Sains dan Komputer (SAINTIKOM)
Vol.17, No.2, Agustus 2018, pp. 239-245
ISSN: 1978-6603 E-ISSN : 2615-3475

Penerapan Metode CRC32 Dalam Pembuatan AntiVirus

Widiarti Rista Maya
Program Studi Informasi, STMIK Triguna Dharma

Article Info

Article history:
Received Mei 09th, 2018
Revised June 15th, 2018
Accepted Aug 05th, 2018

Keyword:
Antivirus
Virus
CRC32

ABSTRAK

Virus komputer merupakan program komputer yang dapat menggandakan atau menyalin dirinya sendiri dan menyebar dengan cara menyisipkan salinan dirinya ke dalam program atau dokumen lain. Virus komputer sifatnya dapat merusak misalnya dengan merusak data pada dokumen, membuat pengguna komputer merasa terganggu dengan keberadaannya dalam sebuah sistem komputer, maupun tidak menimbulkan efek merusak sama sekali. Antivirus adalah sebuah jenis perangkat lunak yang digunakan untuk mendeteksi dan menghapus virus komputer dari sistem komputer.

Metode CRC32 sebagai metode pada proses scanning salah satunya adalah metode CRC32. Sesuai dengan fungsi utama dari fungsi hashing, CRC32 berfungsi untuk mengambil penanda dari sebuah file yang nantinya akan dipakai sebagai acuan untuk memeriksa apakah suatu file adalah file virus atau bukan. Kecil sekali kemungkinan bahwa dua buah file mempunyai nilai CRC32 yang sama. Hal ini disebabkan perbedaan 1 bit saja pada file akan mengubah nilai CRC32 file tersebut.

Perhitungan indeks akan dikonversi kedalam bentuk decimal agar diketahui jelas nilai indeksnya dan dilakukan perhitungan terhadap file yang akan dikoreksi dengan menggunakann bahasa pemrograman visual basic studio 2010. .

First Author
Nama : Widiarti Rista Maya, S.T, M.Kom
Program Studi : Sistem Informasi STMIK Triguna Dharma
Email : widya_rmaya87@yahoo.com

1. PENDAHULUAN

CRC-32 adalah sejenis fungsi yang mengambil input data strem dengan panjang virus komputer merupakan program yang dapat menggandakan atau menyalin dirinya sendiri dan menyebar dengan cara menyisipkan salinan dirinya ke dalam program atau dokumen lainnya. virus komputer dapat dianalogikan dengan virus biologis yang menyebar dengan cara menyisip sendiri.

Virus komputer sifatnya dapat merusak misalnya dengan merusak data pada dokumen-dokumen yang membuat pengguna komputer merasa terganggu dengan keberadaannya dalam sebuah sistem komputer, mampu tidak menimbulkan efek merusak file yang ada di dalam folder atau pun dokumen tertentu.

Dengan berkembangnya teknologi informasi, maka pembuatan aplikasi virus maupun aplikasi antivirus semakin mudah, sehingga diharapkan dengan mengetahui sifat dan perilaku keduanya, aplikasi virus dan antivirus yang akan dibangun dapat semakin memberikan penjelasan yang baik mengenai cara kerja kedua aplikasi tersebut.

CRC-32 (Cyclic Redundancy Check) bekerja secara sederhana yaitu dengan menggunakan perhitungan matematika terhadap sebuah bilangan yang disebut sebagai checksum, yang dibuat berdasarkan total bit yang akan ditransmisikan atau yang hendak disimpan. Dalam transmisi jaringan, khususnya dalam jaringan berbasis teknologi ethernet, checksum akan dihitung terhadap setiap frame yang
hendak ditransmisikan dan ditambahkan ke dalam frame tersebut sebagai informasi dalam header atau trailer. Penerima frame tersebut akan menghitung kembali apakah frame yang ia terima benar-benar tanpa kerusakan, dengan membandingkan nilai frame yang dihitung dengan nilai frame yang terdapat dalam frame.

