ABSTRAK

Produk antivirus yang ada pada masa kini hanya mampu untuk mengesan kewujudan virus, namun ia tiada kemampuan untuk mencatatkan aktiviti serta sifat-sifat bagi sesuatu virus. Bagi sesetengah pengguna, ini adalah salah satu kesukaran bagi mereka untuk mengetahui sifat-sifat sesuatu virus termasuk untuk mengetahui kategori bagi satu-satu virus. Sebenarnya, terdapat beberapa alat yang telah dicadangkan oleh beberapa pengkaji, namun persoalan mengenai kesesuaian bagi sesetengah pengguna yang ingin tahu tentang kategori virus yang telah di uji dan lain masih belum terjawab.

Kajian yang dilakukan dalam thesis ini adalah satu kajian mengenai jenis-jenis virus dan antivirus masa kini, serta system pemantau dan penganalisis, untuk menjumpai punca masalah yang mana ianya juga merupakan asas kepada kajian ini. Pada projek ini, kami mencadangkan sistem dan senibina yang mampu memantau sifat-sifat virus dan mampu untuk mengkategorikan samada virus tersebut merupakan virus tradisional atau virus polimorfik. Kajian pada peringkat awalnya dijalankan untuk mendapatkan sifat-sifat virus pada masa kini dan untuk mencari parameter tertentu yang biasanya digunakan oleh virus untuk menyerang computer yang dijangkiti. Akhirnya, kami menggunakan "test bed environment" untuk menguji sistem kami dengan melepaskan virus dalam persekitaran yang nyata, dan cuba untuk menangkap perilaku dan sifat-sifat mereka, dan diikuti dengan membuat kesimpulan samada virus yang diuji atau dijangka tadi dapat diklasifikasikan sebagai virus tradisional atau polimorfik.