IT Journal Research and Development
Vol.3, No.1, Agustus 2018 e-ISSN: 2528-4053
DOI : 10.25299/itjrd.2018.vol3(1).1884

Rancang Bangun Sistem Keamanan Data Komputer Pada Antivirus Vici Menggunakan Sistem Realtime Protector dan Metode Heuristic Ganda

Yuni Selvita Suci[1], Aryanti Aryanti[2], Asriyadi[3]
[1,2,3]Jurusan Teknik Elektro, Program Studi Teknik Telekomunikasi, Politeknik Negeri Sriwijaya
[1]uciaisaka@gmail.com , [2]aryanti@polsri.ac.id, [3]asriyadi@polsri.ac.id

Abstract

In this study an antivirus application named Antivirus Vici that can detect the presence of viruses using the signature and equipped with dual heuristic method and realtime protector system. This antivirus application also has a process viewer, a feature that allows users to stop an active process through the virus. The result of this research is antivirus application can detect virus not only with signature but also with double heaurisc method and realtime protector system. The advantages of this antivirus feature is that users can manually add the signature of a suspected virus file into the antivirus database. The lack of this antivirus is not able to be used on the operating system under windows xp

Keywords : *Antivirus, Heuristic , Realtime Protector, Virus, Visual Basic*

Abstrak

Pada penelitian ini sebuah aplikasi antivirus diberi nama Antivirus Vici yang dapat mendeteksi keberadaan virus menggunakan signature dan dilengkapi dengan metode heuristic ganda dan sistem *realtime protector*. Aplikasi antivirus ini juga memiliki *process viewer*, yaitu fitur yang memungkinkan user dapat menghentikan sebuah proses yang aktif melalui virus tersebut. Hasil dari penelitian ini adalah aplikasi antivirus dapat mendeteksi virus tidak hanya dengan *signature* saja tapijuga dengan metode heauristic ganda dan sistem *realtime protector*. Kelebihan antivirus ini yaitu memliki fitur dimana user secara manual dapat menambahkan *signature* sebuah file yang dicurigai sebagai virus ke dalam database antivirus. Kekurangan antivirus ini adalah belum bisa digunakan pada sistem operasi dibawah windows xp 2.

Kata kunci: Antivirus, Heuristic, Realtime Protector, Virus, Visual Basic

1. PENDAHULUAN

Virus komputer umumnya dapat merusak perangkat lunak komputer dan tidak dapat secara langsung merusak perangkat keras komputer, tetapi dapat mengakibatkan kerusakan dengan cara membuat program yang memaksa *over process* ke perangkat tertentu. Efek negatif virus komputer adalah memperbanyak dirinya sendiri yang membuat sumber daya komputer (seperti penggunaan memori) menjadi berkurang secara signifikan. Hampir 95% virus komputer berbasis sistem operasi windows. Sisanya menyerang Linux/GNU, Mac, FreeBSD, OS/2 IBM, dan sun Operating System. Virus ang ganas akan merusak perangkat keras [1]. Solusi untuk mengatasi masalah dibuatlah suatu aplikasi yang disebut antivirus. Sesuai dengan namanya, program antivirus mampu

IT Journal Research and Development
Vol.3, No.1, Agustus 2018 e-ISSN: 2528-4053
DOI : 10.25299/itjrd.2018.vol3(1).1884

mendeteksi dan mencegah akses ke dokumen yang terinfeksi dan juga mampu menghilangkan infeksi yang terjadi [2]. Keamaan komputer yaitu suatu cabang teknologi yang disebut dengan keamanan informasi terhadap komputer [3]. Ditinjau dari segi kemampuan, kriteria virus dibagi menjadi 5 hal antara lain:[4]

1. Kemampuan untuk mendapatkan informasi
2. Kemampuan memeriksa suatu program
3. Kemampuan untuk menggandakan diri
4. Kemampuan mengadakan manipulasi
5. Kemampuan menyembunyikan diri

Dalam penelitian [2] telah melakukan pengujian antivirus dengan menggunakan metode tersebut telah berhasil tetapi hanya untuk mendeteksi virus H1N1. Selanjutnya dari penelitan [5] telah berhasil melakukan pengujian antivirus dengan metode tersebut tetapi dalam pengimplementasiannya belum dapat melakukan proteksi PC dan antivirus itu sendiri dalam perlindungan *realtime*.

