Abstract

Jailbreak has an issue in data alteration, as it modifies file(s) in the device to allow user to extract more data than without jailbreaking. This issue raises controversy of the use of jailbreaking in digital forensic investigation, as data integrity is a prominent requirement in a court proceeding. This study aims to analyze the process of jailbreak, what is actually done by the jailbreak code in a device, and what data is actually modified by the jailbreak code. By using the latest version of iOS system, this study uses the voucher_swap exploit as a representation of semi-tethered jailbreaking method to investigate the effects of jailbreak on data integrity on a idevice. The investigation is conducted based on to what extent data can be extracted from the jailbreak device, hash value comparison of the data, and source code analysis to scrutinize the effect of jailbreak to the system and user data inside the device. Results of this study suggest that jailbreak is acceptable to prepare idevice in digital forensic investigations to acquire more data, as it maintains the integrity of user data. These results may help forensic communities, especially investigators in their decision about the acceptability of jailbreaking in idevide forensic investigations.

Keywords: digital forensics, iOS, iPhone, jailbreak, root privilege