Memulihkan File berekstensi doc, xls, jpg, 3gp, dan lainnya (kecuali exe) yang telah menyatu dengan Virus

Nelson Butar Butar
nelson.virologi@yahoo.com
ditulis pada tanggal 03-10-2008 pkl. 16.14 Wita di Waingapu, Sumba Timur-NTT

Anda pernah menjadi korban dari serangan virus komputer bukan? Jika ya, mungkin Anda pernah mengalami hal aneh. Ketika Anda hendak membuka file doc (Microsoft word), xls (Microsoft Excel), jpg (file gambar), 3gp (file video), atau lainnya, yang terjadi adalah file Anda tidak terbuka. Yang kedua, bisa terbuka tapi hanya aplikasi pengolah kata (mis, Microsoft word) yang terbuka sedangkan file Anda tidak ditampilkan. Yang ketiga, bisa terbuka tapi aplikasi pengolah kata/ angka menampilkan dalam keadaan berantakan. Yang keempat, tidak bisa terbuka/ ditampilkan sama sekali. Ini adalah ciri-ciri file yang telah dijangkiti Virus.

Pendahuluan

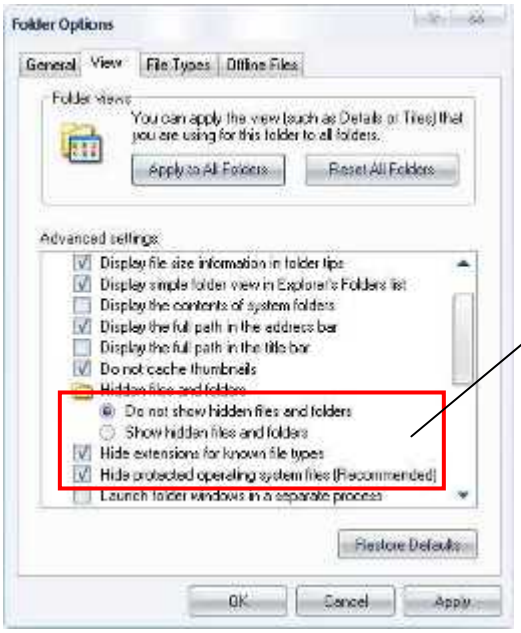
Teknik penularan virus komputer seperti ini sudah umum dimiliki oleh virus-virus, terutama virus lokal (made in indonesia). Dengan menjangkiti data pengguna, virus dapat tetap mempertahankan keberadaannya di dalam sistem operasi komputer.
Sistem Bahasa komputer, ada yang dikenal dengan hexa. Hexa adalah sistem bahasa komputer dengan menggunakan 16 simbol (0,1,2,3,4,5,6,7,8,9,A,B,C,D,E,F) yang mewakili 1 byte karakter alfanumerik dengan menggunakan 2 simbol (Penulis akan membahasnya di bagian isi). Kenapa penulis membahas sistem bahasa ini? Karena kita akan menggunakan program untuk mengedit file dalam bentuk bahasa hexa, salah satunya adalah HxD (hexa editor) yang dibuat oleh Maël Hörz. Dapat diunduh dari alamat berikut http://mh-nexus.de/downloads/HxDen.zip.
(catatan : alamat ini mungkin saja suatu saat bisa berubah. Maka yang perlu dilakukan adalah masuk dulu ke alamat http://mh-nexus.de, cari menu Download dan silahkan pilih program HxD sesuai bahasa lalu klik download)

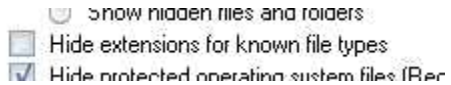
Sekedar Anda ketahui cara kerja virus secara sederhana yang menggunakan teknik penjangkitan ini :
1. Virus masuk dan aktif di dalam sistem operasi komputer;
2. Melakukan aksinya, seperti pemblokiran program, membatasi hak akses
3. Menjangkiti data/ file-file pengguna komputer (user).
   Kadang sebelum file dijangkiti, file asli disembunyikan lalu membuat sebuah file virus dengan menggunakan nama dan ikon seperti file asli. Tujuan untuk mempertahankan keberadaannya dengan mengelabui user.