Berdasarkan referensi tersebut maka akan dilakukan penelitian terhadap metode Heuristic Ganda dan Sistem Realtime Protector dalam mengidentifikasi virus berdasarkan kriteria yang ada yaitu menghapus file, merusak file, menggandakan dan memanipulasi file. Metode *Heuristic Ganda* digunakan untuk mendeteksi, mematikan kinerja virus, dan menghapus virus komputer, sehingga meskipun *virus* sudah melakukan modifikasi terhadap *byte-byte* tertentu, namun pada *pattern* atau pola *virus* secara keseluruhan tidak akan berubah di mana hal ini dapat memudahkan antivirus untuk mendeteksi *virus* dengan kemampuan *polymorph* kemudian Sistem *realtime protector* dimana dalam pengimplemntasiannya sangat efektif dalam melindungi sistem komputer dari serangan virus, karena sistem ini mampu memproteksi komputer dari keberadaan virus walaupun antivirus tidak sedang melakukan proses scanning.

Perancangan antivirus dilakukan dengan menggunakan Visual Basic 6.0 dengan penamaan aplikasi antivirus adalah antivirus Vici yang menerapkan kedua metode tersebut untuk mengatasi virus komputer. Adapun tujuan yang ingin dicapai dalam penelitian ini untuk membuat antivirus yang dapat menghapus dan medeteksi virus dan melakukan pengujian antivirus menggunakan Metode Heuristic Ganda dan Sistem Realtime Protector yang dirancang dengan Visual Basic 6.0.

2. METODE PENELITIAN

2.1. Kerangka Penelitian

Berdasarkan batasan masalah yang telah dijabarkan sebelumnya, maka sampel penelitian yang digunakan dalam penelitian ini adalah file yang dianggap virus dan worm yang pada umumnya memiliki format file berupa exe,com, vbs, bat, scr, dll, db dan lain nya.

Gambar 1. Kerangka Penelitian Secara Keseluruhan

IT Journal Research and Development
Vol.3, No.1, Agustus 2018 e-ISSN: 2528-4053
DOI : 10.25299/itjrd.2018.vol3(1).1884

2.2. Pengumpulan Data

Salah satu faktor penting dalam pembangunan/pengembangan sistem informasi ialah memahami sistem yang ada dan permasalahannya. Adapun uraian secara konkret
dari teknik pengumpulan data penelitian ini akan diuraikan sebagai berikut :

1. Studi Pustaka
2. Ekperimen
3. Dokumentasi

2.3. Konsep Teori

2.2.1 Pengertian Virus

Secara umum virus komputer merupakan sebuah software berbahaya (*malware*) yang dapat menyalin dirinya sendiri dan menyebar dengan cara menginfeksi/menyisipkan salinanya kedalam program maupun menyebarkkan program lain yang dapat di eksekusi. Beberapa kemampuan dasar virus[6], diantaranya adalah:

1. Kemampuan untuk memperbanyak diri.
2. Kemampuan menyembunyikan diri.
3. Kemampuan untuk memanipulasi.
4. Kemampuan mendapatkan informasi.
5. Kemampuan untuk memeriksa keberadaan dirinya.

Penggolongan atau pengelompokkan terhadap virus dapat dilakukan dengan beberapa metode klasifikasi. Beberapa metode yang sangat bagus menggunakan naïve bayes antara lain digunakan dalam klasifikasi deteksi *email spam*[7]. Beberapa kemampuan dasar *worms*, di-antaranya adalah [8]:

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 manipu-lasi, 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.

2.2.2. Pengertian 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 [9], diantaranya:

1. *Fix*, yaitu sebuah *software* yang dapat mendeteksi dan menghapus hanya satu jenis virus.

IT Journal Research and Development
Vol.3, No.1, Agustus 2018 e-ISSN: 2528-4053
DOI : 10.25299/itjrd.2018.vol3(1).1884

2. *Antidot*, yaitu sebuah *software* yang dapat mendeteksi dan menghapus beberapa jenis virus.
3. *Antivirus*, yaitu sebuah *software* yang dapat mendeteksi, melumpuhkan dan menghapus banyak jenis virus, dan umumnya akan langsung aktif ketika komputer dijalankan.

2.2.3. Pengertian Heuristic Ganda

Metode Heuristic adalah teknik yang dipakai setelah penggunaan ceksum dalam pendeteksian virus (file). Heuristicadalah teknik pendekatan untuk mencurigai bahwa sebuah file adalah virus atau bukan. Bahkan, dengan heuristic-heuristic canggih sebuah program visua yang sengaja dibuat untuk menjebak orang lain pun mampu dideteksi kandungan code-code berbahayanya. Heuristic sendiri sangat bervariasi, sesuai kecerdasan dan pengalaman pembuatannya [10].

