ABSTRACT

The growing of Information Technology and Communication that more sophisticated is impacted on many security gaps founded. Therefore, memory forensic technic is being developed for doing investigation on the attacked or hacked system. There are two kind of implementation in memory forensic technic, a traditional forensic and live forensic. The application of traditional forensic in this digital era that rapidly increased is considered not effective anymore and that's how the live forensic is used. The investigation using live forensic technic needs a specific handling because the volatile data on the RAM can be disappeared anytime if the investigating system run down.

Live forensic has two methods for the implementing process, internal method (incident response) and external method (capture memory). The internal method is a direct investigation process using a system which is being attacked by the investigator, while the external method is an investigation process which is conducted on the system investigator by doing a dump memory, memory imaging, or memory acquisition previously on the attacked/targeted system, so that the result of memory acquisition file can be transferred on the investigator system.

dumpmemory process is done by support of additional software for doing capture memory. FTK manager is used for doing dumpmemory process on the windows operation system, while the output of dumpmemory process is analyzed using volatility software, bulk extractor, and wireshark.

The results are dumpmemory method successed on doing acquisition toward the random access memory and giving more information in the file image along with analysis result from testing some attacking scenario is generated an authentic evidence and can be accounted for.

Key words : digital forensic, live forensic, RAM, dumpmemory, memory acquisition, memory imaging