CRC-32 didesain sedemikian rupa untuk memastikan integritas data terhadap degradasi yang bersifat acak. Dikarenakan noise atau sumber lainnya. Metode pencocokan CRC-32 merupakan teknik yang semulanya digunakan untuk memeriksa kerusakan pada file. Metode ini yang sering digunakan oleh antivirus lokal untuk memeriksa signature dari virus malware yaitu program atau perangkat lunak yang sifatnya merusak sistem

komputer yang dirancang untuk merusak sistem komputer jadi istilah malwer lebih bersifat umum yang bisa mencakup virus, horse, worm, dan lain sebagainnya yang sudah mengimplementasikan teknik polymorph.
Penelitian ini menghsilkan Software Antivirus dengan Metode Pendeteksian Heuristik sehingga walau pun virus/worm sudah melakukan modifikasi terhadap byte-byte tertentu di virus, pattern atau pola virus/worm secara keseluruhan tidak akan berubah dimana hal ini akan memudahkan antivirus untuk mendeteksi virus/worm dengan kemampuan polymorph.

2. LANDASAN TEORITIS

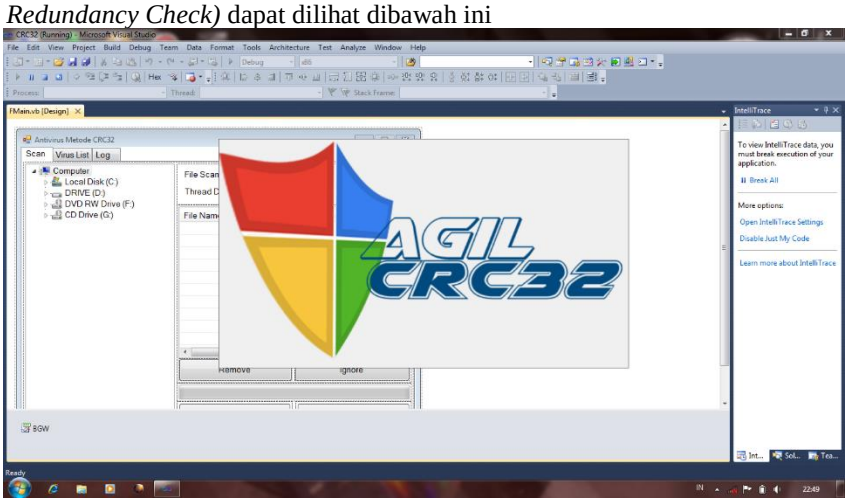
metode CRC-32 lebih efektif jika dibandingkan dengan algoritma metode scan CRC-32 yang selama ini banyak dipakai oleh pembuat antivirus, hal ini disebabkan algoritma CRC-32 (Cyclic Redundancy Check) menghasilkan message digest yang panjangnya 128 bit, sedangkan CRC-32 hanya mengambil 32bit, ini akan memperlambat proses scanning dan akan memperbesar pemakaian media penyimpanan.
Selain itu metode scan dengan CRC-32 dianggap lebih akurat dalam mengenali virus dibandingkan dengan metode monitoring (metode heuristic). Program antivirus ini dapat melakukan penambahan jumlah database virus (update) tanpa harus meminta kepada komputer server yang terdapat pada produsen antivirus.
Perhitungan Nilai CRC (Cyclic Redundancy Check) 32 Dalam pembuatan Pada algoritma CRC-32 adalah cara yang bagus dan teruji untuk pengecekan byte-byte dalam jumlah besar dari suatu file yang telah termodifikasi maupun tidak. Pada algoritma ini mencari file lewat seluruh jumlah byte dan menghasilkan angka 32 bit untuk menggambarkan isi file. Dan sangat kecil sekali kemungkinan dua stream dari byte yang berbeda mempunyai CRC yang sama. Algoritma CRC32 dapat diandalkan juga untuk mengecek error yang terjadi dalam urutan byte. Dengan CRC32 ini kemungkinan perubahan standar (penyimpangan dari penghitungan CRC terhadap file) yang terjadi dapat dikendalikan.
Perkembangan teknologi dan informasi membawa perubahan besar dalam penggunaan metode Checksum CRC32. Banyak bermunculan software-software jahat (baca:Malware) dan juga perkembangan virus computer yang semakin canggih membuat metode Checksum CRC32 lantas digunakan untuk mengetahui mendeteksi virus dengan acuan nilai crc32-nya. Nilai crc32 adalah nilai yang didapat dari garis besar file dan nama file yang dibandingkan dengan tabel crc32 yang sudah ada acuannya. Antivirus ini penulis menggunakan metode CRC32 untuk menghitung nilai pada sebuah file yang akan dijadikan sebagai database virus. Langkah-langkah dalam menghitung nilai CRC32 file adalah sebagai berikut :