2.2.4. Pengertian Realtime Protector

Real-time Protection adalah suatu metode yang amat penting dalam software antivirus, dalam usaha melindungi sistem komputer. Ini bisa dianggap sebagai *standar* pada program antivirus yang baik [11]. Banyak istilah (sinonim) yang digunakan untuk fitur *real-time protection* ini. Misalnya : Resident Shield, On-access Scanning, Background Guard, System Shield, Auto Protect dll. Semuanya mengacu pada cara otomatis dalam melindungi komputer dari serangan malware.

2.2.5 Pengertian Visual Basic

Microsoft Visual basic (sering disingkat sebagai VB saja) merupakan sebuah bahasa pemograman yang menawarkan Integrated Development Environment (IDE) visual untuk membuat pemograman perangkat lunak berbasis sistem operasi Microsoft Windows dengan menggunakan model pemograman (COM) [12].

2.3. Perancangan Sistem

2.3.1 Perancangan Perangkat Keras

Dalam pnelitian ini penulis melakukan pengujian menggunakan beberapa perangkat keras pendukung lainnya yang dapat menjadi faktor perangkat keras yang dibangun dapat berjalan dengan baik, diantaranya :

1. Komputer atau laptop dengan processor minimal core i3.
2. Memori minimal 16Mb.

2.3.2 Perancangan Perangkat Lunak

Pada penelitian ini penulis menggunakan sampel virus dan beberapa perangkat lunak pendukung lainnya yang dapat menjadi faktor perangkat lunak yang dibangun dapat berjalan dengan baik, diantaranya :

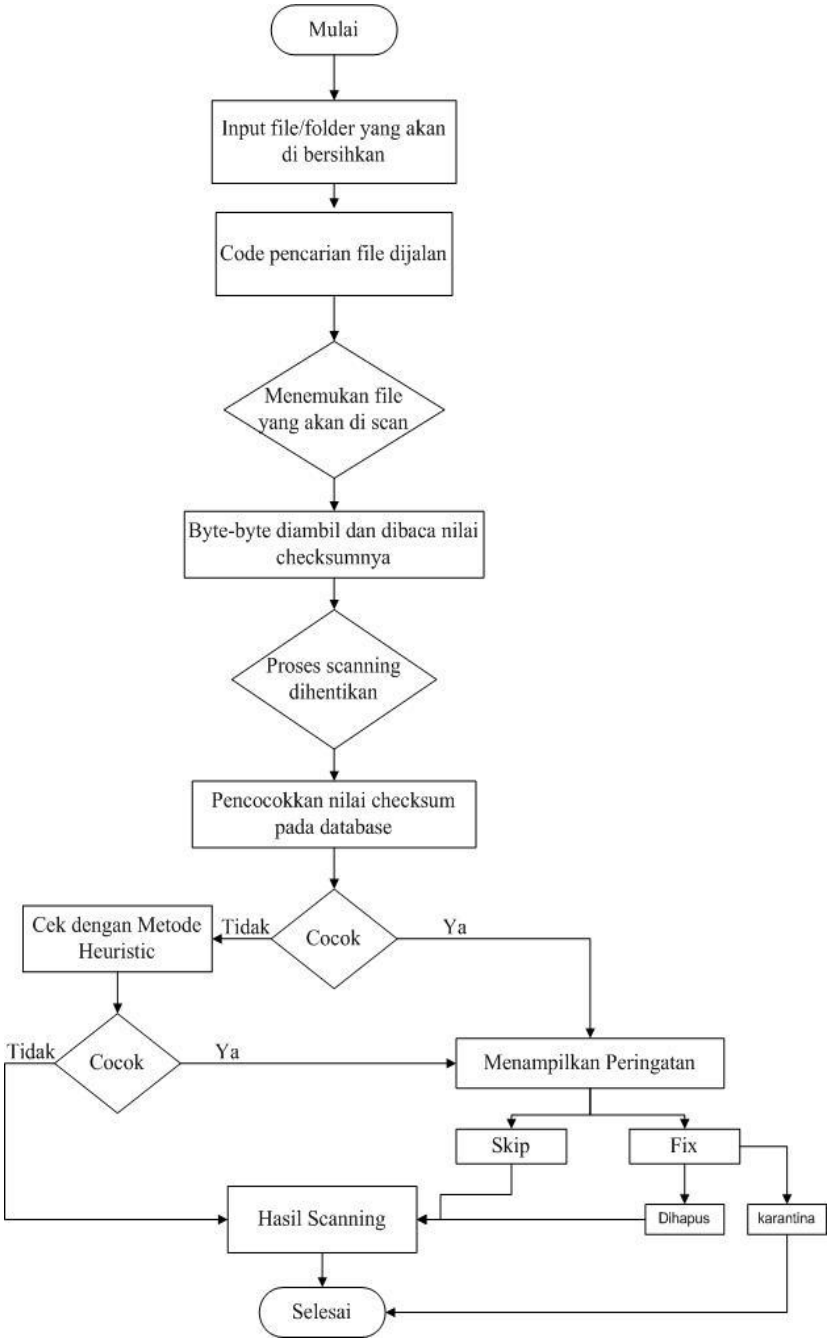
1. Windows 7
2. Microsoft Visual Basic 6.0
3. Sampel virus : Pada antivirus ini diambil 50 buah sampel antivirus yang diperoleh dari website yang menyediakan sampel virus yaitu “vx.netlux.org” dan Morphostlab.com. Sedangkan sampel virus yang digunakan adalah malware (virus, worm dan trojan).

