ABSTRACT

Digital device crimes such as information leaks, embezzlement of money from banks and credit card fraud that utilize file modification methods to carry out their actions can have negative impacts that can harm several parties. File signatures or magic numbers are a forensic science technique that helps identify file types. The file identification process is divided into two, namely file identification based on the extension and file identification based on the file signature or magic number. Even though the file extension has been changed, the file signature can still identify the authenticity of the file extension.

This research presents a file signature analyzer as a new website-based approach with high accuracy for automatic file extension identification. The algorithm applied is repetition. The application supports 196 extensions and 268 file signatures. The application's supported extensions are spread across several file types; video, audio, documents, images, letters and electronic books.

Application testing was carried out using two modification methods, namely changing the extension randomly and removing the extension and the results were that the original file was detected correctly (98%) and detected incorrectly (2%), the detected modified file could be returned (95%) and detected, could not be returned (5%).

Keywords –Extension; File; File Signature; Identification; Magic Number.