“FORENSIC APPLICATION ON DISTRIBUTED NETWORK USING JADE”

Name : I Wayan Bevin Waranugraha
NRP : 5108 100 046
Department : Informatics Engineering - FTIf ITS
Supervisor I : Ary Mazharuddin, S.Kom, M.Comp.Sc
Supervisor II : Baskoro Adi Pratomo S.Kom, M.Kom

Abstract

In the real world there are always some people who commit crimes for personal gain, such crimes can be done to individuals or to an institution. Development of the internet world that is rapidly making entrepreneurs and companies aggressively advertise themselves as well as exchanging information, the information transfer system is certainly not without loopholes, many people who are not responsible exploit loopholes for personal gain such as identity theft, the spread pornography, financial fraud and other. Crime is very difficult to follow up, especially in Indonesia, because the complete lack of evidence of these crimes and scattered that difficult to handle but still has a footprint that can be traced, it is necessary for an application that can help gather evidence that the application is made by using mobile agent technology.

Mobile Agent is a program with an unique identity that able to move its code, the datas that on it and the condition between the machine are connected in a network. That Mobile agent's capability is derived from two disciplines that are artificial intelligence and distributed systems. The application of real-world mobile agent can be used to conduct forensics on a network so all the activities in and out of the data on the network can be recorded so that should help the search in case of digital evidence of a crime on the network.

To implement this forensic applications, the ability of mobile agent itself is not enough, here the mobile agent works as a data log carrier of the server Tcpdump, Snort server and web server to a central server.
In this final project will discuss how to build a forensic applications using the concept of mobile agent migration to distribute data from the server - slave servers to a central server, as well as discussion of the design of the agent in order to carry out these tasks and will also be studied the use of Tcpdump, Snort, and webserver in the construction of these networks so that helps a network analyst for digital evidence so that digital offenders can be penalized. After having tested, the forensic applications are made capable of displaying data - data log snort as much as 400 line 0.35 seconds it takes to search IP takes 0.27 seconds both the process takes less than 1 second while the data for as many as 10 line took 0.05 seconds so the larger the file size the longer time required.

**Keyword:** Log, Distribution, Mobile Agent, Forensic, Digital Evidence