IT Journal Research and Development
Vol.3, No.1, Agustus 2018 e-ISSN: 2528-4053
DOI : 10.25299/itjrd.2018.vol3(1).1884

2.3.3 Perancangan Flowchart

1. *Flowchart Antivirus Vici*

F*lowchart* perancangan antivirus ini merupakan gambaran umum proses ketika antivirus membaca sebuah file dan menentukan apakah file tersebut merupakan sebuah virus atau bukan. Proses pembacaan melalui *checksum error* pada database atau me-lalui metode *heuristic* ganda. *Flowchart* antivirus yang digunakan dalam penelitian ini ditunjukkan pada gambar 2.

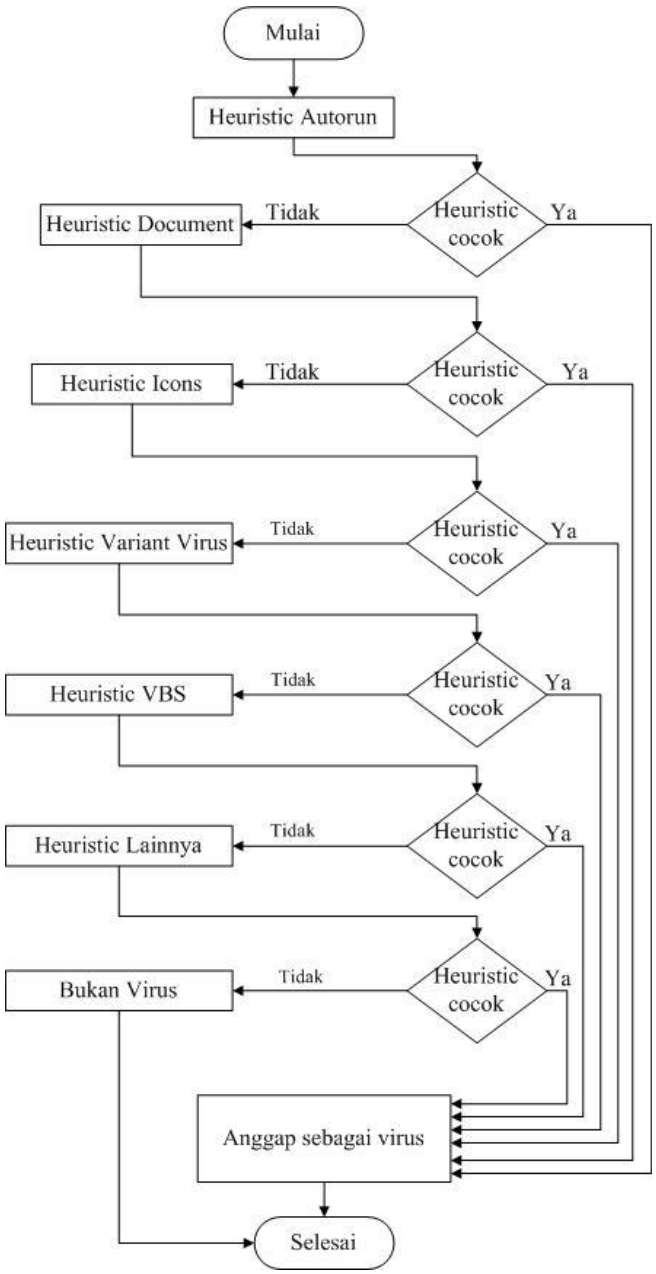


Gambar 2. Flowchart Antivirus Vici

IT Journal Research and Development
Vol.3, No.1, Agustus 2018 e-ISSN: 2528-4053
DOI : 10.25299/itjrd.2018.vol3(1).1884