1. Pertama program akan melakukan operasi Xor FFFFFFFF dengan FF
2. FFFFFFFF And FF = FF
3. Konversi FFFFFFFF dan FF ke dalam biner
4. Konversi biner dari FFFFFFFF adalah 32, maka FF yang konversi binernya hanya 8 digit, harus disamakan jumlah digitnya.
5. Melakukan operasi XOR dan hasilnya dikonversikan ke hexa.
6. Hasil dari konversi ke hexa akan dilakukan operasi Xor dengan isi dari file.
7. Setelah mendapat nilai maka lakukan operasi dengan FF000000 yang didapat dari menggeser nilai 000000FF menjadi sebanyak 8 bit
8. Perhitungan Tabel Lookup Cara pertama kita harus menghitung kalkulasi tabel lookup yang berguna untuk menentukan standar isi dari tabel CRC32, yaitu dengan membandingkan nilai 255 yang heksanya FFFFFFFF dengan polynomial file yang telah distandarkan yaitu EDB88320 menggunakan Xor. Kemudian hasil dari perbandingan disimpan di tiap array ’F’ yang berjumlah 255 array.
9. Untuk menghitung CRC32 suatu file kita perlu ukuran dari file tersebut dan mengeset standar perbandingan untuk CRC32 ke heksa FFFFFFFF. Kemudian untuk mengecek nilai yang ada tiap byte nya.

3. ANALISIS DAN HASIL

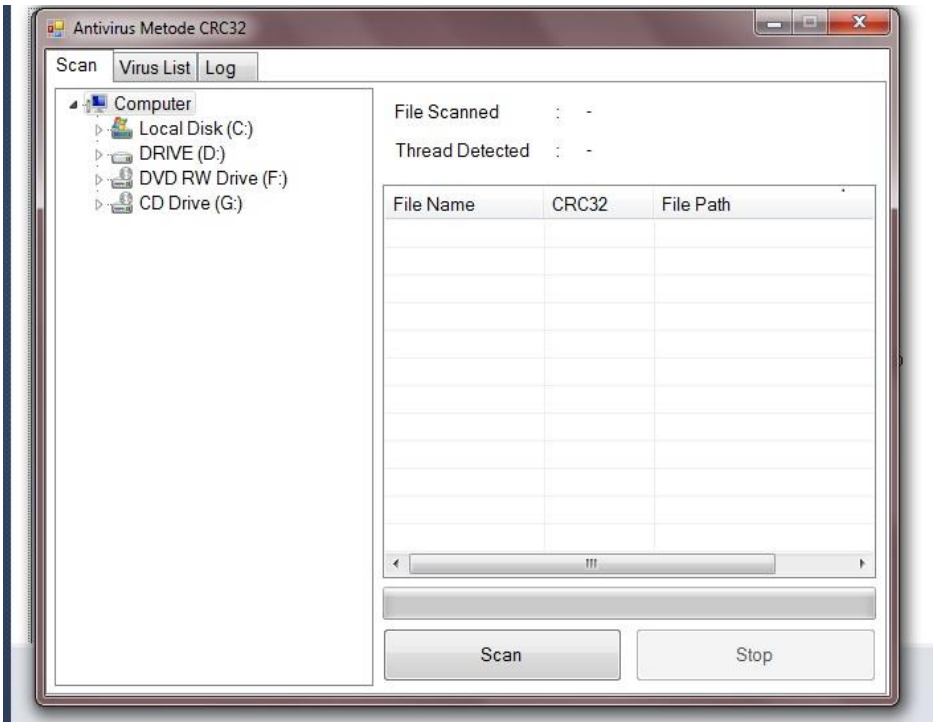
Untuk menganalisis algoritma yang digunakan, akan dilakukan dengan membuat suatu skenario sebagai berikut:
INITXOR CRC32 = FFFFFFFF
FINALXOR = FF
Byte Stream = 61
Perhitungan awal yang harus dilakukan adalah mendapatkan nilai indeks tabel dari *byte stream* yang akan diolah dengan melakukan operasi XOR antara *FINALXOR* dengan *byte stream.*
Indeks = FINALXOR ⊕ Byte Stream

