Abstract

File Carving is a data recovery technique based on file structure and content without relying on filesystem information or metadata. In the traditional file carving technique, the forensics examiners do the carving manually based on the data obtained. The problem that occurs in the carving process is the fragmented file condition and high false positive values generated during the carving process. This study aims to analyze the file carving method, which is signature based and file based structure as a solution to the problem of the carving process. To find out the results of the method used, the carving file implementation and testing are carried out based on the parameters of recovery performance, execution time, and memory usage. The carving process focuses on image file types in JPEG, PNG and GIF formats. The test results are based on recovery performance parameters, the structure file based method gets a higher value than signature based, whereas the signature based method has an average execution time value faster and the use of resources that are not too large compared to the structure file based method. Besides that the problem of high positive false values can be overcome by the structure file based method.

Keywords: *file carving, signature based, structure file based, recovery performance, execution time, memory usage*