

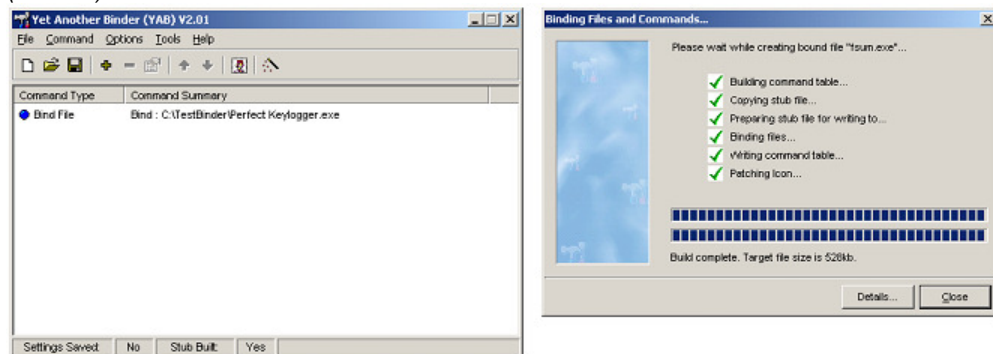
Pengecekan Terhadap Keaslian Suatu Dokumen untuk Menghindari Kejahatan Komputer (*Computer Crime*)

H. Mochamad Wahyudi, MM, M.Kom, CEH, CHFI
Program Pascasarjana Magister Ilmu Komputer STMIK Nusa Mandiri
Jl. Salemba Raya No. 5 Jakarta 10440
wahyudi@nusamandiri.ac.id

Jumlah kejahatan di bidang komputer (*computer crime*) akhir-akhir ini semakin marak terjadi. Hal tersebut sering terjadi karena pada saat ini banyak sekali aplikasi-aplikasi bisnis yang menggunakan komputer atau teknologi informasi (*internet*) sebagai media untuk saling bertukar data maupun program (*software*). Kejahatan di bidang komputer juga didukung lagi dengan semakin meningkatnya kemampuan para pemakai komputer yang pada awalnya hanya sebagai seorang *user* biasa, namun saat ini sudah banyak yang mulai melakukan percobaan atau bermain-main dengan atau bahkan membongkar sistem yang digunakannya untuk lebih memahami secara detail tentang sistem tersebut. Hal ini juga diperburuk lagi dengan banyak beredarnya peralatan (*tools*) yang berupa *software* mulai dari yang gratis alias *free* sampai dengan yang harus mengeluarkan sedikit uang untuk memperolehnya dari *internet* yang dapat dipergunakan untuk melakukan kejahatan di dalam dunia maya (*cyber*).

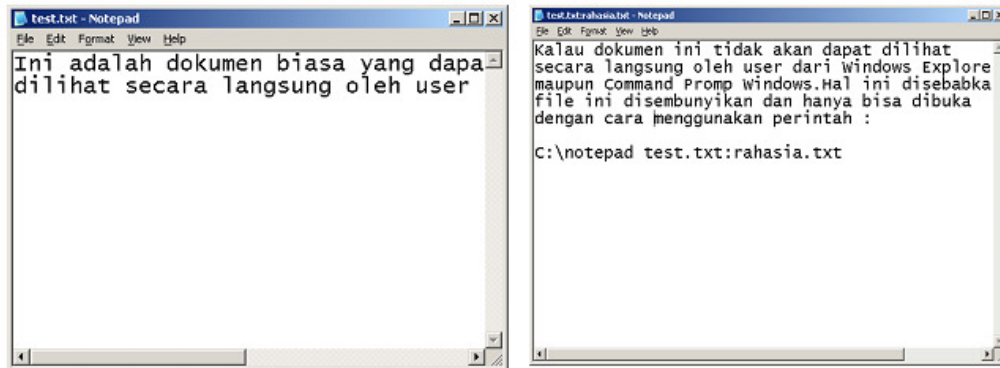
Ada beberapa cara yang banyak dilakukan oleh orang-orang yang tidak bertanggung jawab untuk melakukan kejahatan komputer yang berkaitan dengan penggunaan media pertukaran data secara elektronik dalam bentuk file, antara lain :

1. Mengirimkan file yang di-*bundeling* menjadi satu dengan *file* yang mengandung program *virus*, *trojan*, *spyware* dan sejenisnya (file-file *executable* dalam format *.EXE & *.COM) yang apabila dieksekusi oleh seseorang yang maka program-program tersebut akan ter-*install* dikomputer pengguna. Dampaknya yang lebih buruk lagi adalah apabila pengiriman *file* tersebut di dalamnya dipasangkan suatu program sejenis *keylogger*, maka apapun yang diketikkan oleh *user* melalui *keyboard* komputernya maka akan dikirimkan secara periodik ke *e-mail* pemasang program (*hacker*) tersebut melalui *internet* / *intranet*.