Indeks = FF ⊕ 61
FF = 11111111
61 = 01100001
Indeks = 10011110
Hasil perhitungan indeks akan dikonversi kedalam bentuk desimal agar diketahui jelas nilai indeksnya.
$10011110 = (1.2^7) + (0.2^6) + (0.2^5) + (1.2^4) + (1.2^3) + (1.2^2) + (1.2^1) + (0.2^0)$
10011110 = 128 + 0 + 0 + 16 + 8 + 4 + 2 + 0
10011110 = 158
Setelah mendapatkan nilai indeks, langkah selanjutnya adalah mendapatkan nilai berdasarkan indeks pada tabel *CRC32*.
Dari tabel *CRC32* diperoleh nilai 17b7be43, dimana nilai ini akan kembali dilakukan perhitungan XOR Dengan FF000000 untuk mendapatkan nilai *CRC32*.
17b7be43 = 0001 0111 1011 0111 1011 1110 0100 0011
FF000000 = 1111 1111 0000 0000 0000 0000 0000 0000
17B7BE43 ⊕ FF000000
= 0001 0111 1011 0111 1011 1110 0100 0011 ⊕
1111 1111 0000 0000 0000 0000 0000 0000
=1110 1000 1011 0111 1011 1110 0100 0011
Selanjutnya hasil perhitungan diatas akan dikonversi kedalam bentuk *hexa* untuk mendapatkan nilai *CRC32*.
1110 1000 1011 0111 1011 1110 0100 0011 = E8B7BE43
$1110 = (1.2^3) + (1.2^2) + (1.2^1) + (0.2^0) = 14 = E$
$1000 = (1.2^3) + (0.2^2) + (0.2^1) + (0.2^0) = 8$
$1011 = (1.2^3) + (0.2^2) + (1.2^1) + (1.2^0) = 11 = B$
$0111 = (0.2^3) + (1.2^2) + (1.2^1) + (1.2^0) = 7$
$1011 = (1.2^3) + (0.2^2) + (1.2^1) + (1.2^0) = 11 = B$
$1110 = (1.2^3) + (1.2^2) + (1.2^1) + (0.2^0) = 14 = E$
$0100 = (0.2^3) + (1.2^2) + (0.2^1) + (0.2^0) = 4$
$0011 = (0.2^3) + (0.2^2) + (1.2^1) + (1.2^0) = 3$
Form splash screen CRC32 (*Cyclic Redundancy Check)* ini merupakan suatu *form* yang berfungsi untuk mengenkripsi *file* dan mengambil nilai *CRC32* dari sebuah *file* yang dicurigai sebagai virus. *Form splas screen CRC32* (*Cyclic Redundancy Check)* dapat dilihat dibawah ini



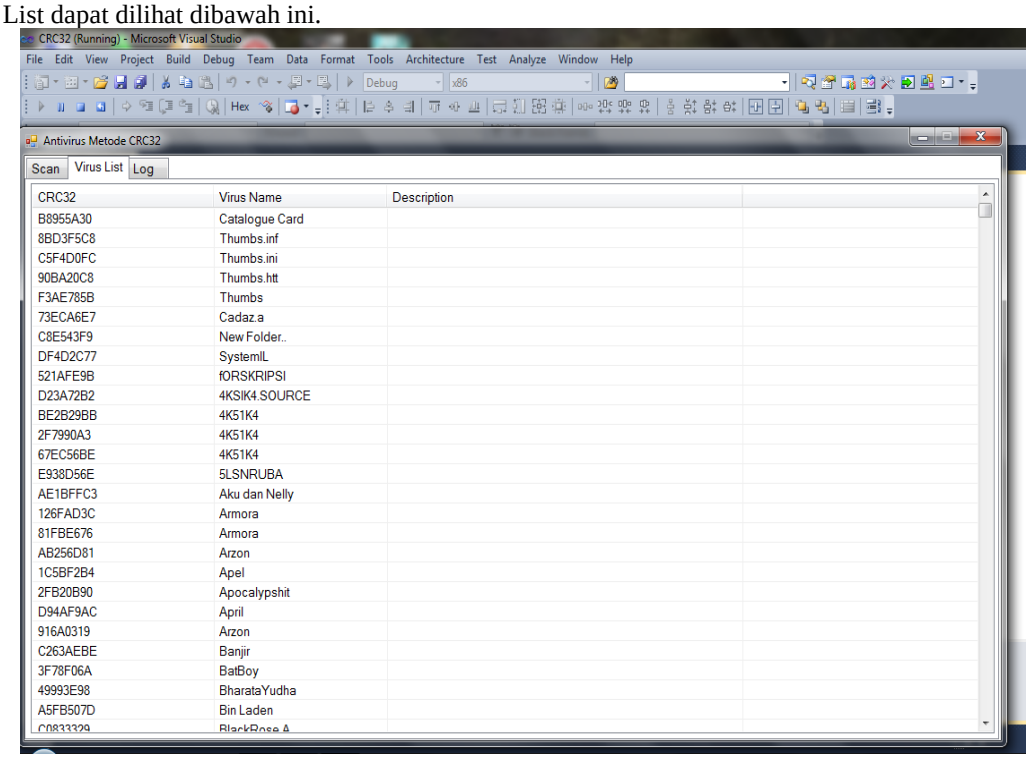
Gambar .1 *From Splash Screen CRC32* (*Cyclic Redundancy Check)*

