ABSTRACT

This research aims to enhance the effectiveness of digital evidence searching in volatile memory, particularly those published on social media forensics. Although a foundational framework in this domain has been established by the previous studies, certain limitations persist, such as the restricted amount of data that are extractable from each social media platform and the potential optimization of string searching using regex. In response to this problem, this study developed an approach to create regular expressions based on social media taxonomy and implemented parallel search algorithms for regex-based searches. This approach was implemented by the "RegTax App", a tool specialized for digital evidence search using regex. Based on the tests conducted in this study, there was an increase in the volume of extractable data and an improvement in the speed of regex-based searching. Furthermore, this study was reported so that it might support forensic activities.

Keywords: memory forensics, social media forensics, regular expression.