2. Flowchart 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*.

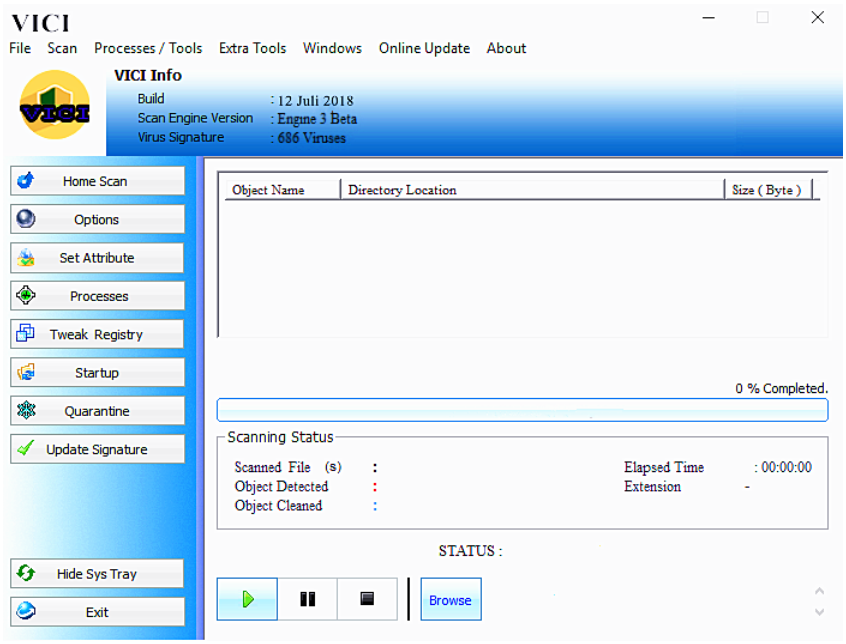
IT Journal Research and Development
Vol.3, No.1, Agustus 2018 e-ISSN: 2528-4053
DOI : 10.25299/itjrd.2018.vol3(1).1884

3. HASIL DAN PEMBAHASAN

Berdasarkan analisa sistem dan pengumpulan data yang dilakukan, maka aplikasi antivirus Vici pada sistem keamanan data komputer mampu meghapus, medeteksi, mengkarantina, dan mematikan kinerja virus dalam proses scanning yang akurat.

1. Tampilan Awal Aplikasi

Tampilan Awal ini berisikan menu-menu pada antivirus tersebut dimaksudkan untuk mempermudah *user* dalam penggunaan antivirus tersebut. Adapun tampilannya sebagai berikut:

