Researchers and security expert has been vigorously on the study of malwares, great interest has been drawn to rootkits. Rootkits are a notably dangerously type of malware with the ability to cover their presence on the compromised host operating system and allow malicious recreation via spyware and other more obvious types of malware undetected. Once a rootkit gained access to a system, it can be very tough to track and do away with them. In this research, various antimalware tools were critically analyzed and studied to ascertain their effectiveness in combating a deadly malware called tdl-4. An analytical model developed was used to obtain all experimental results and findings which are documented for further work.