Abstract

The impact of electronic technology on society is growing. Along with changes in the paradigm of more modern technology, it can cause a problem. Cybercrime is one of them. In most cases, cybercrime leaves traces of its activities so that they can be used as evidence. Because digital evidence is fragile, improper handling can easily cause it to become contaminated or damaged. To combat cybercrimes, a method that is able to search and locate digital evidence is required, as the aforementioned problems indicate. Observations were made to law enforcers to find out how the stages of handling digital evidence are. Preparation, digital evidence identification and collection, preservation, confirmation, and identification are the stages that the observation results divide into. and the submission of evidence. The method used in this study is the National Institute Of Justice (NIJ). There are five stages in it, namely Identification, Collection, Examination, Analysis and Report. This study uses the scenario of fake news being spread through the WhatsApp app. After scenarios are played out in an Android emulator, data are gathered. The acquired data is created in an image file using the FTK Imager to maintain data integrity. The mounted smartphone directory is analyzed in order to locate the WhatsApp database. The WhatsApp viewer is used to decrypt the encrypted WhatsApp databases msgstore.db.crypt14, key.file, and wa.db. The decrypted database was analyzed manually using DB Browser for SQLite. The result found evidence of communication deployment in the table available_message_view, message_view, message, message_ftsv2, message_ftsv2_content.

Keyword : NIJ, Digital Evidence, Whatsapp, forensic