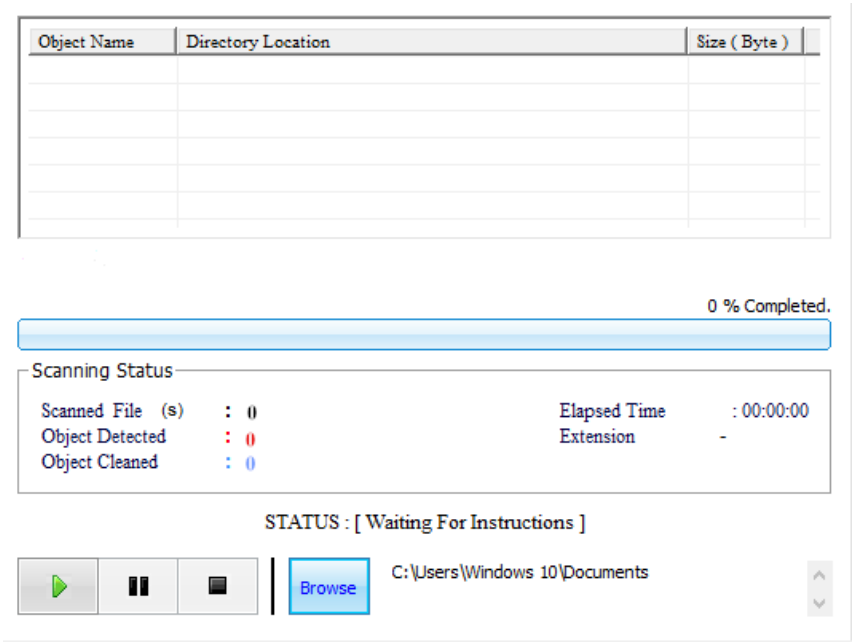


Gambar 4. Tampilan Awal Antivirus Vici

2. Tampilan Input file atau folder

Pada rancangan tampilan input file atau folder antivirus menampilkan file-file yang akan di-scan dalam penelitian ini ditunjukkan pada gambar 5.

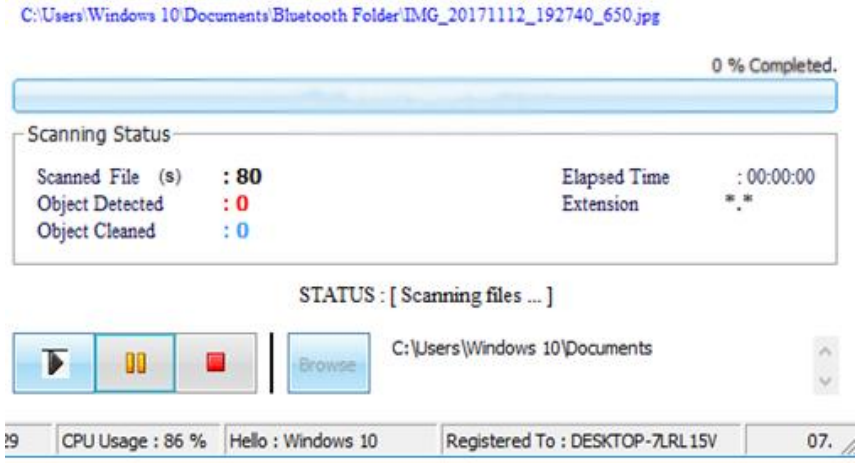
IT Journal Research and Development
Vol.3, No.1, Agustus 2018 e-ISSN: 2528-4053
DOI : 10.25299/itjrd.2018.vol3(1).1884



Gambar 5. Tampilan Input file atau folder

3. Tampilan Proses Scanning

Pada Rancang tampilan proses scanning ini memperlihatkan proses kerja scanning file. Adapun tampilannya sebagai berikut:

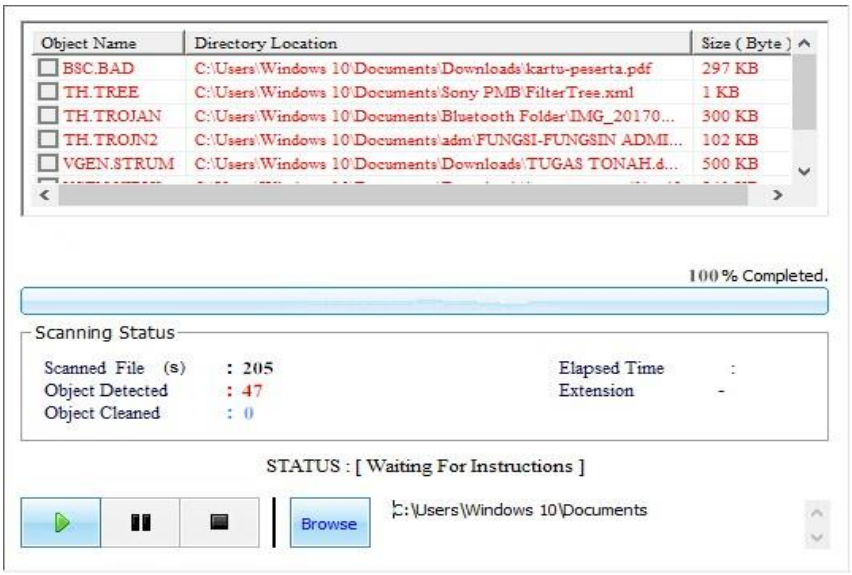


Gambar 6. Tampilan Proses Scanning

4. Tampilan Proses telah di Scanning

Pada rancangan tampilan ini memperlihat kan proses file telah di-scanning, dan menampilkan jumlah virus yang terdeteksi.

