At first, rootkit is a serious type of malicious software that infects computer systems. The rootkit is seeking to take privileges higher than the privileges of administrators of the system, and also to get complete control of the machine, while it is completely hidden from the eyes of users, administrators and even the operating system itself. There are many techniques to detect rootkit like: memory dump analysis, signature based analysis, detecting interception, comparing data from different sources, and integrity check. At first, this project used memory dump analysis to detect kernel rootkit but there were some problems, so another technique which chosen is signature based analysis. So this project focuses on detecting the rootkit based on signature-based analysis technique in Windows platform. This technique was investigated and a simple rootkit detector was created. Moreover, a simple anti-virus has been developed based on signature-based technique.