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 that supported iCloud being enabled. 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

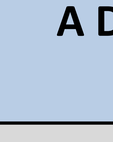
In October 2011, Apple joined its corporate rivals and introduced iCloud, a cloud computing service that is included in the latest Apple operating systems.[1] iCloud's features include storing iTunes in iCloud, backing up mail, contacts, and calendars, and sharing photos through Photostream. iCloud also offers wireless backup of Apple devices. Additionally, iCloud syncs other devices together. As long as an Apple product is running operating system iOS 5, OS X Lion, or higher, it is able to synchronize to another device via iCloud. 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 iCloud 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 sectors of digital forensics. For example, law enforcement can implement this research during a search and seizure. If an Apple device with iCloud capabilities displays that it is connected to an iCloud account, the examiner has probable cause to acquire iCloud 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 iCloud. It is expected that there will be artifacts that show iCloud activation on both devices.

Materials

Tested Devices
- iPod Touch 4G running iOS 5 (5.0.1)
- MacBook Pro running Mac OS X (10.7.3)

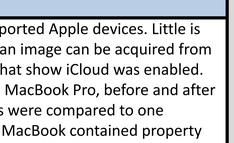
Acquisition Software for iPod
- Cellebrite UFED Physical Analyzer (3.0.0.189)
- Katana Forensics' Lantern 2 (2.3.1)



http://www.everymac.com/systems/apple/ipod/specs/ipod-touch-2g-specs.html

Acquisition Software for MacBook
- FTK Imager (3.0.01443)

Analysis Software
- Forensic Toolkit 3.4 (3.4.1.34295)



http://www.amazon.com/Apple-MacBook-MC700LL-13-3-inch-VERSION/dp/B002QQ8HB

Methods

Took baseline image of MacBook's hard drive
Activated iPod using iTunes on MacBook
Took baseline image of iPod with Cellebrite and Lantern software
Created Apple ID account and activated iCloud on MacBook
Activated iCloud on iPod
Utilized iCloud applications on iPod
- Added 1 Contact
- Added an event to Calendar
- Downloaded Find My Friends application to home screen

Took image of iPod with Cellebrite and Lantern software
Took image of MacBook
Compared all images using FTK

References

Rounak. The Complete iCloud Guide. iPhone Hacks [Internet]. 2011 [cited 2012 June 26]. Available from: http://www.iphonehacks.com/2011/10/the-complete-icloud-guide.html

Panzarino, M. Apple reports 25M user growth for iCloud since April, now at 150M users. The Next Web1 [Internet]. 2012 [cited 2012 July 30]. Available from: http://thenextweb.com/apple/2012/07/24/apple-reports-25m-user-growth-for-icloud-since-april-now-at-150m-users/

Straw T. Apple Pie in the Sky: implications of the iCloud network to digital forensics. Digital Flatfoot [Internet]. 2011 [cited 2012 June 26]. Available from: http://www.digitalflatfoot.com/apple-pie-in-the-sky-implications-of-the-icloud-network-to-digital-forensics-2

Straw T. Cloud Computing and Its Effects on Digital Forensics. Digital Flatfoot [Internet]. 2011 [cited 2012 June 26]. Available from: http://www.digitalflatfoot.com/cloud-computing-its-effects-on-digital-forensics

iCloud-disabled iPod vs. iCloud-enabled iPod Results

Figure 1. Apple ID Authentication Info plist from iCloud-disabled iPod

Key	Value Type	Value
Property list	Dictionary	(6 values)
Accounts	Dictionary	(0 values)
CreationDate	Date (GMT)	2012-02-22T08:03:43Z
Version	Number	100
AccessorVersions	Array	(1 values)
[0]	Number	487.19999999999999
AuthCertificates	Dictionary	(0 values)
MetaInfo	Dictionary	(0 values)

Figure 2. Apple ID Authentication Info plist from iCloud-enabled iPod

Key	Value Type	Value
Property list	Dictionary	(6 values)
MetaInfo	Dictionary	(2 values)
LastSuccessfulConnect	Date (GMT)	2012-06-27T13:40:40Z
LastConnectAttempt	Date (GMT)	2012-06-27T13:40:40Z
CreationDate	Date (GMT)	2012-02-22T08:03:43Z
CertificateToken	String	3101242549--3139333431303530333O
CreationDate	Date (GMT)	2012-06-27T13:40:40Z
ValidationDate	Date (GMT)	2012-06-27T13:40:40Z
Dirty	Boolean	False
AppleID	String	john.marshallfs@me.com
HashedPasswordRef	Binary Data	(offset: 0x2ab length: c bytes)
AuthCertificates	Dictionary	(0 values)

