Abstrak

Jailbreak memiliki masalah dalam perubahan data, karena memodifikasi file di perangkat untuk memungkinkan pengguna mengekstrak lebih banyak data daripada tanpa jailbreak. Masalah ini menimbulkan kontroversi penggunaan jailbreak dalam investigasi digital forensik, karena integritas data merupakan persyaratan utama dalam proses pengadilan. Penelitian ini bertujuan untuk menganalisis proses jailbreak, apa yang sebenarnya dilakukan oleh kode jailbreak di perangkat, dan data apa yang sebenarnya dimodifikasi oleh kode jailbreak. Dengan menggunakan versi terbaru sistem iOS, penelitian ini menggunakan exploit voucher_swap sebagai representasi dari metode jailbreak semi-tethered untuk menyelidiki efek jailbreak pada integritas data pada sebuah idevice. Penyelidikan dilakukan berdasarkan sejauh mana data dapat diekstraksi dari perangkat jailbreak, perbandingan nilai hash data, dan analisis kode untuk meneliti efek jailbreak terhadap sistem dan data pengguna di dalam perangkat. Hasil penelitian ini menunjukkan bahwa jailbreak dapat diterima untuk mempersiapkan idevice dalam investigasi forensik digital untuk memperoleh lebih banyak data, karena menjaga integritas data pengguna. Hasil ini dapat membantu komunitas forensik, khususnya para penyelidik dalam keputusan mereka tentang penerimaan terhadap penjatuhan hukuman dalam penyelidikan forensik pada idevide.

Kata Kunci: digital forensik, iOS, iPhone, jailbreak, root privilege