ABSTRACT

Forensic analysis plays a vital role in addressing cybercrimes within applications. One of the methods employed is the National Institute of Standards and Technology (NIST) method, aimed at evaluating digital evidence within applications used by perpetrators of cybercrimes. The analysis process using the NIST method involves identification, collection, analysis, interpretation, and documentation of digital evidence. Forensic teams utilize specialized software and equipment to access crucial information from digital evidence. The NIST method boasts advantages in standardizing processes, facilitating teamwork among forensic experts, and enhancing analysis quality. It also ensures the integrity of digital evidence for admissibility in court. The results of forensic analysis using the NIST method are crucial in addressing cybercrimes within applications. The structured analysis process guarantees accuracy and validity of digital evidence, serving as a foundation for legal actions against the perpetrators. In an era where technology increasingly permeates various aspects of life, forensic analysis using the NIST method becomes a crucial element in safeguarding digital security and providing robust evidentiary tools in legal proceedings.

Keywords: Forensic analysis, cybercrime handling, WhatsApp, identification, digital evidence.