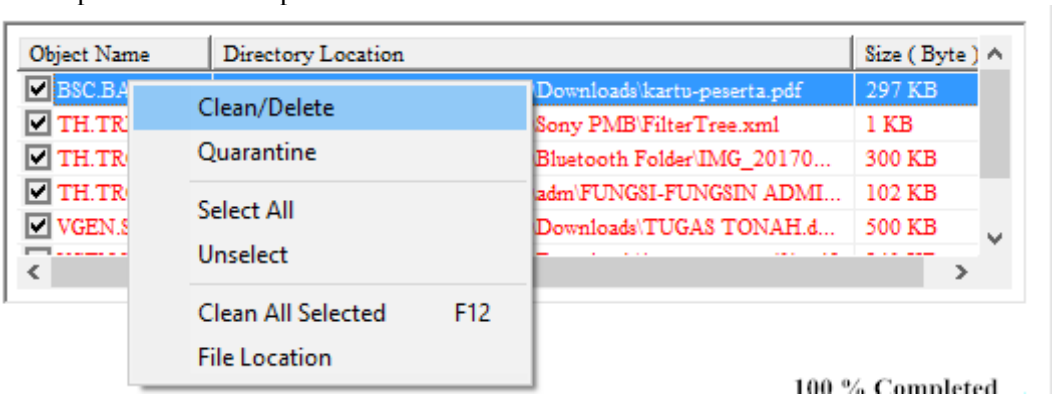
IT Journal Research and Development
Vol.3, No.1, Agustus 2018 e-ISSN: 2528-4053
DOI : 10.25299/itjrd.2018.vol3(1).1884



Gambar 7. Tampilan Proses telah di Scanning

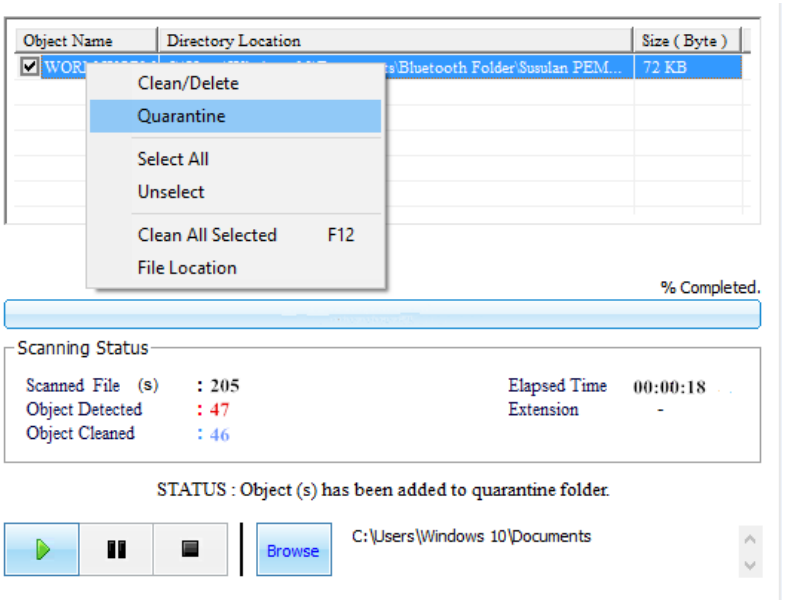
5. Tampilan Peringatan

Pada perancangan tampilan peringatan apabila file tersebut terinfeksi virus dan menampilkan tindakan apakah file membersihkan virus atau dikarantina.



Gambar 8. Tampilan membersihkan atau delete virus

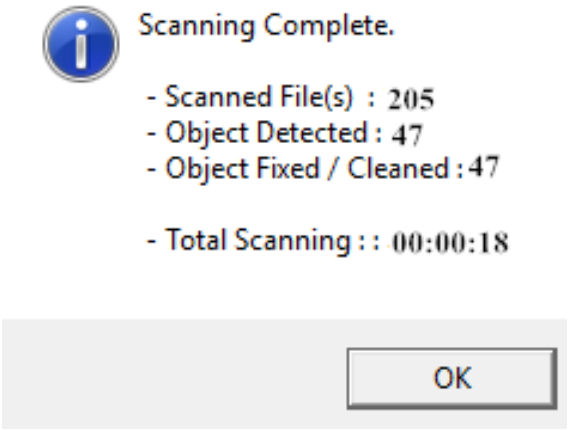
IT Journal Research and Development
Vol.3, No.1, Agustus 2018 e-ISSN: 2528-4053
DOI : 10.25299/itjrd.2018.vol3(1).1884



Gambar 9. Tampilan mengkarantina virus

6. Rancangan Tampilan Aplikasi telah selesai

Pada rancangan tampilan akhir aplikasi memperlihatkan bahwa proses scan telah selesai.



