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 was 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

A revolutionary computing tool of this decade is cloud computing. According to National Institute of Standards and Technology (NIST), cloud computing is defined as "a model of enabling convenient, on-demand network access to a shared pool of configurable resources that can be rapidly provisioned and release with minimal management effort or service provider interaction."[12] In simpler terms, it is a remote service that allows multiple users to access information using multiple devices.

Cloud computing is unique because of five significant characteristics. First, it is a pay-as-you-go service, meaning a customer can rent out cloud space for as long as they need it.[2] The cloud is elastic which allows the customer to expand or reduce the amount of cloud space they desire.[2] The cloud is also an on-demand self-service in which users can manage the amount of server time requested on the cloud.[2] The cloud is scalable; meaning it can increase or decrease the number of resources used by the customer.[2] Finally, the cloud has the ability of resource pooling, which indicates it uses the same resources for multiple customers.[2]

The cloud can be used as three different services: Infrastructure as a Service (IaaS), Platform as a Service (PaaS), and Software as a Service (SaaS).[12] IaaS involves the cloud provider renting servers, applications, and even operating systems to a client.[2] Joyent Cloud® is an IaaS company that provides virtual appliances for specific computing tasks called Smart Machines.[4] PaaS allows the customer to develop applications that run on the cloud for testing.[2] Microsoft® developed a PaaS called Windows Azure for clients to build applications.[11] SaaS means the customer uses a cloud application to do a certain command, such as document management or data storage. Apple[13] has created its own SaaS called iCloud.

In October 2011, Apple joined its corporate rivals and introduced iCloud, a cloud computing service that is included in the latest Apple operating systems.[6] This was an improvement from Apple's original cloud program called MobileMe because it brought multiple internet-based services into one application.[6] 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. It is able to store device settings, application data, application organization, messages, and ringtones.[6] 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.[5]

The cloud has become enticing for businesses, academia, and even government. In 2011, North Bridge Venture Partners conducted a survey about cloud computing by polling 38 industry leading corporations.[8] Forty percent of the companies stated they were experimenting with cloud computing and 13% were using it with full confidence.[8] In 2010, 20% of IT managers in the federal government planned to apply cloud computing in the following year.[7] In addition, the FBI stated the size of the average digital forensics case grew from 83 to 277 GB between 2003 to 2007.[7] Many technology companies are creating their own cloud computing service to profit from this new equipment. By 2014, cloud revenue is projected to grow to $21,057,000,000.[8]

Cloud computing has created new challenges for digital forensics. One issue is what digital forensic software is capable of processing data stored in the cloud using forensic software. Typically, the digital forensic examiner will acquire a physical image of a device and analyze it using industry standard digital forensic tools such as EnCase or Forensic Toolkit (FTK), but these software programs have yet to be tested on capturing live data like in the cloud.[12] Acquisition of evidence depends on the type of cloud used. Some clouds store fragments of data in volatile memory on the local device which can be acquired using a RAM dump.[10] Other clouds store artifacts on the hard drive of the device.[10]

As cloud computing grows exponentially, the research to develop forensic tools to handle acquisition and analysis must grow as well. Tony Straw (2011) conducted a case study using Apple devices to determine what data could be acquired from iCloud on each device when iCloud was enabled, when iCloud account was deleted, when iCloud data was deleted, and when the devices were wiped. Straw created an Apple ID account and enabled it on an iPhone, an iPod, and an iPad. Straw reported that application data was obtained from the first three scenarios. The only scenario in which the data was not recoverable was when the iCloud data was deleted and the devices were wiped. Straw was able to find designated folders on each device that saved iCloud data onto the device. It was concluded that because iCloud stores data on iOS devices, an examiner can acquire it data during a seizure.[9]

In August 2012, a former Gizmodo journalist, Mat Hanon, had all of his Apple devices hacked and wiped through iCloud. Apple customer service had seen cases like this before in which the hacker obtained iCloud access through social engineering. This case emphasizes the need to understand iCloud and what data can be extracted from it because this is only the beginning of malicious behavior on iCloud.[3]

The purpose of the iCloud analysis reported in this study is to determine if there are artifacts that confirm iCloud has been enabled on Apple devices. Straw's study focused on what application data could be collected from each Apple device. Unlike Straw's report, this analysis focuses on what iCloud specifications and relevant forensic artifacts can be obtained from a hard drive acquisition. 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 enablement on both devices. A baseline image of the iPod and the MacBook was created. iCloud was enabled on each device and a second image was created. The before and after images of each device were compared to one another. In addition, images of the MacBook and the iPod after iCloud enablement were also compared to each other.

