Analisis Perbandingan Hasil Akuisisi Forensik Mobile Pada Perangkat iOS Terkunci After First Unlock dan Before First Unlock = Comparative Analysis of Forensic Extraction Results of Locked iOS Devices: After First Unlock and Before First Unlock States

Adly Gilang Kurnia, author

Abstrak

Secara global, perangkat Apple terutama iOS memiliki 24.7% smartphone market share. Hal ini reputasi perangkat iOS menjadi perangkat paling aman dibandingkan Android. Hal ini seiring dengan barang bukti yang dominan dalam kasus forensik digital. Tantangan yang dihadapi oleh pemeriksa forensik pada perangkat iOS adalah bagaimana mendapatkan akses kedalam perangkat tersebut. Perangkat iOS yang terkunci memiliki dua kondisi yang berbeda, yaitu After First Unlock (AFU) dan Before First Unlock (BFU). Oleh karena itu diperlukan suatu penelitian untuk mengetahui informasi apa saja yang dapat diperoleh pada perangkat iOS yang terkunci. Penelitian ini bertujuan untuk melakukan akusisi dan analisa terhadap kondisi perangkat terkunci tersebut. Perangkat yang digunakan pada penelitian ini menggunakan iPhone 11 dengan iOS versi 17.4.1 dan menggunakan tools Cellebrite UFED Premium untuk melakukan akuisisi. Hasil akuisisi dari perangkat tersebut didapatkan informasi bahwa pada kondisi BFU jumlah data yang dapat dipulihkan sekitar 61.31% dan pada kondisi AFU sekitar 97.45% dibandingkan dengan akuisisi Full File System (FFS). Pemeriksaan nilai hash menunjukkan integritas data yang sangat baik, yaitu pada BFU 98.57% dan AFU 89.84% memiliki nilai hash yang sama terhadap akuisisi FFS. Hasil dari tahapan pengujian dan analisis dibuatkan alur instruksi kerja yang diharapkan menjadi referensi.
.....Globally, Apple devices, particularly iOS with a 24.7% smartphone market share, are increasingly encountered as digital forensic evidence. The rank is probably affected by iOS reputation that is the most secure mobile device. This aligns with the dominance of such devices as evidence. A key challenge for forensic examiners with iOS devices is gaining access to them. Locked iOS devices come in two distinct states: After First Unlock (AFU) and Before First Unlock (BFU). Therefore, research is needed to determine the information recoverable from locked iOS devices. This study aims to acquire and analyze data from such locked devices in both AFU and BFU states. An iPhone 11 running iOS 17.4.1 was used for the study, and Cellebrite UFED Premium was employed for data acquisition. The data acquisition process yielded 61.31% files from the BFU device and 97.45% files from the AFU device compared to Full File System (FFS) acquisition result. Hash value verification indicated excellent data integrity, with 98.57% and 89.84% of files in BFU and AFU devices, respectively, matching the hash values obtained from the FFS acquisition. A work instruction flow was made from the examination and analysis results that is expected to be a reference.