Pada tampilan *form splash screen* CRC32 *(Cyclic Redundancy Check)* terdapat nama antivirus. Menu Scan merupakan menu dimana antivirus melakukan scanning atau pencarian virus pada komputer. Menu Scan dapat dilihat dibawah ini..



Gambar .2 Menu Scan *CRC32* (*Cyclic Redundancy Check)*

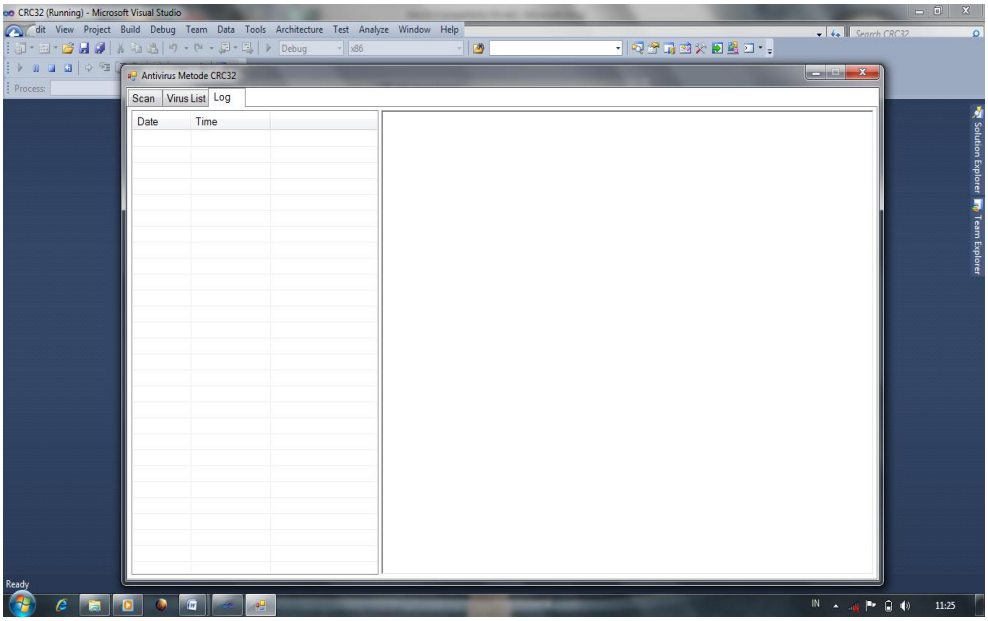
Didalam menu scan terdapat beberapa tombol add yaitu untuk memilih lokasi berfungsi untuk memilih *file* atau *folder* yang akan nanti ya yang akan di scan oleh antivirus, tombol scan berfungsi untuk melakukan pencari virus pada suatu computer, tombol stop berfungsi untukmemberhentikan proses scanning atau pencarian virus. Menu Virus List merupakan menu yang menampilkan nama virus-virus yang terdeteksi, Menu Virus List dapat dilihat dibawah ini.