Materials and Methods

Materials

The iPod Touch 4G (4th generation) was chosen as the mobile device because its operating system, iOS 5.0.1, was an operating system that supported iCloud and it was the latest model of the iPod Touch on the market (Table 1). The MacBook Pro with Mac OS X Lion was chosen as the computer because its operating system supported iCloud and it was the most recent model (Table 2).

iPod Touch Acquisition with Cellebrite UFED Physical Analyzer

On Cellebrite UFED Physical Analyzer, iOS Device Physical Extraction was used to acquire images from the iPod (Tables 3 and 4). The software displayed two options to acquire an image: physical dump or file system extraction. Both options were chosen to determine which would be used. Also under both extractions, one could choose to extract data or system partitions or both. Data and system partitions were selected to be extracted. After extraction was completed, the physical analyzer verified each image through SHA-256 hash values. The file system extraction was saved as a TAR file, a PAS file, and an UFD file. The physical extraction was saved as an IMG file, a PAS file, and a UFD file. The physical analyzer tool was used three times: 1) when the iPod was taken out of its packaging (“Clean iPod”), 2) after the iPod was enabled with iTunes (“iCloud-disabled iPod”), and 3) after iCloud was enabled (“iCloud-enabled iPod”). Device information was recorded into an Excel spreadsheet. The number of certain file types was also documented.

iPod Acquisition with Lantern

Lantern was launched on a MacBook workstation (Tables 5 and 6). A new case was created. In order for Lantern to recognize the iPod, the iPod was left on. Under the acquisition options, Everything was checked. This included system data, application data, photos, videos, and media. When the acquisition was completed, the extraction summary was generated. The image was saved as a lantern file and the report was saved as a .csv file, .html file, and .json file. The iPod was acquired with Lantern before and after iCloud enablement. The device information and identified artifacts were documented in an Excel spreadsheet.

MacBook Acquisition with FTK Imager

The MacBook's solid state drive (SSD) was extracted from the laptop case (Table 7). The SSD was connected to the forensic workstation via a write blocker (Tables 8 and 9). FTK Imager was opened on the workstation and Create Disk Image was selected (Table 10). The SSD was selected as the source drive (\\ \PHYSICALDRIVE1-APPLE SSD TS512C (500GB SCSI)). The image was created as a raw (dd) file, and the 2 TB hard drive was chosen as the destination drive (Table 11). The image hash was verified with MD5 and SHA2 hashing. Once the dd image was created, the SSD was disconnected and placed back into the laptop. This method was used on the SSD before and after iCloud was enabled ("iCloud-disabled MacBook" and "iCloud-enabled MacBook", respectively).

Storage of iPod and Mac Images

All images were saved on the 2 TB hard drive, which was the working drive (Table 12). The images were saved onto an additional drive as a pristine copy (Table 13). Acquisition and analysis steps were documented with digital photography and screenshots.

iTunes Activation

With the sync adapter cable, the iPod was connected to the MacBook. iTunes started automatically when the iPod was plugged in. The MacBook was connected to a Wi-Fi network in order for iTunes to connect to the iTunes store. A "Let's Get Started" page was displayed under the device tab. The terms and conditions of the iPod software were agreed to first. A device name was created (John Marshall). Songs, videos, photos, and apps were selected to synchronize automatically to iPod. A device summary showed the completion of iTunes activation on the MacBook. Setup continued on the iPod itself by using the network connection through the MacBook. United States was selected as the Country or Region. Location Services preference was disabled. Diagnostics and usage information messages were disabled. A "thank you" page finalized the setup.

iCloud Enablement on MacBook Pro

On the MacBook, iCloud was located under the Internet and Wireless section in the System Preferences menu. An Apple ID was not already established, so one was created. A series of fields were filled out, creating a free iCloud email address (john.marshallfs@me.com), a username (John Marshall), and a password (AlsoMisde1). Once the iCloud account was created, a window with all of the iCloud applications opened. All applications were enabled except for Back to My Mac.