Ada juga yang menjangkiti file dengan cara menggabungkan diri/ menyatu dengan file aslinya. Ini cara yang paling efektif agar virus bisa tetap bertahan.

Kasus-kasus seperti ini sering saya dapati pada komputer user yang terserang virus. Tapi jangan takut, karena penulis akan membantu Anda dengan cara manual yang sudah diuji coba.

Penulis membatasi penjelasan untuk kasus file yang menyatu dengan virus. Misalnya doc atau jpg yang tidak/ bisa terbuka tapi ekstensinya berubah (doc berubah menjadi exe atau scr)
Agar ekstensinya terlihat, lakukan cara berikut :
> Buka Windows Explorer, pada menu Tools pilih Folder Options... lalu pilih tab View, lalu lakukan seperti pada gambar.





Hilangkan tanda centang dengan klik 1x pada :
Hide extensions for known file types

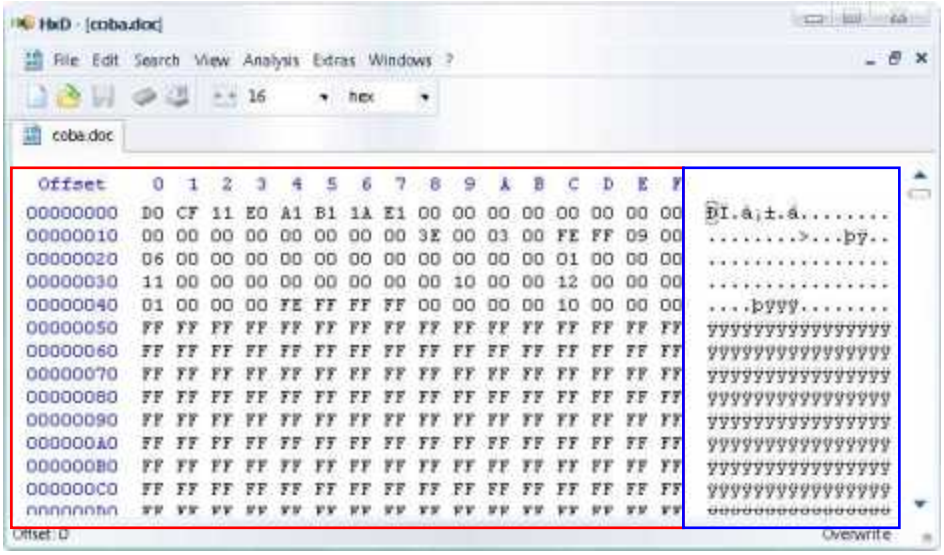
Klik OK.

Isi

→ **Langkah AWAL** yang perlu Anda lakukan adalah mengunduh/ download aplikasi pengedit hexa dari alamat http://mh-nexus.de/downloads/HxDen.zip. Software ini ditampilkan dalam bahasa inggris. Setelah terdownload, ekstrak file HxDen.zip. Lebih baik letakkan dalam folder tersendiri. Terdapat 3 file txt (license.txt, readme.txt, changelog.txt) dan 1 file exe (HxD.exe).
Software ini portable (bisa dibuka tanpa proses instal).

