ABSTRACT

Citadel malware is new version of zeus malware, more likely as the impact of noxiousness, stealing personal information for ilegally banking transaction. A malware activities have serious relation with network and computer memory because all of the process happens when computer is connected with each other and on condition. Consequently need certain threat for investigating malware activities, using live forensics technique in digital forensic. The pinciple of Live forensics is capturing digital evidence with all process and activities inside, and happen when computer is on power and connected to the internet access, it is very necessary because the digital evidence data will loss when computer is off condition, so this technique is the right choice for malware forensics. This study aims to achieve a framework of investigation produced by variety of analysis process related with malware using live forensics technique, the process is preservationing and capturing of digital evidence, process analysis, apihooks, registry, dump process, and dump file. This study using volatility as analysis tools running on kali linux machine. The result shown Aan's have a better result as Philip's on malware forensics.

Keyword : *Malware, Citadel, live forensics, digital evidence, malware forensics.*