iCloud Enablement on iPod Touch

The iPod was turned on and Settings was selected. In Settings, the iPod was connected to a Wi-Fi account. Back in Settings, the iCloud menu was chosen. The Apple ID and password created on the MacBook were typed into the iCloud enablement menu and the account was verified. A new window opened asking to enable location services. Location Services was enabled. In the iCloud menu window, the account name was displayed at the top, followed by the applications and whether they were on or off. All of the applications were already turned on except for Photostream. Photostream was changed to "enabled." Under Storage and Backup, the iCloud Backup application was enabled. This meant the iPod would back up only to iCloud automatically and not the computer. 5 GB of storage were available. Under Manage Storage, it displayed what application was using iCloud storage and how much storage it used. The application Mail was using 5 MB of storage in iCloud. Under the Account tab, the iCloud account information (Apple ID, password), the storage plan, and the advanced email address were listed.

iCloud Functions on iPod Touch

After iCloud was enabled on the iPod, certain applications connected to iCloud were utilized. The Mail application was opened to generate any emails sent to john.marshallfs@me.com. An event called "Birthday Cupcakes!" was added to the Calendar application. In the App Store, Find My Friends application was downloaded. Before the application could be downloaded, the Apple ID account was verified, account settings (payment type and billing information) were entered, and the Terms and Conditions were agreed to. Find My Friends was downloaded to the iPod's home screen. In the Contacts application, a contact (Rachel Friedman) was added to the contact list.

Analysis of iPod Touch with FTK

Three cases were created in FTK correlating with the three iPod images that were acquired: clean iPod image, iCloud-disabled iPod image, and iCloud-enabled iPod image (Table 14). The file system extraction TAR files of the iPod from Cellebrite were added to their respective cases in FTK. The TAR files, which were live files, were converted into ad1 images in FTK before being added as evidence. In all three cases, the following keywords were searched using Index Search: iCloud, Castle, and John.MarshallFS. These keywords were chosen because they referred to the iCloud account. The number of hits and files for each keyword was documented. Files of interest were bookmarked under their respective keyword. Under the

Overview tab, the database and property list[14] (plist) file extensions were searched for relevant files and bookmarked under the appropriate file extension. The number of databases and plists found were documented as well. Under the Explorer tab, files were searched by date of modification. The files were bookmarked under the date they were found. The files located in each iPod image that appeared to have iCloud artifacts were compared to one another.

Analysis of MacBook Pro in FTK

Two cases were made for each MacBook image in FTK and the correlating dd image was added as evidence. Once the images were added to each case, a keyword search was conducted with the following words using Index Search: iCloud, Castle, John.MarshallFS. Files that contained the keywords were bookmarked under their respective keyword. Under the Overview tab, plists and databases were searched for artifacts and those files were bookmarked as well. Under the File Category folder, the number of files in each category was documented in an Excel spreadsheet. Other files were searched by date of creation and modification in the Explorer tab. The differences between each image's evidence log were documented in an Excel spreadsheet also. The contents of the same files from each image were compared to each other.

Analysis of Synchronization of iPod Touch and MacBook Pro

Synced application files were compared from both iCloud-enabled devices. Similar plists were documented. Files were searched based on date of modification for counterpart files.

Results

Acquisition and Analysis Selection for iPod Touch

Cellebrite and Lantern software were compared to determine which application acquired the most information (Table 15). Cellebrite was able to extract the file system structure along with application data. Lantern was only able to extract application data, but no file system data.

Additionally, Cellebrite obtained more device information than Lantern such as the Chip ID, the Sync Hostname, and whether Cloud Backup was enabled. The two Cellebrite extraction methods were also compared. The file system extraction acquired more database and configuration files than the physical dump. Therefore, the Cellebrite file system extraction was chosen to acquire all iPod images. FTK was used for analysis because its Index Search was more robust than Cellebrite's and it displayed certain files in a more user-friendly format.

Artifacts on iCloud-enabled iPod

Artifacts were found on the iPod as a result of iCloud being enabled. There were differences between the three iPod images regarding the number of files in each file system as well as the number of hits for the listed keywords (Table 16). Since the first two iPod images showed similar results, the iCloud-disabled image was the primary image used.

Evidence was found in plists. By reviewing the plists between the iCloud-enabled iPod and the iCloud-disabled iPod, significant differences were determined between the two images. The Apple ID Authentication Info plist displayed the dates and times of an Apple ID. The iCloud-disabled iPod only showed the creation date and time of the physical iPod (Figure 1). However, the iCloud-enabled iPod identified the name of the Apple ID account along with the creation timestamp of the account and when the account was last successfully connected (Figure 2).

The data_ark.plist file was found on both iPod images. It listed specific characteristics about the iPod and whether these characteristics were enabled or disabled. One property key was labeled iCloudBackupEnabled. On the iCloud-disabled iPod, the CloudBackupEnabled property key was not enabled (Figure 3). On the iCloud-enabled iPod, the CloudBackupEnabled property key was enabled (Figure 4). The data_ark.plist from the iCloud-enabled iPod also showed iCloud was the source for the data sync of certain applications: Contacts, Calendars, Bookmarks, and Notes.