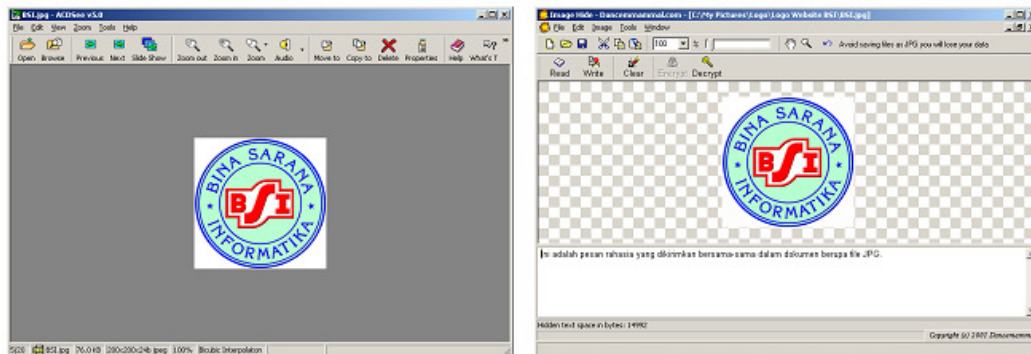


2. Mengirimkan pesan rahasia yang dikirimkan bersama-sama dengan *file* yang dikirimkan ke orang lain. Misalnya saja seorang mengirimkan suatu dokumen kepada orang lain, tetapi pengirim dokumen tersebut menyisipkan suatu *file* rahasia yang dibuat dengan sengaja untuk menghindari sensor terhadap data-data yang telah dikirimkan. Hal ini juga sangat dimungkinkan dilakukan oleh para teroris yang akan memanfaatkan pengiriman pesan rahasia melalui media elektronik dalam bentuk *file*. Hal ini dilakukan dengan memanfaatkan *slack space* yang ada pada *hardisk* dengan menggunakan metode *ADS "NTFS" Streaming*. Jadi *file* yang dibuat tidak akan terlihat karena letaknya yang

tersembunyi di dalam *slack space* pada *hardisk* meskipun dicari dengan perintah internal *command* di DOS atau Microsoft Windows seperti DIR atau menggunakan Windows Explorer.



3. Penyisipan pesan-pesan ke dalam dokumen dalam bentuk format gambar (JPEG, JPG, GIF, PIP, TIF, dll) dengan maksud untuk melakukan pengiriman pesan rahasia yang tidak dapat dilihat secara langsung.



Dari ketiga contoh yang penulis jelaskan tadi, sebenarnya contoh-contoh tersebut merupakan salah satu cara melindungi informasi dengan teknik *steganografi*. Dimana dengan suatu teknik tertentu informasi dikirimkan dan dibuat seolah-olah pesan rahasia yang dikirimkan tidak ada atau tidak nampak, padahal pesan tersebut ada dan hanya saja kita tidak sadar bahwa sebenarnya pesan tersebut ada. Penggunaan teknik *steganografi* untuk mengirimkan data (dokumen) untuk tujuan yang baik sangat disarankan, apalagi apabila kita menginginkan informasi yang akan dikirimkan tersebut tidak ingin bocor ditengah jalan dan rahasia yang akan dikirimkan akan diterima oleh orang-orang yang tidak bertanggung jawab.

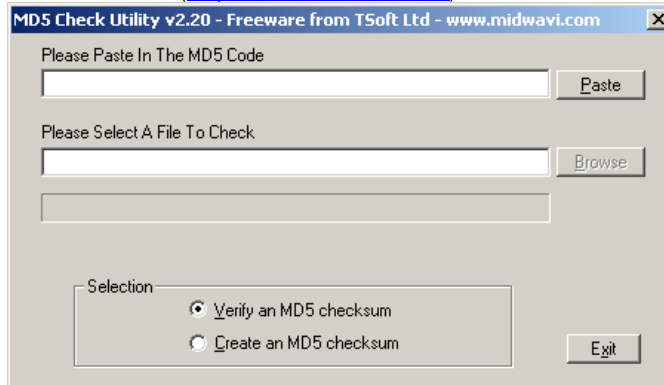
Untuk menghindari dari penyalahgunaan tadi, sebaiknya anda melakukan pengecekan terhadap *file-file* yang dibuat maupun yang anda terima, baik berupa file dokumen maupun *file-file* berupa program (*software*). Pengecekan dilakukan dengan menggunakan mengecek *hash* dari suatu *file* dengan menggunakan suatu *Algoritma Hash Function* tertentu. Beberapa algoritma *Hash Function* yang populer antara lain adalah : MD2/4/5, SHA1/2/256/512, RMD, Tiger, Panama, Adler, CRC32 dan Edonkey.

