% Illegal*. Jasakom.