The accountsettings.plist displayed the number of accounts attached to the iPod and each account's features. The iCloud-disabled iPod had only one account, known as Device Local Account, meaning the account was the iPod itself (Figure 5). Its type string was On My iPod Touch, showing the account was for the physical iPod. The iCloud-enabled iPod displayed 3 accounts, with the primary account being the Apple ID account (Figure 6). The type string was iCloud, showing the account was connected to iCloud. The iCloud account also listed eight data classes that corresponded to the enabled applications in iCloud.

Artifacts on iCloud-enabled MacBook Pro

Artifacts were found on the MacBook as a result of iCloud enablement. The two images differentiated by the number of plists and databases as well as the number of hits of the listed keywords (Table 17). The iCloud-disabled and iCloud-enabled MacBook images contained the Apple ID authentication info plist file. The plist from iCloud-disabled MacBook showed only the creation date of the physical MacBook (Figure 7). However, on the iCloud-enabled MacBook, the Apple ID authentication info plist showed the creation date of the apple ID account, the name of the Apple ID, and the last successful connect date (Figure 8). No other plists were found on the iCloud-disabled MacBook that had counterpart files on the iCloud-enabled MacBook.

The MacBook created plists after iCloud was enabled and therefore those plists were not found on the iCloud-disabled MacBook image. The Apple Online Services (AOS) Notification accounts plist was only found on the iCloud-enabled MacBook and it represented MobileMe syncing. It listed the iCloud specifications: username, personID, and Owner Display Name (Figure 9).

The AlsoMISDE.plist showed linked identities between the MacBook named AlsoMISDE and the Apple ID, john.marshallfs@me.com (Figure 10). The xml string listed the keys and arrays that pointed to the two names becoming linked. The timestamp matched the time in which iCloud was enabled as well.

Another artifact that supported iCloud enablement on the MacBook was a migration log (Figure 11). The log listed a web address that pointed to iCloud. The first part of the address, john.marshallFS, matched the Apple ID. “Contacts.icloud.com” referred to the contacts application in iCloud. The number 1934105030 was the person ID assigned to the iCloud account when it was created. After iCloud enablement, three contacts were found in the Address Book. In the migration log, the number of local people was three.

Artifacts of Synchronization between the iPod Touch and the MacBook Pro

No artifacts were found that clearly showed the iPod and the MacBook were synchronized to each other by iCloud during the analysis. However, artifacts were found in plists that showed the iPod and MacBook shared the same data from iCloud. In the Apple ID authentication info plists, the Apple ID and the encDsId keys had the same values on both devices (Figures 1 and 8).

The applications that were enabled and used on the iPod and the MacBook shared plist characteristics. The calendar event “Birthday Cupcakes!” was found on the iPod image and the MacBook image (Table 8 and Table 9). The path to the event on the iPod was:

root\private\var\mobile\Library\Calendar\Calendar.sqlitedb\table\CalendarItem

The path to the event on the MacBook Pro was:

Users\AlsoMISDE\Library\Calendars\E57FCAB7-2DE1-473E-8E98-89A977AFD497.caldav\2CC2CF7A-C7D9-460A-8720-53EA49D36508.calendar\Events

The calendar event was labeled DA873387-8660-4522-9740-972F1F665451. The unique identifier (UID) from the MacBook's calendar event matched the UID from the iPod's calendar event. This number was also found on the MacBook's event under Server File Name. The created and modified time stamps also matched.

The iPod and the MacBook shared the same calendars via iCloud. iCloud added four calendars to the iPod when it was enabled: Work, Home, Reminders, and Inbox (Figure 12). The Work, Home, and Reminders calendars were added to the MacBook (Figure 13, 14, and 15). Each calendar file shared the same calendar path and owner principal path. These paths were part of web addresses that may have led to storage on iCloud. The calendars also used an internet protocol called CalDAV (Calendar Distributed Authoring and Versioning), meaning the files were stored on the web, or in this case, iCloud.