Software populer yang dapat dipergunakan untuk melakukan *checksum*, antara lain :

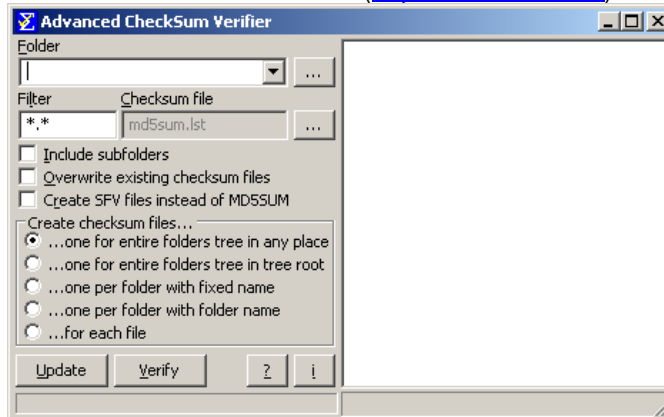
1. Fsum (<http://www.fsum.org>)

```
C:\WINDOWS\system32\cmd.exe
C:\>fsum -md5 "Basic Networking.doc"
SlavaSoft Optimizing Checksum Utility - fsum 2.51
Implemented using SlavaSoft QuickHash Library <www.slavasoft.com>
Copyright (C) SlavaSoft Inc. 1999-2004. All rights reserved.
; SlavaSoft Optimizing Checksum Utility - fsum 2.51 <www.slavasoft.com>
;
; Generated on 07/27/06 at 14:32:00
;
; 7228aebb3423c01361db0e456f71ccd *Basic Networking.doc
C:\>
```

