

# Packer Checker

Anharku

v\_maker@yahoo.com

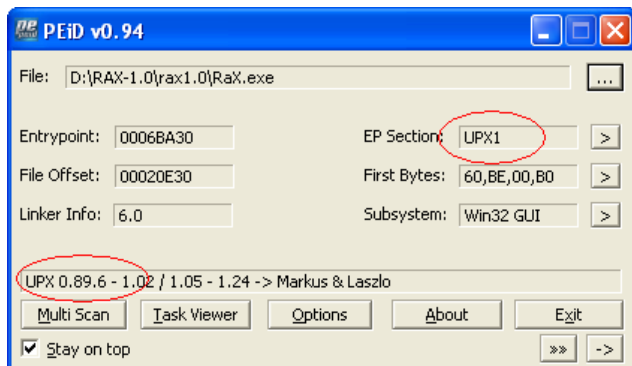
http://anharku.freevar.com

Lisensi Dokumen:

Copyright © 2003-2009 IlmuKomputer.Com

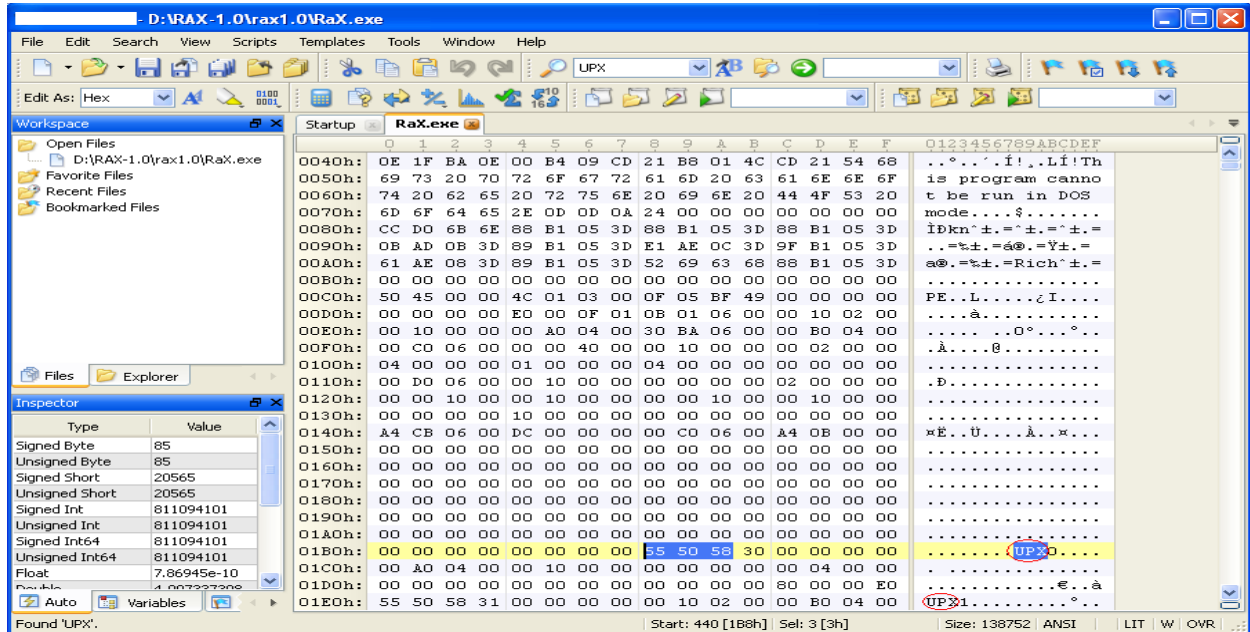
Seluruh dokumen di IlmuKomputer.Com dapat digunakan, dimodifikasi dan disebarkan secara bebas untuk tujuan bukan komersial (nonprofit), dengan syarat tidak menghapus atau merubah atribut penulis dan pernyataan copyright yang disertakan dalam setiap dokumen. Tidak diperbolehkan melakukan penulisan ulang, kecuali mendapatkan ijin terlebih dahulu dari IlmuKomputer.Com.

Pasti kalian semua sudah tidak asing dengan tools ini PEiD. Tool paporit para *cracker* untuk mengetahui sebuah program di pack menggunakan packer apaan?? Mungkin para *cracker* memiliki banyak jenis *Packer Detector* yang mereka rahasiakan untuk kepentingan pribadi mereka hehehe...☺

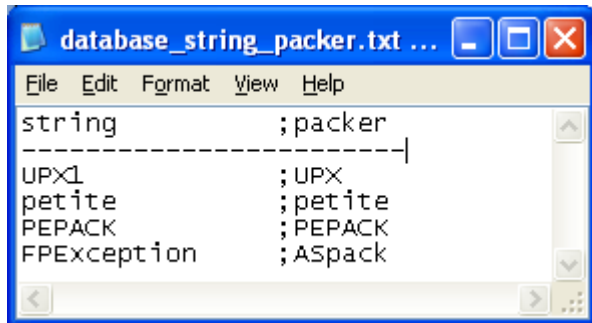


*PEiD detects most common packers, cryptors and compilers for PE files. It can currently detect more than 600 different signatures in PE files(readme.txt)* Peid dapat mendeteksi sebagian besar pakers umum, umumnya dapat mendeteksi lebih dari 600 signature yang berbeda pada file Executable.