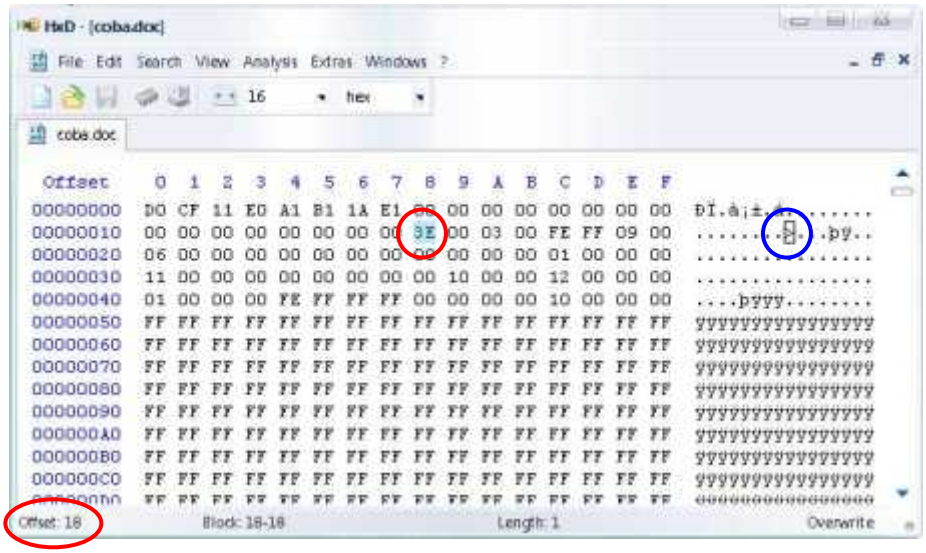
→ **Langkah KEDUA**, setelah ekstrak, klik 2x pada HxD.exe untuk menjalankan software. Jika muncul sebuah kotak konfirmasi *First Start of HxD*, klik OK.
Lalu pada menu File klik Open untuk membuka file.

Maka akan muncul seperti ini (misalnya penulis membuka file coba.doc)

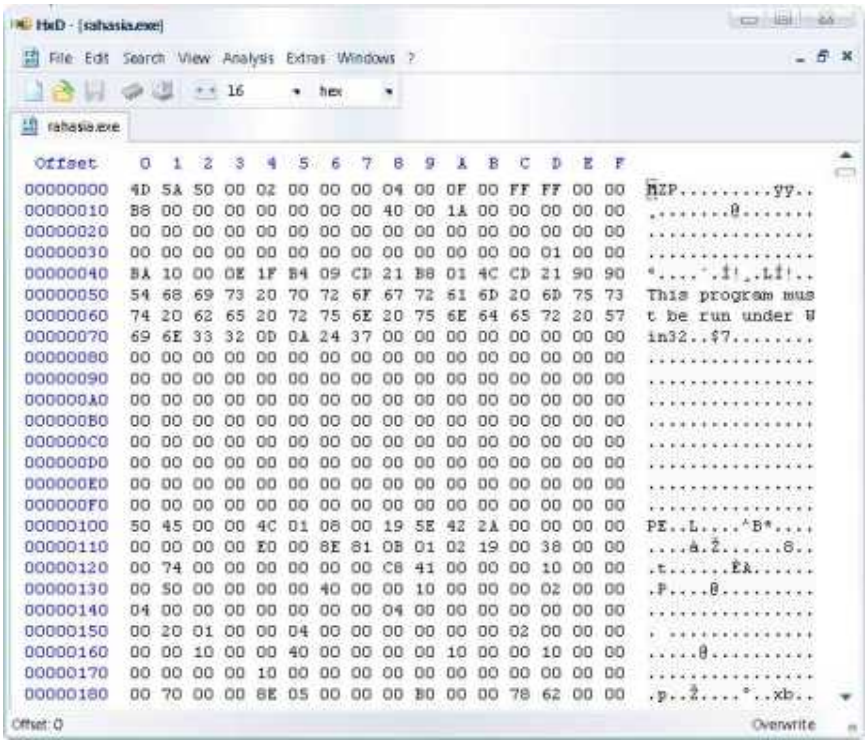


Nah perhatikan.
Halaman ini ditampilkan dalam 2 bahasa. Sebelah kiri bahasa Hexa (bahasa yang dipahami komputer) dan kanan bahasa Desimal (bahasa yang dipahami user).
Pada bahasa Hexa terlihat 2 karakter yang berdekatan. Masing-masing mewakili 1 karakter pada bahasa Desimal. Contoh : “ A1 ” pada Hexa mewakili karakter “ ; ” pada Desimal.