Gambar .3 Menu Virus List *CRC32* (*Cyclic Redundancy Check)*

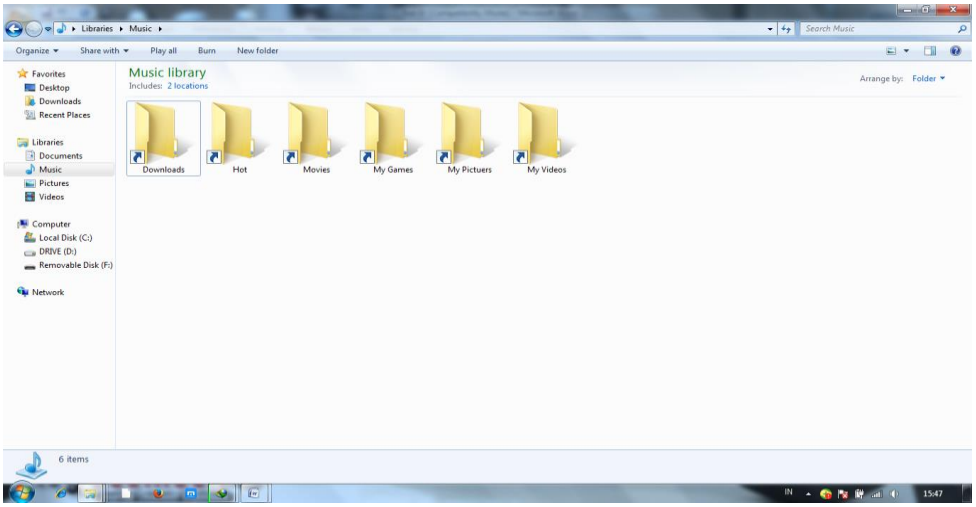
Didalam menu virus list terdapat nama-nama virus yang akan discan nanti ya.

Menu Log Log-File adalah sebuah file yang berisi daftar tindakan kejadian (aktivitas) yang telah terjadi didalam suatu sistem computer yang telah menyajikan tampilan *file* yang telah discan atau history pada setiap scanning. Gambar Menu Log dapat dilhat dibawah ini



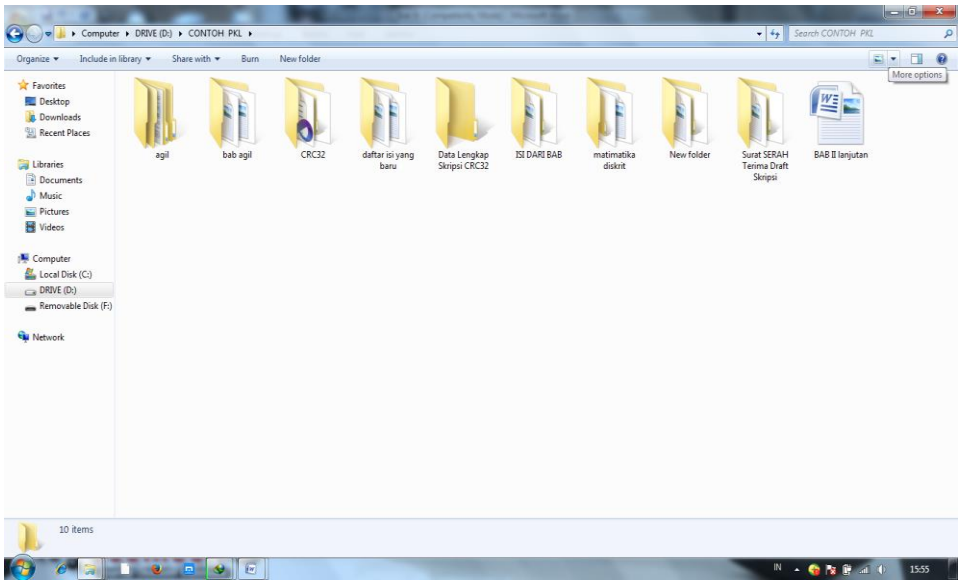
Gambar .4 Menu Log *CRC32* (*Cyclic Redundancy Check)*

Menyajikan tampilan *file* yang telah discan atau history pada setiap scanning. Pada Pemilihan folder yang Keberadaan terinfeksi virus bisa diketahui dalam driver, lewat file yang bernama "shortcut" tanpa icon, dengan file pemicu "autorun.inf" dan file induk "*.bat" (jika ada), target virus ini biasanya adalah file Folder yang terinfeksi virus yang berbentuk (*.exe) dalam drive aktif, seperti halnya flashdisk. Jika file atau folder. semua aplikasi bermasalah, pastikan didrive anda terdapat virus boot. exe atau file anda telah terinfeksi virus ini.