The Address Books of both devices shared similarities as well. The Contact list from iCloud-enabled iPod contained four contacts (Figure 16). After iCloud was enabled, three were automatically added to the iPod and one was added manually to the iPod. Three contacts were found on the MacBook (Figures 17, 18, and 19). The contact manually added to the iPod did not sync to the MacBook through iCloud. Two weeks after the MacBook's second image was acquired, the fourth contact did appear in the Address Book. The three contacts on the MacBook shared the same .vcf number and creation date and time as its counterparts on the iPod.[15]

Discussion and Conclusions

Artifacts were found that showed iCloud was enabled on both devices. Multiple plists recognized that iCloud was enabled 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.

The Apple ID authentication info plist from the iCloud-enabled iPod corroborated iCloud enablement because its creation date of the apple ID account matched the date the Apple ID was made. Moreover, the property key CloudBackupEnabled on the data_ark.plist from the iCloud-enabled iPod had the value true. This meant iCloud was clearly enabled on the iPod. This plist also showed the certain applications were synced to iCloud because the value of the data sync source was iCloud. The iCloud account was recorded in the account settings plist file, showing it was added after iCloud was enabled. Therefore, these plists supported iCloud was enabled on the iPod Touch.

The creation date of the Apple account on the Apple ID Authentication Info plist from the iCloud-enabled MacBook matched the date the iCloud account was created on the MacBook. This indicated iCloud was enabled on the MacBook. Additionally, the iCloud specifications found in the AOS notification plist verified the iCloud account was recorded on the MacBook. The AlsoMISDE plist showed AlsoMISDE, the user account, was linked to the Apple ID, john.marshallFS. Additionally, the migration log provided evidence that the MacBook was connected to iCloud because the listed web address was the web address to contacts in iCloud and the number of local people matched the number of contacts on the Macbook.

It was more difficult to find an artifact that showed synchronization between the two devices through iCloud. In spite of that, the calendar and address book applications did share the same internet addresses to iCloud. Therefore, these applications linked to the same space on iCloud regardless of what device they were found on originally.

The synchronization between the devices is still a mystery. The subsequent question to ask is if there is another way to see synchronization between devices, for example in the volatile memory. Memory dumps are acquirable in various forensic tools, so it would be the next place to search for iCloud artifacts on each device. Another question is why all of the iPod contacts did not transfer to the MacBook in a timely fashion, like the calendar event did. One place to look for answers would be on the server connection. To understand the synchronization of iCloud connecting two devices, it would be helpful to run a packet sniffer to record and capture the traffic between the devices. The migration log is an example that needs more analysis by reviewing network traffic. Ultimately, the results and upcoming research can be combined to create a preliminary protocol on how to acquire evidence from iCloud.

Acknowledgements

The authors would like to 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.

References

[1] Capturing the Cloud- Computer Forensics and Cloud Computing. Kroll Ontrack OnPoint Blog [Internet]. 2011 [cited 2012 June 26]. Available from: http://www.krollontrack.com/blog/post/2011/04/19/Capturing-the-Cloud-e28093-Computer-Forensics-and-Cloud-Computing.aspx

[2] Coyle, F. Cloud Computing: Safe Haven or 21st Century Battlefield? Bob Lyle School of Engineering- SMU [Internet]. 2011 [cited on 2012 July 30]. Available from: lyle.smu.edu/~coyle/cse7343/handouts/2011.s26.coyle.cutterCloudHacking.pdf

[3] Honan, M. How Apple and Amazon Security Flaws Led to My Epic Hacking. Wired.com [Internet]. 2012 [cited 2012 Aug 9]. Available from: http://www.wired.com/gadgetlab/2012/08/apple-amazon-mat-honan-hacking

[4] Joyent [Internet]. 2012 [cited 2012 July 31]. Available from: http://joyent.com/.

[5] Panzarino, M. Apple reports 25M user growth for iCloud since April, now at 150M users. The Next Web [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/

[6] 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

[7] Ruan K, Carthy J, Kechadi T, Crosbie M. Cloud forensics: An overview. Cloud Forensics Research [Internet]. [Dublin, Ireland]: University College Dublin. 2011 [cited 2012 June 26]. Available

from: http://cloudforensicsresearch.org/publication/Cloud_Forensics_An_Overview_7th_IFIP.pdf

[8] Skok, M. North Bridge Future of Cloud Leadership Panel. The Future of Cloud Computing [Internet]. 2011 [cited on 2012 July 30]. Available from http://www.northbridge.com/2011-cloud-computing-survey.

[9] 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

[10] 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

[11] Windows Azure [Internet]. 2012 [cited 2012 July 31]. Available from: http://www.windowsazure.com/en-us/

[12] Zimmerman S, Glavach D. Cyber Forensics in the Cloud. IAnewsletter [Internet]. 2011 [cited 2012 June 26]; 14 (1). Available from: http://iac.dtic.mil/iatac

[13] All Apple products are copyrighted by Apple Incorporated.

