B12 A Digital Forensic Analysis on the iCloud® and Its Synchronization to Apple® Devices

Rachel Friedman, BS, 8804 Cold Spring Rd, Potomac, MD 20854; and Joshua L. Brunty, MS, and Terry Fenger, PhD, 1401 Forensic Science Dr, Huntington, WV 25701*

After attending this presentation, attendees will know what iCloud® artifacts can be found on the iPod Touch 4G® and the MacBook Pro®. Additionally, the audience will learn one way to determine if two Apple devices are synced together through the iCloud®.

This presentation will impact the forensic science community by showing preliminary steps of how to capture artifacts from iCloud®-enabled devices.

In October 2011, Steve Jobs introduced the iCloud® to Apple customers.[1] The iCloud® was a service that allowed Apple device users to sync various applications to remote servers and access the data from each of their Apple products.[2] The study of cloud computing services, like the iCloud®, is a burgeoning area of research for the digital forensic community. The goal of this project was to show artifacts that confirmed iCloud® activation. Since the iCloud® is not a physical device that an investigator can seize, it is important for forensic examiners to know how to determine if a device is iCloud®-enabled.[3] Additionally, if multiple devices were connected to the iCloud®, there could have been residual artifacts that showed a link between the devices.

The iPod Touch® and MacBook Pro® were tested because their operating systems, iOS 5.0.1 and Mac OS X 10.7 Lion, respectively, were equipped to utilize the iCloud®, and were supported by current forensic tools. Three images were taken of the iPod Touch®: (1) before iTunes and iCloud® activation; (2) after iTunes and before iCloud® activation; and, (3) after iTunes and iCloud® activation. Two images were made of the MacBook's® solid state drive: before and after iCloud® activation. A comparison and analysis of the images were then performed to identify artifacts resulting from the enabling and use of the iCloud®.

On the iPod Touch® and MacBook Pro®, property lists (plists) differed between images created both before and after enabling the iCloud®. Certain dates and key values that were found to support the iCloud® were enabled on the iPod Touch® and MacBook Pro®. However, little evidence was found to show both devices were clearly connected to each other via iCloud®. The evidence that was identified came from the synced applications that were linked to the iCloud®. Data from certain applications were displayed on both devices, which supported the theory that the data was synchronized.

Therefore, it is possible to obtain iCloud® information from the local drives of iDevices. Further research must be done to determine the synchronization of information to and from the iCloud®. A subsequent step to take would be to attempt to monitor iCloud® traffic between Apple devices. Also, a protocol should be written on a standard way to capture the iCloud®, as well as create live image tools.

References:

1. Bosker, B. Apple Announces iCloud, iTunes Match At WWDC 2011. Huffington Post [Internet]. 2011 [cited 2012 July 25] Available from: http://www.huffingtonpost.com/2011/06/06/apple-announces- icloud-wwdc-2011_n_871885.html
2. Rounak. The Complete iCloud Guide. iPhone Hacks [Internet]. 2011 [cited 2012 July 25]. Available from: http://www.iphonehacks.com/2011/10/the-complete-icloud- guide.html
3. Straw, T. Cloud Computing & Its Effects on Digital Forensics. Digital Flatfoot [Internet]. 2011 [cited on 2012 July 25]. Available from: http://www.digitalflatfoot.com/cloud-computing-its-effects-on- digital-forensics

iCloud®, Apple®, Synchronization

 ** Presenting Author*