# ABSTRACT

*At this paper focus on Malicious Software also known as Malware APT1 (Advance Persistent Threat) codename WEBC2-DIV the most variants malware has criteria consists of Virus, Worm, Trojan, Adware, Spyware, Backdoor either Rootkit. Although, malware could avoidance scanning antivirus but reverse engineering could be know how dangerous malware infect computer client. Lately, malware attack as a form espionage (cyberwar) one of the most topic on security internet, because of has massive impact. Forensic malware becomes indicator successful user to realized about malware infect. This research about reverse engineering. A few steps there are scanning, suspected packet in network and analysis of malware behavior and disassembler body malware.*

*Keyword : forensic malware, analysis, advance persistent threat, cyberwar, disassemble, static analysis, dynamic analysis*