Gambar 10. Desain tampilan aplikasi telah selesai

4. KESIMPULAN

Setelah dilakukan pengujian dan analisa kinerja terhadap antivirus vici dikembagkan maka dapat ditarik kesimpulan sebagai berikut:

1. Pengujian metode heuristic ini dapat mematikan kinerja virus, mendeteksi dan menghapus infeksi virus komputer dengan menguji dan menganalisa sampel beberapa virus berdasarkan kriteria ataupun tingkah laku dari virus-virus tersebut.
2. Sistem realtime protector sangat efektif dalam melindungi komputer dari serangan virus, karena mampu mendeteksi keberadaan virus meskipun antivirus tidak sedang meakukan proses scanning. Metode ini telah diuji sebanyak 15 kali

IT Journal Research and Development
Vol.3, No.1, Agustus 2018 e-ISSN: 2528-4053
DOI : 10.25299/itjrd.2018.vol3(1).1884

dengan sampe malware (virus, worm dan trojan) dan didapat rasio 100% dalam pengujian tersebut.

3. Pada scanning dari Antivirus Vici memiliki rasio atau akurasi pendeteksian sebesar 96% dimana dari 50 virus(worm, trojan dan malware) dapat mendeteksi 47 virus. Kelebihan dari antivirus ini adalah akurasi dari pendeteksiannya sudah cukup tinggi, bahkan untuk virus yang sebelumnya masih luput dari pendeteksiannya, akan tetapi bisa dideteksi dengan cara menambahkan signature virus tersebut secara manual ke database virus menggunakan fitur update signature. Kekurangan antivirus ini adalah belum bisa dioperasikan pada sistem operasi windows xp 2.

5. SARAN

Antivirus Vici yang dikembanngkan menggunakan file text sebagai database eksternal. Namun akan lebih baik jika database antivirus menggunakan ekstensi sendiri dan terinkripsi sehingga file database akan lebih aman. Oleh dari itu penulis berharap agar antivirus ini nantinya dapat dikembangkan lagi dengan penambahan lebih banyak *heuristic* ataupun database virus agar kualitas antivirus ini menjadi semakin baik dan aplikasi proteksi tambahan yang dapat melindungi komputer dari serangan virus.

DAFTAR PUSTAKA

[1] A.M. Hirin., 2010. *Cara Praktis Membuat Antivirus Komputer*, Mediakita, Jakarta Selatan.
[2] Suhandi. 2009. Pengembangan Antivirus Songket Untuk Virus H1N1 Dengan Metode Behavior Blocking Detection, *Journal Portal Garud*, vol 4, hal 19-22.
[3] Arta, Yudhi. 2017. Implementasi Itrusion Detection System Pada Rule Based System Menggunkan Sniffer Mode Pada Jaringan Lokal. *IT Journal Research and Development*, vol 2, hal 43-50.
[4] Dr. Solomon's. 1995. *Virus Encylopedia*. ISBN:1-897661-00-02.
[5] Rahmawati, Rita., Nursikuwagus, Agus. 2012. Perancangan Antivirus Dengan Menggunakan Metode MD5 Dan Heuristic AARS, *Jurnal Teknologi dan Informatika*, vol 8, hal 40-53.
[6] Salim, Hartojo. 1990. *Virus Kom-puter*. Andi Offser:Yogyakarta,.
[7] Chaphalkara, N.B, et all. 2015. Prediction of outcome of construction dispute claims using multilayer perceptron neural network model N.B.*International Journal of Project Management*, Volume 33, hal 1827-1835.
[8] S'to. 2010. *CEH (Certified Ethical Hacker):300% Illegal*. Jasakom.
[9] Shadewa, Aat. 2007.*Rahasia Membuat Antivirus Menggunakan Visual Basic*. DSI Publishing: Yogyakarta.
[10] Suyanto. 2011. *Articial Intelligence Searching, Reasoning, Planning dan Learning.* Informatika, Bandung.
[11] Stefano. 2016. *Cara membangun Sistem Informasi Menggunakan VB.Net dan Komponen Dxperience.* C.V Andi Offset, Yogyakarta.
[12] Anhar. 2016. *Membuat Program Antivirus dengan Visual Basic 6.0*. PT. Elex Media Komputindo, Jakarta.