Figure 3. data_ark plist from iCloud-disabled iPod

-ProtocolVersion	String	2
com.apple.MobileDeviceCrashCopy-ShouldSubmitVersion	Number	1
com.apple.mobile.backup-CloudBackupEnabled	Boolean	False
com.apple.mobile.restriction-ProhibitAppInstall	Boolean	False
com.apple.purplebuddy-SetupState	String	SetupUsingAssistant
com.apple.mobile.chaperone.NotSoFresh	Boolean	True

Figure 4. data_ark plist from iCloud-enabled iPod

com.apple.itunesstored-AccountSocialEnabled	Boolean	False
com.apple.mobile.iTunes.store-Storefront	String	143441-1,12
com.apple.mobile.backup-CloudBackupEnabled	Boolean	True
com.apple.mobile.data_sync-Calendars	Dictionary	(2 values)
Sources	Array	(1 values)
[0]	String	iCloud

iCloud-enabled iPod vs. iCloud-enabled MacBook Results

Figure 8. Calendar event from iPod

Key	Value
ROWID	1
SUMMARY	Birthday Cupcakes!
START DATE	362518200
START TZ	America/New_York
END DATE	36251800
LAST MODIFIED	362498692.9
EXTERNAL ID	http://john.marshallfs%40me.com@p09-caldav.icloud.com/443;1934105030/calendars/work/DA873387-8660-4522-9740-972F1F665451.ics
EXTERNAL MOD TAG	"C=8@U=297790a7-741a-4b84-825a-c350998549c1"
UNIQUE IDENTIFIER	DA873387-8660-4522-9740-972F1F665451
UUID	C3788A86-684A-4936-B52D-5ACC47E4D776
CREATION DATE	362498692.9

Figure 9. Calendar event from iPod

Key	Value
BEGIN	VCALENDAR
VERSION	2.0
PRODID	-//Apple Inc.//iCal 5.0.2//EN
CALSCALE	GREGORIAN
BEGIN	VEVENT
DTEND;TZID	America/New_York:20120627T163000
TRANSP	OPAQUE
UID	DA873387-8660-4522-9740-973F1F665451
DTSTAMP	20120627T140459Z
LOCATION	SF
X-APPLE-SCHEDULETAG	
XAPPLE-SERVERFILENAME	DA873387-8660-4522-9740-973F1F665451
SEQUENCE	0
X-APPLE-EWS-BUSYSTATUS	BUSY
SUMMARY	Birthday Cupcakes!
LAST-MODIFIED	20120627T140452Z
DTSTART;TZID	America/New_York:20120627T153000
CREATED	20120627T140452Z
X-APPLE-ETAG	C=8@U=297790a7-741a-4b84-825a-c350998549c1
END	VEVENT
END	VCALENDAR

Figure 10. Calendar List from iPod

https://john.marshallfs%40me.com@p09-caldav.icloud.com:443/1934105030/calendars/work/	C1BF
https://john.marshallfs%40me.com@p09-caldav.icloud.com:443/1934105030/calendars/home/	AB81
https://john.marshallfs%40me.com@p09-caldav.icloud.com:443/1934105030/calendars/tasks/	B180
https://john.marshallfs%40me.com@p09-caldav.icloud.com:443/1934105030/calendars/inbox/	03A4

Figure 11. Calendar List from MacBook

Key	Value Type	Value
Property list	Dictionary	(19 values)
AlarmsDisabled	Boolean	False
Availability	Boolean	True
CalendarPath	String	/1934105030/calendars/work/
Checked	Number	1
Color	String	#711A76FF

Key	Value Type	Value
Property list	Dictionary	(20 values)
AlarmsDisabled	Boolean	False
Availability	Boolean	True
CTag	String	FT=:@RU=297790a7-741a-4b84-825a-c350998549c1@S=3
CalendarPath	String	/1934105030/calendars/home/
Checked	Number	1
Color	String	#0E61B9FF

Key	Value Type	Value
Property list	Dictionary	(20 values)
AlarmsDisabled	Boolean	False
Availability	Boolean	True
CTag	String	FT=:@RU=297790a7-741a-4b84-825a-c350998549c1@S=5
CalendarPath	String	/1934105030/calendars/tasks/
Checked	Number	1
Color	String	#F64F00FF

Figure 12. Contacts from iPod

ExternalIdentifier
https://john.marshallfs%40me.com@p09-contacts.icloud.com/1934105030/carddavhome/card/MmI2OWI0ZDctNmVjNC00OGUwLWE1YWMtMTU4NDA3MmUxMzg4.vcf
https://john.marshallfs%40me.com@p09-contacts.icloud.com/1934105030/carddavhome/card/MmFiOWI4MzMtYTNhMS00ODI2LWI4NjYtMzk5ZjQ1MmNjYjhm.vcf
https://john.marshallfs%40me.com@p09-contacts.icloud.com/1934105030/carddavhome/card/NzU5YzQxYTUtMjZiYy00Njc1LWIxNDUtMWI5ZjAzZjc1Nm11.vcf
https://john.marshallfs%40me.com@p09-contacts.icloud.com/1934105030/carddavhome/card/AF168C47-359F-4EF6-A4A1-7C752E85309C.vcf