Lalu bagaimana cara kerja peid? peid akan mendeteksi String suatu file Executable apakah di dalamnya terdapat signature atau tanda jika ada tanda tersebut maka golongan packernya. Signature tersebut telah di daftar sebagai sebuah kumpulan database, Yah mirip2 teknik antivirus gitu deh dalam mengenali virus. Nah untuk lebih jelasnya mari kita buka file yang kita pack dengan UPX, signature apakah yang selalu terkandung didalamnya??

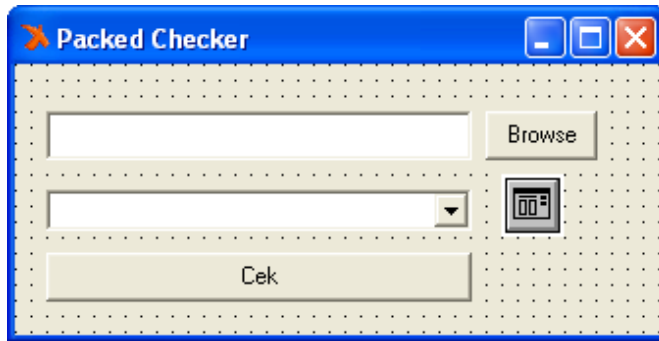


Ternyata file yang kita pack dengan UPX selalu mengandung string “UPX” ,dan setelah penulis melakukan beberapa ujicoba pengepack-an dengan beberapa packer ternyata sebagian packer meninggalkan string nama packernya pada file yang telah dipack.misalnya..



lalu bagaimana cara kita membuat program agar dapat membuka sebuah file Executable? Lanjut ke project:

No.	Object	Properti	Value
1	form	name	Form1
2	Common Dialog	name	Cd
3	TextBox	name	Text1
4	ComboBox	name	Combo1
5	CommandButton	name	Command1 Command2



```
' Code
Private Sub Command1_Click()
Cd.ShowOpen
If Len(Cd.FileName) > 0 Then Text1.Text = Cd.FileName
Cd.Filter = "Application|*.exe"
End Sub

Private Sub Command2_Click()
isvb (Text1.Text)
End Sub

Function isvb(alamat As String)
Dim sTemp As String
Open alamat For Binary As #1
sTemp = Space(LOF(1))
Get #1, , sTemp
Close #1
If InStr(sTemp, (Combo1.Text)) Then _
MsgBox "Ini packernya" Else _
MsgBox "bukan Ini packernya"
End Function

Private Sub Command3_Click()
List1.AddItem Combo1.Text
Combo1.SetFocus
End Sub

Private Sub Form_Load()
Combo1.AddItem "UPX1"
Combo1.AddItem "petite"
Combo1.AddItem "PEPACK"
Combo1.AddItem "FPEXception"
End Sub
```

Sedikit penjelasan:

Open **alamat** For Binary As #1

sTemp = Space(LOF(1))

Get #1, , sTemp

Close #1

file Executable dibuka dalam mode binary, dan seluruh isinya langsung ditampung ke dalam sebuah variable. Lalu dengan referensi dari string yang telah ditentukan misal string "UPX1" lalu dengan logika **if-then-else** kita bisa mengecek apakah string tersebut terdapat didalam suatu file Executable.

**If** InStr(sTemp, (Combo1.Text)) **Then** \_

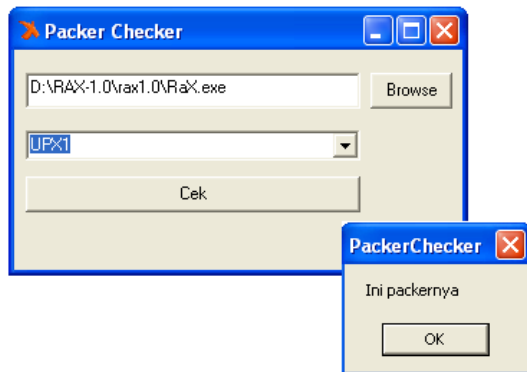
MsgBox "Ini packernya" **Else** \_

MsgBox "bukan Ini packernya"

End Function

Jika terdapat string seperti pada ComboBox maka keluarkan pesan "Ini packernya" jika tidak maka akan keluarkan pesan "bukan Ini packernya".

Coba jalankan programnya:



Code diatas masih sangat sederhana anda dapat mengembangkannya sendiri seperti membuat database diluar program ini agar data string dapat terus di tambah atau diupdate.

Semua yang ada dalam artikel ini hanya untuk pembelajaran semata.. semoga bermanfaat bagi kita semua

☺

4

## 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 pemrograman seperti 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.*