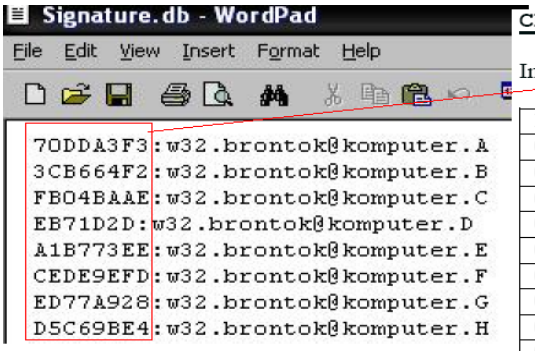
Checksum CRC32

Anharku
v_maker@yahoo.com
http://anharku.freevar.com

Tutorial ini di buat untuk yang belum ngerti ajah yah yang udah Master harap membenarkan kalo dalam penulisan tutorial ini terdapat kesalahan hehehe☺ .Pertama pasti yang menjadi pertanyaan apa sih Checksum CRC32 itu? Cyclic Redundancy Check (CRC) adalah salah satu fungsi hash yang dikembangkan untuk mendeteksi kerusakan data dalam proses transmisi ataupun penyimpanan. CRC menghasilkan suatu checksum yaitu suatu nilai dihasilkan dari fungsi hash-nya, dimana nilai inilah yang nantinya digunakan untuk mendeteksi error pada transmisi ataupun penyimpanan data. Nilai CRC dihitung dan digabungkan sebelum dilakukan transmisi data atau penyimpanan, dan kemudian penerima akan melakukan verifikasi apakah data yang diterima tidak mengalami perubahan ataupun kerusakan. CRC32 32 juga melambangkan panjang checksum dalam bit. Bentuk CRC yang disediakan untuk algoritma sesuai dengan ide pembagian ”polynomial”. Dan hal ini digunakan untuk memperhitungkan checksum yang sama dari seluruh algoritma CRC. Algoritma CRC adalah cara yang bagus dan teruji untuk pengecekan byte dalam jumlah besar dari suatu file yang telah termodifikasi maupun tidak. Algoritma ini mencari 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 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 besar file dan nama file yang dibandingkan dengan tabel crc32 yang sudah ada acuannya.



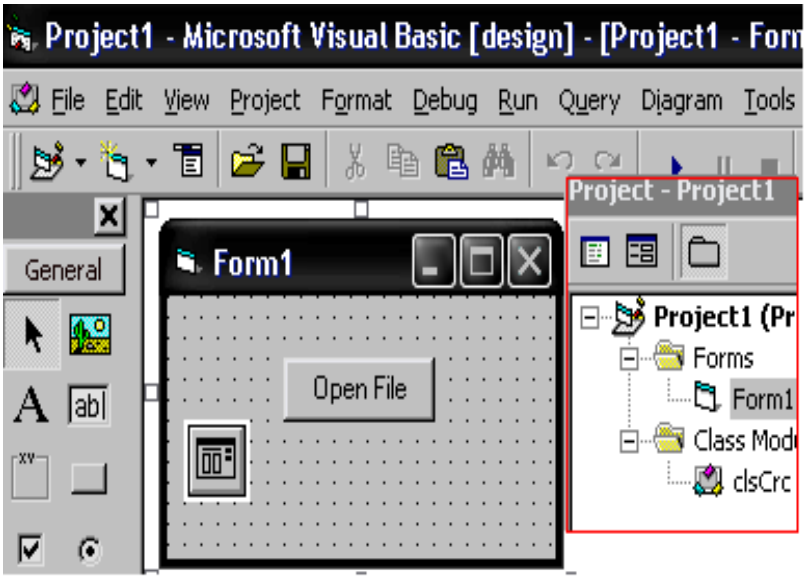
CRC-32 Table

Index Awal — Nilai

Idx	Nilai		Idx	Nilai
00h	00000000		80h	EDB88320
01h	77073096		81h	9ABFB3B6
02h	EE0E612C		82h	03B6E20C
03h	990951BA		83h	74B1D29A
04h	076DC419		84h	EAD54739
05h	706AF48F		85h	9DD277AF
06h	E963A535		86h	04DB2615
07h	9E6495A3		87h	73DC1683
08h	0EDB8832		88h	E3630B12
09h	79DCB8A4		89h	94643B84
0Ah	E0D5E91E		8Ah	0D6D6A3E
0Bh	97D2D988		8Bh	7A6A5AA8
0Ch	09B64C2B		8Ch	E40ECF0B
0Dh	7EB17CBD		8Dh	9309FF9D
0Eh	E7B82D07		8Eh	0A00AE27

Untuk menghitung dengan metode CRC32 dilakukan dengan beberapa cara, yaitu : 1.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.

