CHAPTER 3

RESEARCH METHODOLOGY

The first step to complete this project is to search for references and journals via the internet that provide information about the package sniffer and malware analysis. Next learn the process theory that occurs when sending data packets based on OSI network architecture model (Open System Interconnection) model.

The next step is to create a sniffer program. The main library used is the socket library to capture raw data packets from the network and structs for binary data handling. Data will be stored in the sqlite database. After making the "packet sniffer" program complete, the next step is to design a web based program. This program serves to monitor the data obtained from packet sniffer.

The next step is to design a network topology. Topology is made simple by using Virtual Machines to run 2 virtual Windows, 2 virtual linux and 1 virtual linux as Router. The router acts as the link of two or more networks. The packet sniffer program will be installed on the PC Router. To test the program, one of these virtual windows will be deliberately given malware to know the difference with windows virtual uninfected malware on the network.