ABSTRACT

The current antivirus products were only able to detect the existence of viruses, but it could not record the activity or behavior of viruses. Inability of antivirus to record the viruses' behavior made difficult certain users who want to know the behavior of viruses as well as to know the category or classification of certain viruses. Actually, there were several architectures already proposed, but they still could not answer the needs of those certain users who want to know the classification of virus that they test.

In this project, we studied the current types of viruses as well as current virus monitoring and analysis system. This study came up with the problems that become basic of this research. Then, we proposed an architecture and a system, which are able to monitor the viruses' behavior and classify those viruses whether as a traditional or polymorphic virus. Preliminary research was conducted to get the current virus behaviors and to find out the certain parameters, which are usually used by viruses to attack the computer target. Finally, we applied "test bed environment" toward our system by releasing several viruses in a real environment, and attempt to capture their behaviors. These activities were followed by generating the conclusion that the tested or monitored virus is classified as a traditional or polymorphic virus.