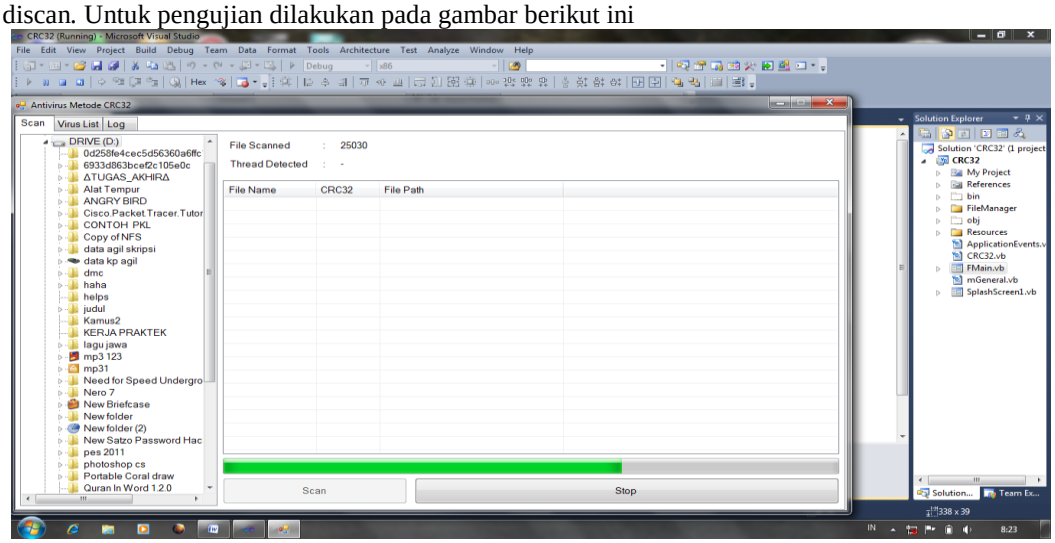
Gambar 5 Folder yang Terinfeksi Virus

Pada Pemilihan folder yang Keberadaan tidak terinfeksi virus bisa diketahui dalam driver, yang tanpa icon, jika ada target virus ini biasanya adalah pada file atau pun Folder yang tidak terinfeksi virus yang berbentuk (*.exe) dalam drive aktif, seperti halnya flashdisk.



Gambar 6 Folder yang Terinfeksi Virus

Pada saat pengujian sistem ini yang dimaksud untuk mengetahui sejauh mana mana tingkat dari keberhasilan dari sebuah sistem *schaning antivirus CRC32* (*Cyclic Redundancy Check)* dengan ada ya sebuah file yang akan discan. Untuk pengujian dilakukan pada gambar berikut ini



Gambar 7 Form Antivirus *CRC32* Proses Scaning

4. KESIMPULAN

Dari hasil teknik uji coba dari sistem antivirus ini dapat di ambil kesimpulan bahwa: Dalam Teknik Metode CRC-32 merupakan teknik yang semulanya digunakan untuk mengecek kerusakan pada file. Metode ini yang sering digunakan oleh anti virus lokal untuk mengecek signature dari virus, tetapi teknik ini tidak efesien apabila diterapkan pada malware yang sudah mengimplementasikan tekni polymorph. Kasus virus lokal sudah ditemukan penggunaan teknik polymorph. Baik itu secara sederhana maupun kompleks file addres Of entry point dan sizeo fcode, Sangat akurat dalam mengenal virus, walaupun virus telah merubah header filenya tapi datanya tetap sama.

Engine scanernya juga cepat dan ringan tidak terlalu memberatkan memori. Berdasarkan analisa terhadap hasil percobaan yang didapat, maka dapat diambil beberapa simpulan sebagai berikut:

1. Kemampuan penambahan database secara manual oleh pengguna pada sistem antivirus, mampu memudahkan pengguna untuk mengupdate database antivirus setiap saat berbasis objek virus yang ada pada sebuah sistem operasi. Dan pengguna bisa menghemat pemakaian media penyimpanan dengan mengisi database sesuai file virus yang akan menjadi target pencarian pada sebuah sistem operasi komputer. Nilai crc32 yang dihitung dari dari sebuah file virus digunakan sebagai signature atau fingerprint (sidik jari) dari virus tersebut dalam mendeteksi keberadaan virus tersebut dalam directory sistem operasi komputer.