2. 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 next buat aja crc32 generator-nya hehehe☺



Bahan: form (CommandButton,CommonDialog), Class Modules

‘Source of Form1:

```
Option Explicit

Dim crc As New clsCrc

Private Sub Command1_Click()

Dim rieysha() As Byte, lcrc As Long

On Error Resume Next

  cd.ShowOpen

  cd.Filter = "All File|*.*"

  Open cd.FileName For Binary Access Read As #1

  ReDim rieysha(LOF(1) - 1)

  Get #1, , rieysha

  Close #1

  lcrc = UBound(rieysha())

  lcrc = crc.CRC32(rieysha, lcrc)

  MsgBox UCase(Hex(lcrc)) 'menampilkan kotak peringatan besisi nilai Checksum CRC32

End Sub
```

‘next source of Class Modules:

```
Option Explicit

Private crcTable(0 To 255) As Long

Public Function CRC32(ByRef bArrayIn() As Byte, ByVal lLen As Long, Optional ByVal lcrc As Long
= 0) As Long

  Dim lCurPos As Long

  Dim lTemp As Long

  If lLen = 0 Then Exit Function
```

```
  lTemp = lcrc Xor &HFFFFFFFF

  For lCurPos = 0 To lLen

    lTemp = (((lTemp And &HFFFFFF00) \ &H100) And &HFFFFFF) Xor (crcTable((lTemp And 255)
Xor bArrayIn(lCurPos)))

  Next lCurPos

  CRC32 = lTemp Xor &HFFFFFFFF

End Function

Private Function BuildTable() As Boolean

  Dim i As Long, x As Long, crc As Long

  Const Limit = &HEDB88320

  For i = 0 To 255

    crc = i

    For x = 0 To 7

      If crc And 1 Then

        crc = (((crc And &HFFFFFFFE) \ 2) And &H7FFFFFFF) Xor Limit

      Else

        crc = ((crc And &HFFFFFFFE) \ 2) And &H7FFFFFFF

      End If

    Next x

    crcTable(i) = crc

  Next i

End Function

Private Sub Class_Initialize()

  BuildTable

End Sub

'------------------------------------------------------------
```

Cara – cara antivirus dalam mengenali sebuah virus melalui metode checksum crc32 adalah sebagai berikut :
-Memilih file yang akan diperiksa
-Mengambil informasi dari file tersebut, yaitu nama, ukuran
-Menghitung checksum file yang diambil dari ukuran file dengan metode crc32.
-Tentunya hasil checksum tersebut akan dikumpulkan dalam ***database signature checksum CRC32*** dari virus-virus yang telah dicari nilai checksum CRC32-nya.kemudian antivirus akan bekerja dengan menggunakan hasil checksum tersebut untuk mengenali bahwa program tersebut adalah virus.

Tetapi CRC tidak cukup aman karena telah ditemukan cara untuk melakukan **reversing** terhadap hasil CRC. Kemampuan untuk melakukan reverse terhadap nilai CRC ini dimanfaatkan ketika kita ingin melakukan manipulasi terhadap data yang kita ketahui nilaiCRCnya. Teknik reverse ini telah saya terangkan pada tutorial **Virus Header Modifier** dimana kita dapat mengubah nilai checksum CRC32 dari suatu file aplikasi dan file aplikasi tersebut masih dapat berjalan dengan normal. Hal ini sama halnya ketika kita melakukan proses kompresi data dengan menggunakan packer semisal UPX, PETITE,dll. File hasil kompresi ukurannya akan menjadi lebih kecil dari ukuran asli akan tetapi saat file dijalankan tetap berjalan dengan normal namun nilai dari checksum CRC32-nya telah berubah.

Untuk itu para programer antivirus tidak hanya menggunakan teknik checksum CRC32 saja akan tetapi juga menggunakan teknik-teknik lain seperti:

- Menggunakan **checksum MD5**
- Menggunakan **Heuristic Icon**
- Menggunakan **Pattern tersendiri**
- antivirus tersebut tidak menggunakan metode checksum dalam pendeteksian tetapi lebih cenderung mengacu ***string*** pada body file. Trik ini biasa diaplikasikan pada mayoritas antivirus professional.
- Dll

Dah ah.. cuapek juga…moga tutorial ini dapat bermanfaat bagi kita semua. Jam dirumahku udah pukul 01.30 WIB waktunya untuk ku memejamkan kedua mataku….

Thank's to:

Admin "Mengenali Virus Lewat Checksum Error dengan metode CRC32"

"virologi Tutorial Pemrogaman Antivirus Menggunakan VB Antivirus, Konsep dan Pengertiannya"

Indra Sakti Wijayanto "Penggunaan CRC32 dalam Integritas Data"

Biografi Penulis

Anharku. *Pertama mengenal komputer saat SMP pertamanya kenal komputer hanya bermain game bawaan window's lambat laun karna pergaulan dan pertumbuhan,merasakan anehnya cinta monyet...patahhati lalu melampiaskannya pada bermain Game online namun karena satu persatu game itu servernya runtuh (gameOver kali) jadi aku memutuskan vakum dari dunia gamer waktu itu juga saat aku masih UAS jadi aku fokus ke skull dulu.Lanjut mengenal dunia internet sejak hobi main di warnet untuk sekedar mengecek e-mail, fs, dan sekedar chatting ga jelas..Dari temanku bernama DNZ lah aku mulai mengenal dunia virus. lalu aku belajar secara otodidak karna temanku DNZ lebih suka dunia Hacking. Belajar algoritma dan pemrograman, membuat flowchart,dan belajar bahasa pemrogramanseperti visual basic, delphi, C++, pascal, asmbly. Belajar tentang micro, website, PHP, Basis data, MySQL,belajar tentang Jaringan Komputer..belajar tentang segala sesuatu yang berbau komputer.*