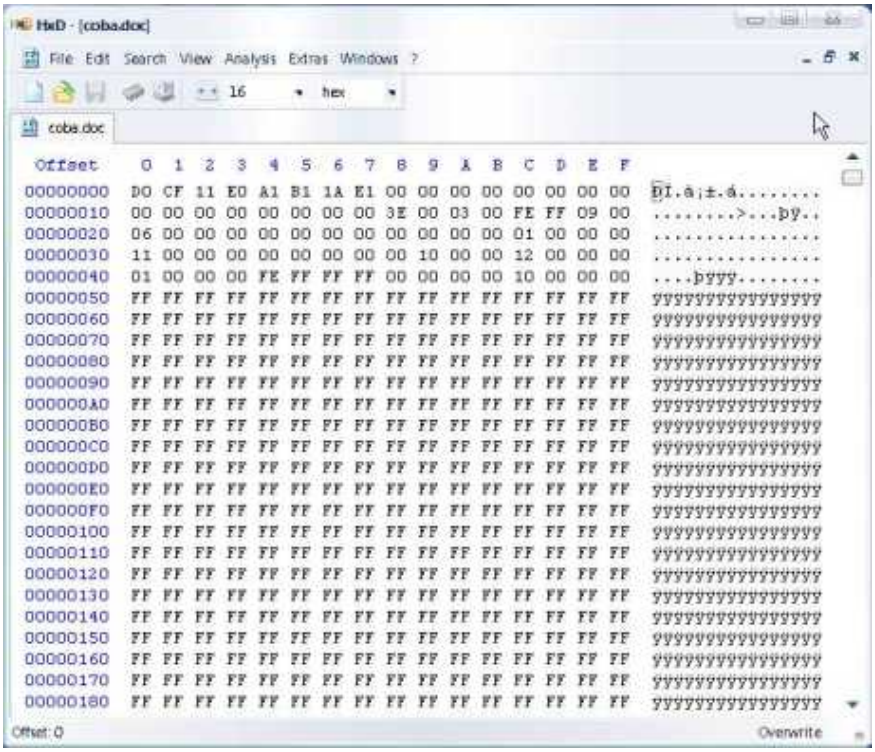
Pada halaman, terdapat istilah Offset. Ini dipakai untuk pemetaan sel (seperti pada microsoft excel).
Misalnya, baris 00000010 kolom 8 dibaca Offset: 00000018 atau disingkat 18. Pada gambar, Offset 18 jatuh pada **3E** (Hexa) atau karakter > (Desimal)



Sekarang saya akan mencoba membuka contoh file yang sudah dijangkiti virus (kspoold.A)



Lalu saya membuat sebuah file doc baru bernama coba.doc yang bebas virus untuk perbandingan.



Apa perbedaannya?
Ya, perhatikan...

Offset	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F	
00000000	D0	CF	11	E0	A1	B1	1A	E1	00	00	00	00	00	00	00	00	ÐÏ.à¡±.á.....
00000010	00	00	00	00	00	00	00	00	3E	00	03	00	FE	FF	09	00	.....>...þÿ..
00000020	06	00	00	00	00	00	00	00	00	00	00	00	00	01	00	00	.....
00000030	11	00	00	00	00	00	00	00	00	10	00	00	12	00	00	00	.....
00000040	01	00	00	00	FE	FF	FF	FF	00	00	00	00	10	00	00	00	....þÿÿÿ.....
00000050	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	ÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿ
00000060	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	ÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿ
00000070	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	ÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿ
00000080	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	ÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿ

Gambar 1. **Ini asli** (bebas virus)

