# Detecting JFIF header using FORHEADER

*Kamaruddin Malik Mohamad, Tutut Herawan, Mustafa Mat Deris*
Faculty of Computer Science and Information Technology Universiti Tun Hussein Onn Malaysia
Faculty of Computer System and Software Engineering, Universiti Malaysia Pahang
{malik,mmustafa}@uthm.edu.my, tutut@ump.edu.my

**ABSTRACT**
Header and footer are important in digital investigation for JPEG file detection as only 16% of files are fragmented. The use of efficient algorithm to detect them is vital to reduce time taken for analyzing ever increasing data in hard drive or physical memory. Even though there are few applications developed for file carving that rely on header and footer e.g. Foremost, Scalpel; however the algorithm used for header detection is not much discussed. In this paper, we introduce three novel algorithms; single-byte-marker, dual-byte-marker and 20-point-reference for JPEG File Interchange Format (JFIF) header detection using a newly introduced FORHEADER model. Three experiments have been carried out using an image from hard disk and physical memory; and raw data from Digital Workshop Forensics Research Workshop 2006 (DFRWS 2006) challenge. The results obtained showed that dualbyte-marker algorithm provides better performance in terms of processing time for JFIF header detection.

**KEYWORDS:**
File Carving, Digital Forensics, JFIF Detection, JPEG

**ACKNOWLEDGEMENT**

This paper is an extension to the papers that have been published in [22] and [23]. We also wish to note that this work was supported by Universiti Tun Hussein Onn Malaysia (UTHM).