by S N

Submission date: 27-Jun-2021 10:29AM (UTC-0500)
Submission ID: 1612761768
File name: ensic_Hardware_and_Software_for_Apple_Devices.edited.edited.docx (17.98K)
Word count: 626
Character count: 3332

Forensic Hardware and Software for Apple Devices

Name

Institution

Course

Instructor

Date

Forensic Hardware and Software for Apple Devices

It is incredible how with Apple technology, software and hardware, forensic has been revolutionized where Apple has platforms serving mobile computations. These platforms include the iPhone, iPod, and iPad. They are the most used platforms of Apple in the modern world. Specifically, their forensic interest stems from their high rate of adoption and potentiality to contain digital evidence.

Additionally, the Apple platforms have similar designs alongside the operating system (iOS), which necessitate sharing the methods and forensic tools across the product types (Xing et al., 2018). An iOS is an operating system that is uniquely used in Apple's products. It is a version of the OS X operating system that the Apple computers use. Some of the digital forensic tools unique to the Apple platforms include iTunes, which provides the backing up by the device, commercial software tools, and modernized methodologies grounded on jailbreaking functionality thanks to Apple technology (Hay et al., 2017).

There are differences in procedures and acquisition methods for both iOS and OS X operating systems. In the field of Apple forensics, there are four types through which data is extracted. One of such methods is logical extraction. This method can only hold such types of data as calls, contacts and SMS. In most cases, the acquisition is achieved through the installation of special software on a mobile device. However, this method does not hold in this case because the Apple devices have varied data organization. The second method is the creation of a backup replica. This means the acquisition of data whose storage is the device's memory and can be extracted through security regulations terms. Besides, this method is the widespread one in Apple devices. The third method is creating a physical bump which entails the extraction of logical data from a mobile device (Hoog & Strzempka, 2018). Again, it applies to all Apple

devices. Lastly, there is the creation of a physical dump that encompasses the acquisition of logical and deleted data. This method can, however, only be used by the iPhone 4 users and the latest models. It is worth mentioning that the Belkasoft acquisition tool is also helpful in extracting data from a blocked Apple gadget and making iPhone forensic images.

Although there are currently several tools for Apple platforms regarding digital forensic lab, I would recommend the digital forensic lab use the iOS software development kit (SDK). Most interesting are some of the essentials found in the iOS (SDK) which include the gamekit tool, UIkit, Pushkit, Mapkit, and Foundation Kit. Another tool that I would recommend the digital forensic lab to use is the Xcode (Hoog & Strzempka, 2018). Mostly, it is appropriate for iOS and Mac apps. One can use the interface in writing iOS applications. In addition, this tool comprises tools, frameworks, and compilers in developing, designing, writing a code and debugging an iOS app. The Xcode is recommended because of its speed and consistency of smoothness in developing an app. Thus, through these tools, the digital forensic lab would make building software easier.

References

Hay, A., Krill, D., Kuhar, B., & Peterson, G. (2017, January). Evaluating digital forensic options for the Apple iPad. In *IFIP International Conference on Digital Forensics* (pp. 257-273). Springer, Berlin, Heidelberg.

Hoog, A., & Strzempka, K. (2018). *iPhone and iOS forensics: Investigation, analysis, and mobile security for Apple iPhone, iPad, and iOS devices*. Elsevier.

Xing, L., Bai, X., Li, T., Wang, X., Chen, K., Liao, X., ... & Han, X. (2018, October). Cracking App Isolation on Apple: Unauthorized Cross-App Resource Access on MAC OS~ X and iOS. In *Proceedings of the 22nd ACM SIGSAC Conference on Computer and Communications Security* (pp. 31-43).

I

ORIGINALITY REPORT

0%	0%	0%	0%
SIMILARITY INDEX	INTERNET SOURCES	PUBLICATIONS	STUDENT PAPERS

PRIMARY SOURCES

Exclude quotes	Off	Exclude matches	Off
Exclude bibliography	On		