I. INTRODUCTION

IOS was first introduced in 2007 on an iPhone device [1]. The iOS was developed by the Apple Machintosh Team, which is officially called the iPhone OS. Then it was changed to iOS in 2010. iOS can be used on iPhone, iPad and iPod Touch devices. iOS has been going on for eleven years and has undergone changes and increased security since it was first launched [2]. At the time of writing this paper, iOS 12.3 is the latest stable version that can be used.

Jailbreak has an issue in data alteration. It somehow needs to modify files in the device in order to extract more data. This file modification raises concern of data integrity as the prominent consideration in forensics examination. We need to maintain the data integrity that is required by the court proceeding, by conducting data extraction in a forensically sound manner. However, as in contrast, one proprietary forensic tool states that jailbreaking is necessary to perform physical acquisition stage in order to do file system extraction and keychain decryption, for 64-Bit iOS [3]. Without jailbreaking, the tools can only support logical acquisition that limit data extraction only on idevice information, iTunes format backup, list of installed apps, media and shared files [4]. The pros and cons of data integrity issue in a jailbreaking device makes the use of this method in forensic examination is needed to be examined further, as it may influence the acceptability of digital data in a court of law.

However, despite of this importance issue of data modification in jailbreak, there are a few studies that investigate to what extent jailbreaking modify the data, either system data or user data. Previous investigation on the controversy of jailbreaking, in 2015, clarifies that this procedure will not change the internal digital evidences of iPhone [5]. As iOS operating system and jailbreaking tools developed, we need to keep up to date to analyze the process of jailbreak, what is actually done by the jailbreak code in a device, and what data is actually modified that may raise concern in data integrity.

Therefore, this study aims to scrutinize the jailbreak impact to the latest version of iOS device in data integrity, by conducting a digital forensic analysis particularly in iOS device as it is known as a device that has taken care of users privacy and security on the top level of its architecture that may complicate the data extraction process. Results of this research can be used as a basis by investigator, to decide whether the jailbreak can be accepted or not by the forensic community to conduct an investigation on iOS.

In section I of paper contains the background of digital forensic on the idevice jailbreak. In section II explain the jailbreak process on iOS and literature review. In section III explain the design of a digital forensic test is done on the idevice, including in the form of flow testing as well as equipment needed for the test. Then in section IV described in detail the results and discussion. Finally, in section V the conclusions were given.