2. MD5 Checker (<http://www.soft14.com>)

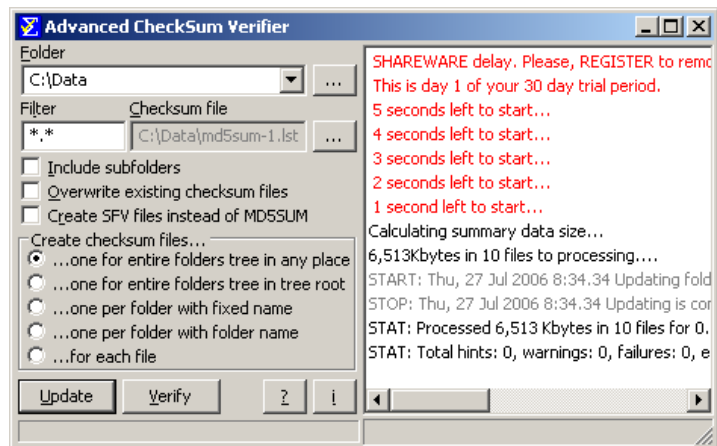


3. Advanced CheckSum Verifier (<http://www.iris.net/>)

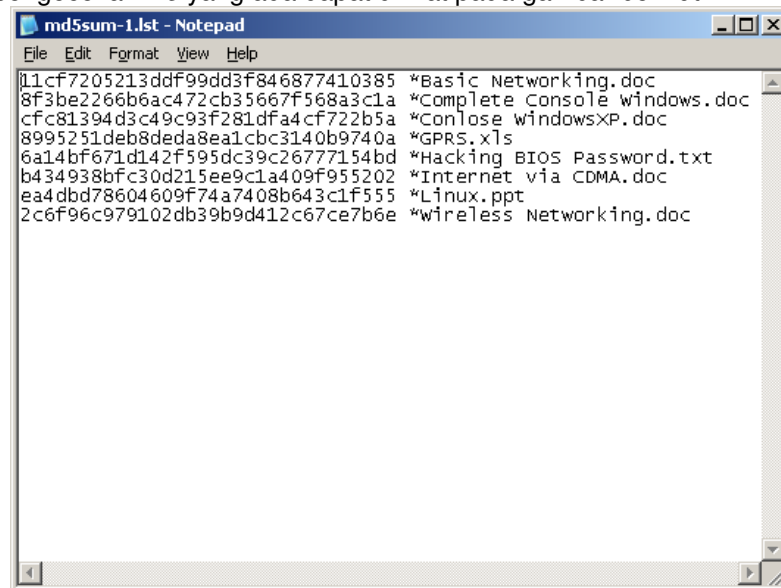


Penulis akan mencoba untuk menjelaskan pengecekan data-data penulis yang terdapat pada folder C:\Data, yang di dalamnya terdapat 8 (delapan) file, yaitu : Basic Networking.doc, Complete Console Windows.doc, Conlose WindowsXP.doc, GPRS.xls, Hacking BIOS Password.txt, Internet via CDMA.doc, Linux.ppt dan Wireless Networking.doc. Pada contoh ini penulis menggunakan *software* Advanced CheckSum Verifier untuk melakukan *checksum* dari file-file tersebut menggunakan *Algoritma MD5* yang sangat populer.

Bukalah program Advanced CheckSum Verifier, kemudian masukan *folder* yang anda inginkan untuk melakukan pengecekan terhadap file yang ada di dalamnya. Setelah itu silahkan tentukan file hasil pengecekan. Dalam contoh ini penulis meyimpannya ke dalam *folder* C:\Data\md5sum-1.lst. Hasil pengecekan tersebut disimpan ke dalam file dengan format *clear text* yang dapat dibuka menggunakan *editor* seperti Notepad.



Hasil dari pengecekan *file* yang ada dapat dilihat pada gambar berikut ini :



Pada setiap *file* asli milik penulis tersebut terlihat kode-kode bilangan heksa desimal yang panjangnya adalah 32 bit. Hasil *checksum* dari *file* tersebut tidak akan pernah sama antara satu *file* dengan *file* lainnya. Hal yang harus diperhatikan adalah, bahwa setiap perubahan yang terjadi pada suatu *file*, sekecil apapun perubahannya maka kode-kode tersebut akan berubah.

Berikut ini penulis mencoba melakukan perubahan terhadap *file* Basic Networking.doc yang ada folder C:\Data. Untuk menunjukkan perbedaan yang terjadi pada, perhatikanlah hasil *checksum* pada gambar berikut ini :

```
md5sum-2.lst - Notepad
File Edit Format View Help
77228aebb3423c01361db0e456f71ccd *Basic Networking.doc
8f3be2266b6ac472cb35667f568a3c1a *Complete console windows.doc
cfc81394d3c49c93f281dfa4cf722b5a *Conlose windowsXP.doc
8995251deb8deda8ea1cbc3140b9740a *GPRS.xls
6a14bf671d142f595dc39c26777154bd *Hacking BIOS Password.txt
b434938bfc30d215ee9c1a409f955202 *Internet via CDMA.doc
ea4dbd78604609f74a7408b643c1f555 *Linux.ppt
2c6f96c979102db39b9d412c67ce7b6e *wireless Networking.doc
```

Hasil dari pengecekan *file* Basic Networking.doc tersebut terlihat perbedaan pada kode-kode yang dihasilkan sebagai berikut :

1. File asli : 11cf7205213ddf99dd3f846877410385 *Basic Networking.doc
2. File hasil modifikasi : 77228aebb3423c01361db0e456f71ccd *Basic Networking.doc

Perubahan terhadap *file* tersebut bisa saja dilakukan langsung oleh pemilik dokumen secara sah, tetapi juga dapat dilakukan oleh pihak lain yang bertanggung jawab. Misalnya dengan memodifikasi *file* tersebut dan ditambahkan ke dalamnya sejenis *virus*, *trojan*, *backdoor*, *spyware* ataupun *keygen* seperti di jelaskan sebelumnya.

Beberapa hal yang harus dilakukan dalam menerima atau mengirimkan data atau *transfer (software / program)* bahkan *men-download file* dari *internet* baik secara *free*, *freeware* maupun harus membayar (membeli) adalah:

1. Lakukan pengecekan *md5checksum* sebelum mengirimkan file agar anda mengetahui kealian dari file asli anda.
2. Lakukan pengecekan terhadap file yang diterima dari seseorang dengan cara meminta hasil *md5checksum* dari pengirim, kemudian lakukanlah *cross check* dengan hasil *checksum* yang anda lakukan sendiri terhadap file yang anda diterima.
3. Untuk file-file yang diterima dengan cara *men-download* dari *internet*, pastikanlah anda *men-download*-nya dari *situs* atau *website* resmi dari pembuat *software* tersebut atau penjual resminya. Secara umum biasanya pembuat *software* atau penjual resmi akan menampilkan *md5checksum* dari file yang dibuat atau dijualnya, yaitu dengan menampilkan 32 bit kode dalam bilangan heksa decimal hasil *checksum*.