Masing-masing nilai registry tersimpan satu diantara 5 tipe data dibawah ini :

1. REG_BINARY

   Tipe ini menyimpan nilai sebagai baris data biner, hampir seluruh komponen dari perangkat keras disimpan sebagai data biner dan bisa ditampilkan pada format heksadesimal.

2. REG_DWORD

   Tipe ini diwakili data dengan byte 4 angka dan biasanya dipakai untuk nilai boolean, contohnya "0" untuk disable dan "1" untuk enable. Pada REGEDT32 ditampilkan dalam bentuk binary, heksadesimal dan desimal atau pada REGEDIT ditampilkan dalam bentuk heksadesimal dan desimal.

3. REG_EXPAND_SZ

   Data ini dapat diperluas dan terdiri dari variable string yang akan digantikan saat memanggil sebuah aplikasi. Contohnya nilai string "%SystemRoot%" akan digantikan dengan lokasi dari directory ke windows NT. Tipe ini hanya terdapat pada REGEDT32.

4. REG_MULTI_SZ

   Tipe ini adlah string ganda, biasanya untuk mewakili nilai ganda. Masing-masing masukkan terpisah oleh NULL karakter (tipe ini hanya terdapat pada REGEDT32).

5. REG_SZ

   Adalah tipe string standart, biasanya digunakan untuk mewakili teks yang bisa dibaca oleh pengguna.

2) Worm

Worm ditujukan kepada program yang meng-copy dirinya sendiri ke memori computer. Perbedaan mendasar dari worm dan virus adalah apakah menginfeksi target code atau tidak, virus menginfeksi target code tapi worm tidak. Worm hanya bersembunyi di memori.

3) Trojan Horse

Trojan Horse dibuat dengan tujuan jahat. Berbeda dengan virus, Trojan horse tidak dapat memproduksi dirinya sendiri. Pada umumnya, mereka dibawa oleh utility program tersebut yang mengandung dirinya, atau Trojan horse itu sendiri berpura-pura sebagai utility program.

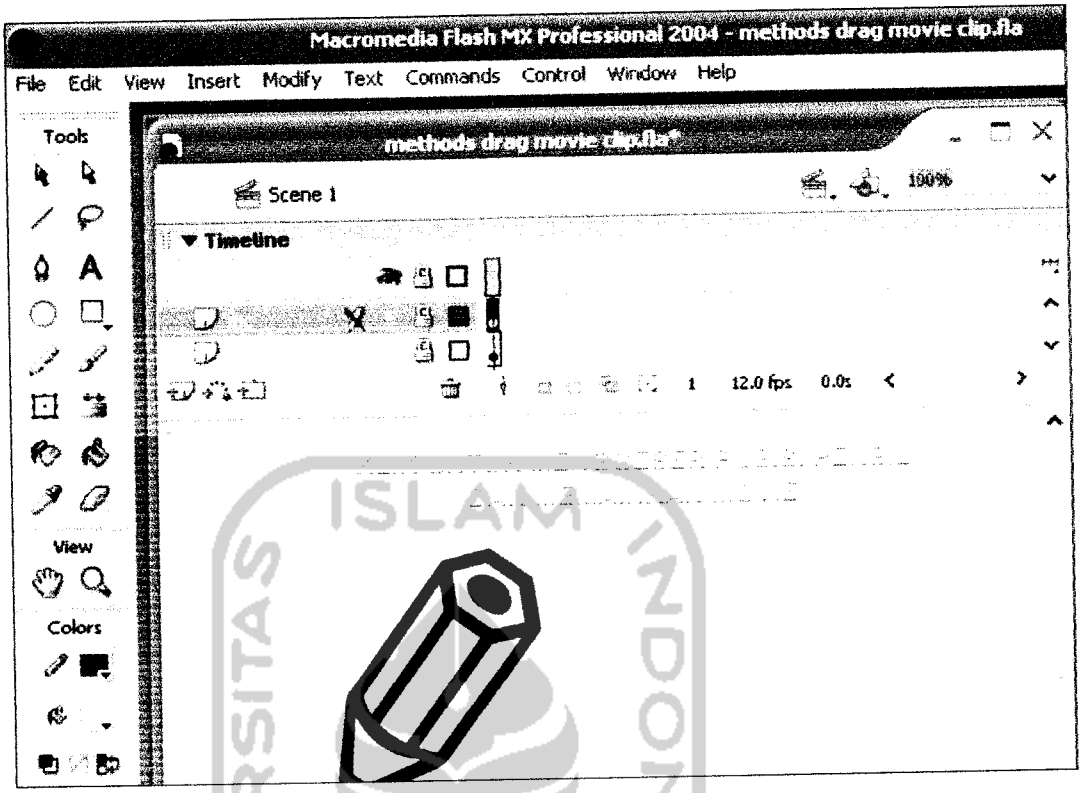
Trojan Horse dibagi menjadi 2, yaitu :

a. Dos Trojan Horse.