2. Pencarian file virus oleh sistem antivirus dilakukan dengan menghitung nilai crc32 dari setiap file yang ada pada suatu directory, kemudian nilai crc32 yang diperoleh akan dibandingkan dengan nilai crc32 yang terdapat pada database, jika tidak terdapat dalam database maka file tidak dapat dianggap sebagai virus.

DAFTAR PUSTAKA

[1] C. Security, Computer Security. 2005.
[2] C. S. Education, "Buffer Overflow Vulnerability Lab," Science (80-.)., pp. 1–8, 2014.
[3] Computer Fraud & Security, "UK launches new security awareness campaign," Comput. Fraud Secur., vol. 2013, no. 7, p. 3, 2013.
[4] N. Security, "Computer Network Security Computer Network Security," Netw. Secur., vol. 1, pp. 1–10, 2007.
[5] J. Dray and C. S. Division, "Report on the NIST JavaTM AES Candidate Algorithm Analysis," Test, 1999.
[6] S. Information, S. Security, and V. Issue, "Computer Crime Investigation & Computer Forensics," Inf. Syst. Secur., vol. 6, no. 2, 2009.
[7] I. I. Journal, C. Science, and N. Security, "Application Of Analytic Hierarchy Process (AHP) In The Evaluation and Selection Of an Information System Reengineering Projects," IJCSNS Int. J. Comput. Sci. Netw. Secur., vol. 11, no. 1, pp. 172–177, 2011.
[8] I. I. Journal, C. Science, and N. Security, "Real Time Vehicle Detection and Counting Method for Unsupervised Traffic Video on Highways," IJCSNS Int. J. Comput. Sci. Netw. Secur., vol. 10, no. 8, pp. 112–117, 2010.
[9] V. D. Gligor and N. C. S. C. (US), A guide to understanding covert channel analysis of trusted systems, no. November. 1994.
[10] S. M. Radack and C. S. D. Staff, "Security in open systems networks," Comput. Stand. Interfaces, vol. 10, no. 3, pp. 213–218, 1990.
[11] L. Zhuang and C. Sciences, "Security Inference from Noisy Data," 2008.
[12] D. Gollmann, "Computer security," Wiley Interdiscip. Rev. Comput. Stat., vol. 2, no. 5, pp. 544–554, 2010.
[13] C. Network, "Computer Network Defense 10," Network, pp. 179–191, 2011.
[14] Z. Genova and K. Christensen, "Efficient summarization of URLs using CRC32 for implementing URL switching," in Proceedings - Conference on Local Computer Networks, LCN, 2002, vol. 2002–January, pp. 343–344.
[15] K. Salah, "An online parallel CRC32 realization for Hybrid Memory Cube protocol," in 2013 9th International Computer Engineering Conference: Today Information Society What's Next?, ICENCO 2013, 2013, pp. 1–4.
[16] S. Gueron, "Speeding up CRC32C computations with Intel CRC32 instruction," Inf. Process. Lett., vol. 112, no. 5, pp. 179–185, 2012.
[17] S. Anwar, I. Nugroho, and A. Ahmadi, "Implementasi Kriptografi Enkripsi Shift Vigenere Chipher Serta Checksum Menggunakan CRC32 Pada Data Text," Sist. Inf., vol. 2, pp. 44–50, 2015.
[18] Y. S. Dandass, N. J. Necaise, and S. R. Thomas, "An empirical analysis of disk sector hashes for data carving," J. Digit. Forensic Pract., vol. 2, no. 2, pp. 95–104, 2008.
[19] M. Stigge, H. Plötz, W. Müller, and J.-P. Redlich, "Reversing CRC - Theory and Practice," HU Berlin Public Rep., no. May, pp. 1–3, 2006.
[20] M. Walma, "Pipelined cyclic redundancy check (CRC) calculation," in Proceedings - International Conference on Computer Communications and Networks, ICCCN, 2007, pp. 365–370.

BIOGRAFI PENULIS

Widiarti Rista Maya, ST, M.Kom merupakan Dosen Tetap STMIK Triguna Dharma yang mengampu beberapa mata kulih komputas lunak diantaranya : Pemrograman Visual, Pemrograman Web, Algoritma dan Pemrograman, Sistem Manajemen Basis Data, Security, Simulasi. Tamat S1 ISTP bidang Teknik Informatika dan Tamat S2 USU Bidang Teknik Informatika.