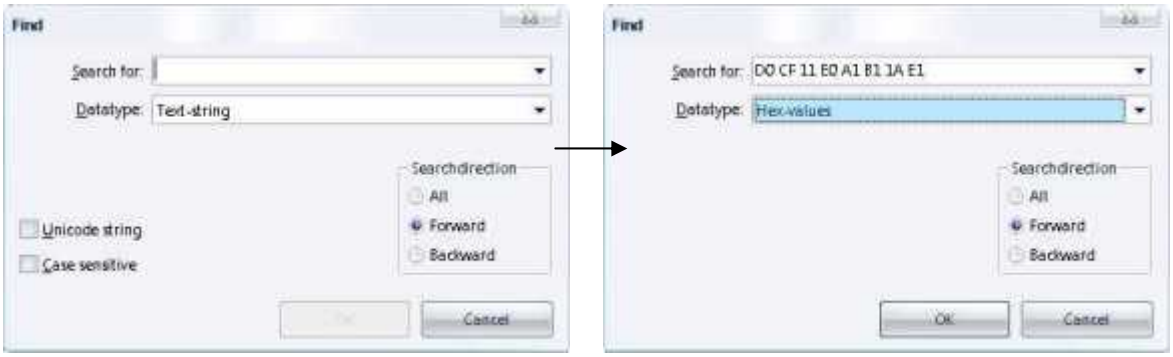
Offset	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F	
00000000	4D	5A	50	00	02	00	00	00	04	00	0F	00	FF	FF	00	00	MZP.....ÿÿ..
00000010	B8	00	00	00	00	00	00	00	40	00	1A	00	00	00	00	00	.....@.....
00000020	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	.....
00000030	00	00	00	00	00	00	00	00	00	00	00	00	00	01	00	00	.....
00000040	BA	10	00	0E	1F	B4	09	CD	21	B8	01	4C	CD	21	90	90	°....´.Í!¸.LÍ!..
00000050	54	68	69	73	20	70	72	6F	67	72	61	6D	20	6D	75	73	This program mus
00000060	74	20	62	65	20	72	75	6E	20	75	6E	64	65	72	20	57	t be run under W
00000070	69	6E	33	32	0D	0A	24	37	00	00	00	00	00	00	00	00	in32..$7.....

Gambar 2. **Ini palsu**.

Yang menjadi referensi utama untuk perbandingan adalah
Gambar 1. >> Perhatikan Offset 0 sampai Offset 7 (D0 CF 11 E0 A1 B1 1A E1).

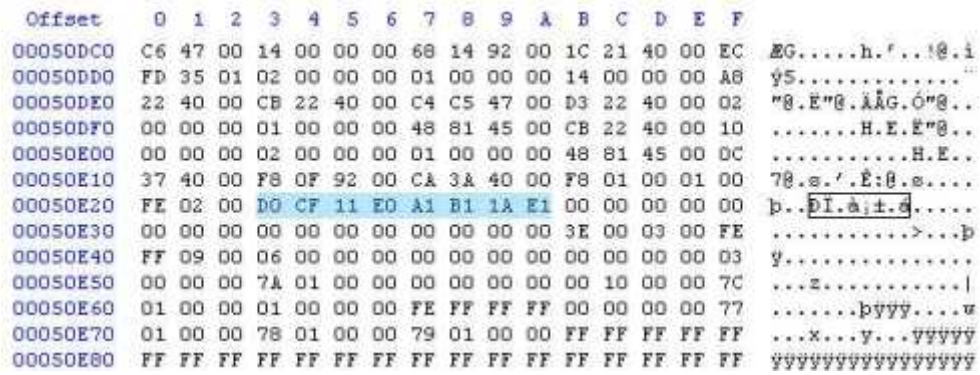
Inilah Offset KUNCI untuk menghapus semua “kebohongan”.

→ **Langkah KETIGA**. Blok Offset 0 – 7 pada file doc yang asli dan klik kanan pilih Copy. Buka doc yang dijangkiti virus, kemudian pada menu Search, pilih Find.



Klik kanan pada kotak Search for, pilih Paste. Pada Datatype, ubah menjadi Hex-values. Dan klik OK untuk memulai pencarian.

Hasil pencarian....



