## C9 Apple® iCloud® Message Sync Forensic Investigations and Artifacts

*Andrew N. Crouse, BA*, Epiq Systems, Inc, Washington, DC 20006; Kaylee A. Schoepe, BS*, Huntington, WV 25701; Brian Smith, BS, Epiq Systems, Inc, Atlanta, GA 85034; Wesley Wong, BA, Epiq Systems, Inc, Los Angeles, CA 90071*

**Learning Overview:** After attending this presentation, attendees will better understand Apple's® iCloud® Message Sync functionality and its impact on Apple® device forensic examinations of property lists and SQLite databases. Studies of relevant artifacts will be discussed and the changes observed when different user actions occur on an iOS® device in regard to native text messaging and message synchronization to the Apple® iCloud®.

**Impact on the Forensic Science Community:** This presentation will impact the forensic science community by presenting Apple® iOS® artifact differences relating to user activity surrounding Apple's® iCloud® Message Sync functionality and usage on iOS® devices.

Apple® iCloud® Message Sync has introduced a natively new way for users to sync and store Apple® iMessages®, Short Message Service (SMS), and Multimedia Messaging Service (MMS) (native Apple®) messages. Prior to the introduction of iCloud® Message Sync, an examiner would expect the native Apple® messages to be extracted through an iTunes® backup or using a variety of third-party forensic tools. With the new option for users to store native Apple® messages in their iCloud® account, Apple® no longer needed to include messages in iTunes® and iCloud® backups for disaster recovery or "new device data transfer" purposes.[1] Due to forensic methods and tools relying on iTunes® and iCloud® backup technology to perform extractions, this presented an issue whereby data could potentially be overlooked. This presentation will discuss the forensic analysis of iCloud® message sync artifacts on Apple® iOS® devices that would be potentially relevant to findings in both civil and criminal cases.

Mobile devices, particularly Apple® iOS® devices, have become a common occurrence in both the worlds of digital forensics and e-discovery. Obtaining data from these devices is critical, and oftentimes text messages, such as iMessages®, SMS messages, and MMS messages, contain valuable information relevant to cases. Text messages are typically extracted from Apple® mobile devices through two methods: (1) direct-device collections using a forensic tool or Apple® iTunes®; and (2) analysis of Apple® iTunes® backup files stored via backups to either a local computer or the Apple® iCloud®. In researching these methods, the native Apple® messaging database (sms.db) was collected and parsed by the examiner's tool of choice.

Apple® iCloud® storage services allow users to sync and store data, such as photos, contacts, notes, keychain information, health data, map data, reminders, and more, in their online account. In 2018, Apple® released an iCloud® service called Apple® iCloud® Message Sync, which allowed native Apple® text messages to be stored in a user's iCloud® account and synced to all Apple® iDevices® connected to that iCloud® account.[2] The synchronization of this data from a local device to a user's iCloud® account is controlled from options in the settings of the device. Some of this data, such as photos, notes, and reminders, are set up to sync by default once iCloud® is initially turned on; however, Apple® iCloud® Message Sync data is not turned on by default and must be manually turned on by the user.

The addition of this iCloud® Message Sync service to Apple® devices complicated standard Apple® device collections when native messaging needed to be analyzed. The utilization of iCloud® Message Sync on an Apple® mobile device can lead to the possibility of some data being stored on both the iCloud® and the device or only in the iCloud®. Additionally, when a user has enabled iCloud® Message Sync, traditional iCloud® backups may not contain native Apple® text messages when collected with third-party forensic tools.

Through research, it was able to be determined that the above can affect the conclusions digital examiners make upon collecting text messages from a device. The enabling of the Apple® iCloud® Message Sync option on the device does make changes to both the sms.db database and property list (.plist) files on the device. If examiners do not observe specific data, they may incorrectly conclude it does not exist, when in reality it may be stored solely in the iCloud®.

This presentation will focus on a comparison of Apple® iOS® artifacts to show where examiners can find evidence of iCloud® Message Sync activity. Studies of devices with and without iCloud® message sync turned on will be analyzed and compared, as well as time stamp variances in the sms.db database that may reflect the originating device when multiple iOS® mobile devices are logged into the same iCloud® account. Additionally, a comparison of identified artifact differences in the sms.db tables and property list files will be presented.

**Reference(s):**

1. Apple® Support. (2019, July 30). *iCloud: Store Messages in iCloud*. Retrieved from Apple Support: https://support.apple.com/kb/PH26887?locale=en_US.
2. Cross, J. (2018, June 01). *How to enable Messages in iCloud on your iPhone, iPad, and Mac*. Retrieved from Macworld: https://www.macworld.com/article/3276353/how-to-enable-messages-in-icloud-on-iphone-ipad-mac.html.





*Presenting Author