Rootkit is a fatal malware devouring user and kernel mode kind which inclines to take complete control of a compromised system by means of various infection and evasion techniques. Several detection algorithms has been offered and joined into the anti rootkit tools with many degree of performance in handling rootkit incidence. There is a severe rise in the rootkit attack with irregular rootkit samples such as, zeroaccess, darkmegi, tdl-4 and xpaj.mbr with each one having different impact on the internal structure of an operating system. Therefore, in this study analysis of rootkits tools were carried out using active detectors tools and malware forensic analysis tools, applying system scanning, network scanning and malware forensic analysis methodology. Altogether the samples rootkit have one or more rootkit detectors to handle their incidence though at a varied performance rate except darkmegi. Though two of the detectors were able to detect its presence on a compromised system, but failed in removal attempt.