Offset	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F	
00050DC0	C6	47	00	14	00	00	00	68	14	92	00	1C	21	40	00	EC	ÆG.....h.'..!@.ì
00050DD0	FD	35	01	02	00	00	00	01	00	00	00	14	00	00	00	A8	ý5.....¨
00050DE0	22	40	00	CB	22	40	00	C4	C5	47	00	D3	22	40	00	02	"@.Ë"@.ÄÅG.Ó"@..
00050DF0	00	00	00	01	00	00	00	48	81	45	00	CB	22	40	00	10	.......H.E.Ë"@..
00050E00	00	00	00	02	00	00	00	01	00	00	00	48	81	45	00	0C	...........H.E..
00050E10	37	40	00	F8	0F	92	00	CA	3A	40	00	F8	01	00	01	00	7@.ø.'.Ê:@.ø....
00050E20	FE	02	00	D0	CF	11	E0	A1	B1	1A	E1	00	00	00	00	00	þ..ÐÏ.à¡±.á.....
00050E30	00	00	00	00	00	00	00	00	00	00	00	3E	00	03	00	FE	...........>...þ
00050E40	FF	09	00	06	00	00	00	00	00	00	00	00	00	00	00	03	ÿ...............
00050E50	00	00	00	7A	01	00	00	00	00	00	00	00	10	00	00	7C	...z...........|
00050E60	01	00	00	01	00	00	00	FE	FF	FF	FF	00	00	00	00	77	.......þÿÿÿ....w
00050E70	01	00	00	78	01	00	00	79	01	00	00	FF	FF	FF	FF	FF	...x...y...ÿÿÿÿÿ
00050E80	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	ÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿ

Ternyata, didapat Offset KUNCI-nya (Offset 50E23 – 50E2A) yang mengandung Hexa KUNCI (Asli) seperti pada file asli. Ini yang menjadi patokan.
Kita dapat menyimpulkan bahwa : Hexa yang berada di belakang Offset KUNCI adalah Hexa VIRUS.

→ **Langkah KEEMPAT**. Selanjutnya, lakukan penghapusan Hexa VIRUS dengan cara Blok semua Hexa tepat mulai dari Offset 50E22 – 00000 (00000 = awal) dan tekan tombol Delete pada kibor. (ini semua berdasar contoh kasus. Offset virus tidak selalu berada pada Offset seperti yang tertera pada contoh).

Ingat! Yang menjadi patokan adalah Harga Hexanya (D0 CF 11 E0 A1 B1 1A E1).

Lalu simpan.
Setelah itu, ubah ekstensi file yang telah disimpan tadi dengan cara klik kanan pada file dan pilih Rename (atau tekan tombol F2 pada kibor), lalu ubah .exe menjadi .doc atau mungkin ekstensi sebelumnya .scr ubah menjadi .doc. (rahasia**.exe** menjadi rahasia**.doc**).

Lakukan juga seperti 4 langkah di atas untuk memulihkan (*restore*) file berekstensi lainnya yang dijangkiti virus. Berikut saya berikan referensi Hexa yang dapat Anda pakai untuk mencari Offset KUNCI pada file palsu, sebagai berikut :

1. doc = D0 CF 11 E0 A1 B1 1A E1
2. xls = D0 CF 11 E0 A1 B1 1A E1
3. ppt = D0 CF 11 E0 A1 B1 1A E1
4. pdf = 25 50 44 46
5. jpg = FF D8 FF E1
6. gif = 47 49 46 38 39 61
7. 3gp = 00 00 00 1C 66 74 79 70 33 67 70 34
8. avi = 52 49 46 46

Untuk ekstensi/ tipe file lain dapat Anda temukan sendiri dengan cara membuka file menggunakan HxD, lalu lihat Hexa pada beberapa Offset awal. Lakukan perbandingan lebih dari satu kali akan membuat Anda menemukan Offset KUNCI yang tepat.

Teknik Pemulihan/ Restorasi ini cukup efektif untuk membersihkan data Anda dari Virus. Kelebihan cara seperti ini tidak hanya untuk menghapus virus, tapi bisa juga untuk memperbaiki file Anda dari kerusakan. Seperti doc. Mungkin Anda pernah membuka file doc Anda, terbuka namun isinya berantakan dan dalam bentuk simbol-simbol aneh. Anda bisa melakukan seperti langkah-langkah tadi untuk memperbaikinya.

Penutup

Demikian yang bisa penulis bagikan pada Anda, semoga bermanfaat.

Biografi Penulis

Nelson P. Butar Butar. Dilahirkan di propinsi NTT tepatnya di kota Kupang, 20 Agustus 1987. Lulus SMAN 1 Kupang pada tahun 2005. Sekarang bekerja pada salah satu instansi di propinsi NTT.

Info lebih lanjut tentang penulis bisa didapat melalui:
Email : *nelson.virologi@yahoo.com*
Blog : *http://solusi-virus.blogspot.com*