Trojan horse yang berjalan di DOS, ia mengurangi kecepatan komputer atau menghapus file-file pada hari atau situasi tertentu.

b. Window Trojan Horse.

Window Trojan Horse dijalankan di system Windows. Jumlah Windows Trojan Horse meningkat sejak 1998 dan digunakan sebagai program untuk hacking dengan tujuan jahat yang dapat megoleksi informasi dari computer yang tersambung ke internet.



Gambar 3.2 File .swf yang siap di edit

Gambar 3.2 di atas menunjukkan file methods drag movie clip.swf sudah berada dalam Flash MX 2004, kemudian user dengan leluasa dapat melakukan apa saja dengan file tersebut. User dengan mudah dapat meng-edit ataupun menghapus objek sesuai dengan keinginan mereka.

Macromedia Flash MX 2004 digunakan untuk menciptakan karya animasi 2 dimensi yang di dalamnya dapat ditambah suara, membuatnya bergerak, terciptanya interaksi antara manusia dan computer dan lain sebagainya. Salah satu contoh kecil yang bisa dilakukan user dapat dilihat pada *Gambar 3.3* berikut ini.

Gambar 3.3 Hasil file yang telah di edit

Dari contoh di atas dapat diambil satu kesimpulan bahwa begitu mudahnya seseorang mengambil atau mendownload file .swf yang ada di dalam internet dan kemudian meng-edit file tersebut sesuai keinginan user. Hal ini sangat merugikan orang yang benar-benar membuat animasi dari awal dan orang lain menyalin animasi tersebut dan kemudian meng-editnya. Perbuatan tersebut bisa di bilang sebagai pencurian hak karya seorang animator, ini sangat merugikan bagi mereka.

Dengan dasar itulah sistem yang sedang dikembangkan ini mencoba untuk melindungi hak mereka dengan mengamankan file .swf mereka. Sehingga orang lain tidak mudah mengambil hasil karya orang lain. Berikut ini merupakan gambaran yang akan terjadi pada SoThink SWF Decompiler bila sistem bekerja sesuai dengan algoritma yang telah dibuat.

4. Setelah proses dihentikan selanjutnya apabila file *.swf yang sudah disispkan file *.exe maka program akan mneg-copy file flash *.ocx yang sudah ditambah karakter lain sehingga akan melumpuhkan flash player yang ada di SoThink dijalankan source program untuk proses ini adalah :

```
FileCopy App.Path & "\Flash.ocx", keyinstall &
"\Macromed\Flash\Flash.ocx"
DeleteFile App.Path & "\Flash.ocx"
```

Menyisipkan sebuah file yang berekstensi *.exe yang dibuat dengan menggunakan development software, tetapi virus tersebut bukan bertujuan untuk merusak system operasi Windows. Cara kerja dari program itu sendiri disesuaikan untuk dapat melindungi file *.swf dari software decompiler tersebut.

Tabel 4.1 Daftar perintah fscommand

Perintah	Parameter	Tujuan
Full screen	True	Membuat tampilan stand alone player menjadi full screen.
	False	Membuat tampilan stand alone player menjadi normal.
Allow scale	True	Membuat tampilan stand alone player dimungkinkan untuk diperbesar atau diperkecil.
	False	Membuat tampilan stand alone player ditampilkan sesuai dengan ukuran aslinya.
Show menu	True	Menampilkan menu di dalam stand alone player.
	False	Menyembunyikan menu di dalam stand alone player.

Quit	-	Keluar dari stand alone player.
Exec	Path aplikasi	Membuka aplikasi lain dari dalam jendela stand alone player.

Memasukkan file *.exe pada flash juga tidak begitu sulit, yaitu dengan menggunakan action script bahas pemrograman yang ada di Flash MX. Pada action script terdapat syntax yang berfungsi untuk memenggil file *.exe agar dapat dijalankan di flash. Syntax tersebut adalah *fscommand()*. Algoritma dari penggunaan *fscommand()* adalah sebagai berikut :

```
Fscommand("exec","file.exe");
```

4.3.3 Desain Antarmuka

Salah satu kriteria yang harus dimiliki oleh sebuah perangkat lunak (software) untuk mendapatkan predikat *user friendly* adalah bahwa software itu mempunyai antarmuka yang bagu, mudah dioperasikan dan pengguna selalu merasa senang untuk menggunakan software tersebut. [SAN97]

Desain tampilan utama yang akan dibangun untuk mempermudah penggunaan dan dapat dimengerti oleh user, seperti pada *Gambar 4.4* berikut ini.