A Digital Forensic Analysis on the iCloud® and its Synchronization to Apple® Devices
Rachel Friedman, BS, Josh Brunty, MS, Terry Fenger, PhD
Marshall University Forensic Science Center, 1401 Forensic Science Drive, Huntington, WV 25701

Abstract
Apple’s iCloud is a popular application on supported Apple devices. Little is known about how to obtain data from iCloud. If an image can be acquired from an Apple device, then there should be artifacts that show iCloud was enabled. Images were taken of the iPod Touch 4G and the MacBook Pro, before and after iCloud was enabled. The before and after images were compared to one another. Both iCloud images of the iPod and the MacBook contained property lists representing iCloud enabled devices. However, no artifacts were found showing the two devices were synced to each other. This information will provide preliminary evidence about how iCloud syncs to Apple devices and what evidence it stores on them.

Introduction
In October 2011, Apple joined its corporate rivals and introduced iCloud, a cloud computing service that is included in the latest Apple operating systems.1 iCloud’s features include storing iTunes on iCloud, backing up emails, contacts, and calendars, and sharing photos through PhotoStream. iCloud also offers wireless backups of Apple devices. Additionally, iCloud syncs other devices together. As long as an iPhone product is running operating system iOS 5, OS X Lion, or higher, it is able to synchronize to another device via-Cloud. For example, if a document is created on an iPad, it is accessible on the user’s MacBook. Today, more than 150 million people are using iCloud on multiple devices.2

The purpose of the Cloud analysis reported in this study is to determine if there are artifacts that confirm iCloud has been activated on Apple devices. This iCloud research is pertinent to both the public and private writing of digital forensics. For example, law enforcement can implement this research during a search and seizure. If an Apple device with Cloud capabilities displays that it is connected to an iCloud account, the examiner has probable cause to acquire Cloud as evidence. Private organizations are interested in this information, for example, to create a timeline of events that occur on an Apple device. The Apple devices tested in this experiment are the iPod Touch 4G and the MacBook Pro because their operating systems are capable of using Cloud. It is expected that there will be artifacts that show Cloud activation on both devices.

Materials
Tested Devices
- iPod Touch 4G running iOS 5 (5.0.1)
- MacBook Pro running Mac OS X10.7.3

Acquisition Software
- CellFINDER Physical Analyzer (3.0.1.189)
- Katanalabs’ Xentum 2.3.1.1

Acquisition Software for MacBook
- FTK Image (3.0.0.493)

Analysis Software
- Forensic Toolkit 3.4 (2.4.1.3499)

Methods
Task baseline image of MacBook’s hard drive
- Activated iPad using iTunes on MacBook
- Task baseline image of iPod with Cellulite and Lantern software
- Created Apple ID account and activated iCloud on MacBook
- Activated iCloud on iPod
- Utilized iCloud applications on iPod
- Added an Contact
- Added an event to Calendar
- Downloaded Feed My Apps application to home screen
- Task image of iPod with Cellulite and Lantern software
- Task image of MacBook
- Compared all images using FTK

References

Discussion
Artifacts were found that showed iCloud was enabled on both devices. Multiple pilots recognized that iCloud was activated on the iPod and the MacBook. There was little evidence showing the two devices were connected to each other through iCloud. Instead, artifacts were found on each device that shared the same data through the iCloud syndr applications.

Future experiments would include obtaining memory from the devices and running packet sniffers to see the traffic the devices are sending over the internet. Ultimately, the results and upcoming research can be combined to create a preliminary protocol on how to acquire evidence from iCloud.

Acknowledgments
The authors thank Joshua Shomo, Thomas Harris-Warrick, and Jessica Smith, MPS, for supporting this research project in its entirety. Also, Struck Forensic LLC is acknowledged for providing the software and space to conduct the project.

This project was funded by the National Institute of Justice award 2010-IJ-CX-00.