Figure 13. Contacts from MacBook

Key	Value Type	Value
Property list	Dictionary	(15 values)
com.apple.carddavvcf	String	MmI2OWI0ZDctNmVjNC00OGUwLWE1YWMtMTU4NDA3MmUxMzg4.vcf
Organization	String	Apple Inc.
UID	String	392524F3-6DF6-42ED-9060-B4838B277590:ABPerson
com.apple.synced	String	1
com.apple.vcardhash	String	da0bab3893013a1edfd571023cdab2f
Creation	Date (GMT)	2012-06-27T13:18:52Z

Key	Value Type	Value
Property list	Dictionary	(12 values)
com.apple.carddavvcf	String	MmFiOWI4MzMtYTNhMS00ODI2LWI4NjYtMzk5ZjQ1MmNjYjhm.vcf
com.apple.uuid	String	2ab9b833-a3a1-4826-b866-399f452ccb8f
UID	String	710925C2-B51A-408F-8249-B652E272A63A:ABPerson
com.apple.synced	String	1
First	String	AlsoMISDE
Creation	Date (GMT)	2012-06-27T13:18:52Z

Key	Value Type	Value
Property list	Dictionary	(15 values)
com.apple.carddavvcf	String	NzU5YzQxYTUtMjZiYy00Njc1LWIxNDUtMWI5ZjAzZjc1Nm11.vcf
Organization	String	Apple Inc.
UID	String	91B37D55-E914-47B9-8787-8907A8FD5F52:ABPerson
com.apple.synced	String	1
com.apple.vcardhash	String	91b0fc101a9bf549bc2c4307cf6b21e5
Creation	Date (GMT)	2012-06-27T13:18:52Z

iCloud-disabled MacBook vs. iCloud-enabled MacBook Results

Figure 5. Apple ID Authentication Info plist from iCloud-disabled MacBook

Key	Value Type	Value
Property list	Dictionary	(3 values)
Version	Number	100
CreationDate	Date (GMT)	2012-05-04T14:44:09Z
AccessorVersions	Array	(1 values)
[0]	Number	478.29000000000002

Figure 6. Apple ID Authentication Info plist from iCloud-enabled MacBook

Accounts	Dictionary	(1 values)
john.marshallfs@me.com	Dictionary	(12 values)
HashedPasswordRef	Binary Data	(offset: 0x18c length: 94 bytes)
CreationDate	Date (GMT)	2012-06-27T13:16:00Z
CertificateToken	String	3101221931--3139333431303530333O
CertificatePrivateKeyReference	Binary Data	(offset: 0x24f length: d6 bytes)
ModificationDate	Date (GMT)	2012-06-27T13:16:07Z
AppleID	String	john.marshallfs@me.com
encDsId	String	314d4e784c515a68304e2f453341346b34636e3446773d3d
LastConnectAttempt	Date (GMT)	2012-06-27T13:16:05Z
LastSuccessfulConnect	Date (GMT)	2012-06-27T13:16:05Z
NextCertificateFetchDelta	Number	300
NextCertificateFetchDate	Date (GMT)	2012-06-27T13:21:04Z
CSRCreationDate	Date (GMT)	2012-06-27T13:16:02Z
AccessorVersions	Array	(1 values)
[0]	Number	478.29000000000002
CreationDate	Date (GMT)	2012-05-04T14:44:09Z

Figure 7. AOS Notification plist from iCloud-enabled MacBook

Key	Value Type	Value
Property list	Dictionary	(1 values)
InternalAccounts	Array	(1 values)
[0]	Dictionary	(6 values)
username	String	john.marshallFS@me.com
userInfo	Dictionary	(1 values)
InUseOwnerDisplayName	String	John Marshall
userid	Number	501
enabledDataclasses	Array	(1 values)
[0]	String	com.apple.Dataclass.DeviceLocator
dataclassProperties	Dictionary	(1 values)
com.apple.Dataclass.DeviceLocator	Dictionary	(4 values)
apsEnv	String	Production
hostname	String	p09-fmip.icloud.com
authMechanism	String	token
scheme	String	https
personID	String	1934105030

Discussion

Artifacts were found that showed iCloud was enabled on both devices. Multiple plists 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-synced applications.

Future experiments would include obtaining memory from the devices and running packet sniffers to see the traffic between the devices. 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, MFS, for supporting this research project in its entirety. Also, Stroz Friedberg LLC is acknowledged for providing the software and space to conduct the project.

This project was funded by National Institute of Justice award 2010-IJ-CX-K0.