ABSTRACT

The rapid advancement of information technology has significantly influenced various aspects of human life, including the growing prevalence of cybercrime, particularly through Android-based smartphones. User security and privacy have become critical issues due to the high frequency of mobile device usage in daily activities. This study aims to analyze and investigate digital traces on Android smartphones that are suspected of being involved in cybercrime activities. The research adopts the Integrated Digital Forensic Investigation Framework version 2 (IDFIF v2), which consists of five main phases: Identification, Preservation, Collection, Examination & Analysis, and Presentation.

A case study was conducted on a rooted Android device used to simulate suspicious activities such as illegal data transmission and the installation of malicious applications. The results demonstrate that IDFIF v2 provides a systematic and effective approach to digital forensic investigation, enabling the accurate identification of digital artifacts such as activity logs, hidden files, and application metadata. Furthermore, the analysis revealed patterns of cyberattacks and potential vulnerabilities within the system. This research contributes to the enhancement of mobile device forensic methodologies and serves as a reference for digital law enforcement efforts in Indonesia.

Keywords: Cybercrime, Android, Digital Forensics, IDFIF v2, Investigation, Smartphone

ABSTRAK

Perkembangan teknologi informasi yang pesat telah membawa dampak signifikan terhadap pola kehidupan manusia, termasuk dalam aspek kejahatan digital (cybercrime) yang semakin marak terjadi melalui perangkat smartphone, khususnya berbasis Android. Keamanan dan privasi pengguna menjadi isu krusial mengingat tingginya intensitas penggunaan perangkat mobile dalam aktivitas sehari-hari. Penelitian ini bertujuan untuk menganalisis dan menginvestigasi jejak digital pada perangkat Android yang diduga menjadi sarana atau objek tindak kejahatan siber. Metode yang digunakan adalah Integrated Digital Forensic Investigation Framework v2 (IDFIF v2), yang terdiri dari lima fase utama: Identification, Preservation, Collection, Examination & Analysis, dan Presentation. Melalui pendekatan forensik digital ini, penelitian dilakukan dengan studi kasus pada perangkat Android yang telah dimodifikasi (rooted) dan digunakan untuk simulasi aktivitas mencurigakan, seperti pengiriman data ilegal dan instalasi aplikasi berbahaya.

Hasil dari penelitian menunjukkan bahwa IDFIF v2 mampu memberikan alur kerja sistematis dan efisien dalam proses investigasi, memungkinkan identifikasi artefak digital secara tepat seperti log aktivitas, file tersembunyi, dan metadata aplikasi. Selain itu, hasil analisis juga mampu mengungkap pola-pola serangan siber serta potensi kerentanannya. Penelitian ini memberikan kontribusi terhadap penguatan metode investigasi digital pada perangkat mobile dan dapat menjadi referensi dalam proses penegakan hukum digital di Indonesia.

Kata kunci: Cybercrime, Android, Digital Forensic, IDFIF v2, Investigasi, Smartphone