[14] Property lists (plists) are databases that store configuration settings.

[15] Lists of all artifact files reviewed can be found in Tables 20, 21, 22, and 23.

Tables and Figures

Table 1. iPod Touch Specifications

Device	iPod Touch 4G
Generation	4th Generation
Manufacturer	Apple Inc.
Model	A1367
Serial Number	CCQH7U6SDT77
Storage	32 GB
Operating System Version	iOS 5.0.1 (9A405)

Table 2. MacBook Pro Specifications

Device	15" MacBook Pro
Generation	Late 2011
Manufacturer	Apple Inc.
Model	A1286
Serial Number	C02H62H0DV7P
Storage	512 GB
Operating System	Mac OS X Lion 10.7.3 (11D50d)
Processor	2.5 GHz Intel Core i7
RAM	8 GB I333 MHz DDR3 memory
iTunes version	10.6 (40) 64-bit

Table 3. Cellebrite UFED Physical Analyzer Specifications

Software	UFED Physical Analyzer
Manufacturer	Cellebrite
Version	3.0.0.189

Table 4. Laptop with Cellebrite Software Specifications

Computer	Precision M4500
Manufacturer	Dell
Operating System	Microsoft Windows XP Professional, Version 2002 SP3
Processor	Intel Core i7 CPU, Q 720 @ 1.60 GHz
RAM	3.24 GB RAM

Table 5. Lantern Software Specifications

Software	Lantern
Manufacturer	Katana Forensics, Inc. (Copyright 2010-2012)
Version	2.3.1

Table 6. Laptop with Lantern Specifications

Computer	15" MacBook Pr 2,2
Manufacturer	Apple Inc.
Model	A1211
Serial Number	W870856EW0G
Processor	Intel Core Duo, 2.16 GZ speed
RAM	2 GB
Operating System	Mac OS X 10.6.7 (10J869)

Table 7. MacBook’s Hard Drive Specifications

Storage Device	Solid state drive
Manufacturer	Toshiba
Model	THNSNC512GBSJ
Serial Number	X15S10A0TO3Z

Table 8. Forensic Workstation Specifications

Computer	Optiplex Desktop
Manufacturer	Dell
Operating System	Windows XP Professional x64 Edition SP2
Processor	Intel Core 2 Quad CPU Q9650 @ 3.00 GHz
RAM	7.93 GB

Table 9. Write Blocker Specifications

Device	eSATA Forensic Bridge
Manufacturer	Tableau
Model	T35es-R2
Serial Number	21351025

Table 10. FTK Imager Specifications

Software	FTK Imager
Manufacturer	AccessData
Version	3.0.0.1443

Table 11. USB Adapter Specifications

Device	SATA/IDE to USB 2.0 Adapter
Manufacturer	Vantec

Table 12. Working Hard Drive Specifications

Device	Hard Drive
Manufacturer	Western Digital
Storage	2.0 TB
Model	WD2002FAEX
Serial Number	WMAY02906636

Table 13. Duplicate Hard Drive Specifications

Device	Hard Drive
Manufacturer	Western Digital
Storage	2.0 TB
Model	WD2002FAEX
Serial Number	WMAY01551336

Table 14. Forensic Toolkit Specifications

Software	Forensic Toolkit
Manufacturer	AccessData
Version	3.4.1.34295 (2011)

Table 15. Comparison between Acquisitions of Cellebrite and Lantern Software.

Device Specifications	Cellebrite File System Extraction before iCloud Enablement	Lantern Acquisition before iCloud Enablement
Device Model	iPod Touch 4G	iPod Touch 4G (32 GB)
iOS Version	5.0-5.0.1	5.0.1
UDID		54df13f7dab5416b349104f22166 dd93e936a9ab
Serial Number	CCQH7U6SDT77	CCQH7U6SDT77
ECID	0000008D3D1EBD2E	
Board	n81ap	
iBoot Firmware Version	iBoot-1219.42.32	
Chip ID	8930	
Acquisition Manner	DFU mode	Live Acquisition
Owner Name	John Marshall	John Marshall
Bluetooth MAC		70:73:cb:96:65:6d
Wi-Fi MAC	70:73:CB:9E:E3:86	70:73:cb:9e:e3:86
Time Zone	America/New_York	
Cloud Backup Enabled	FALSE	
Sync Host Name	AlsoMISDE's MacBook Pro	

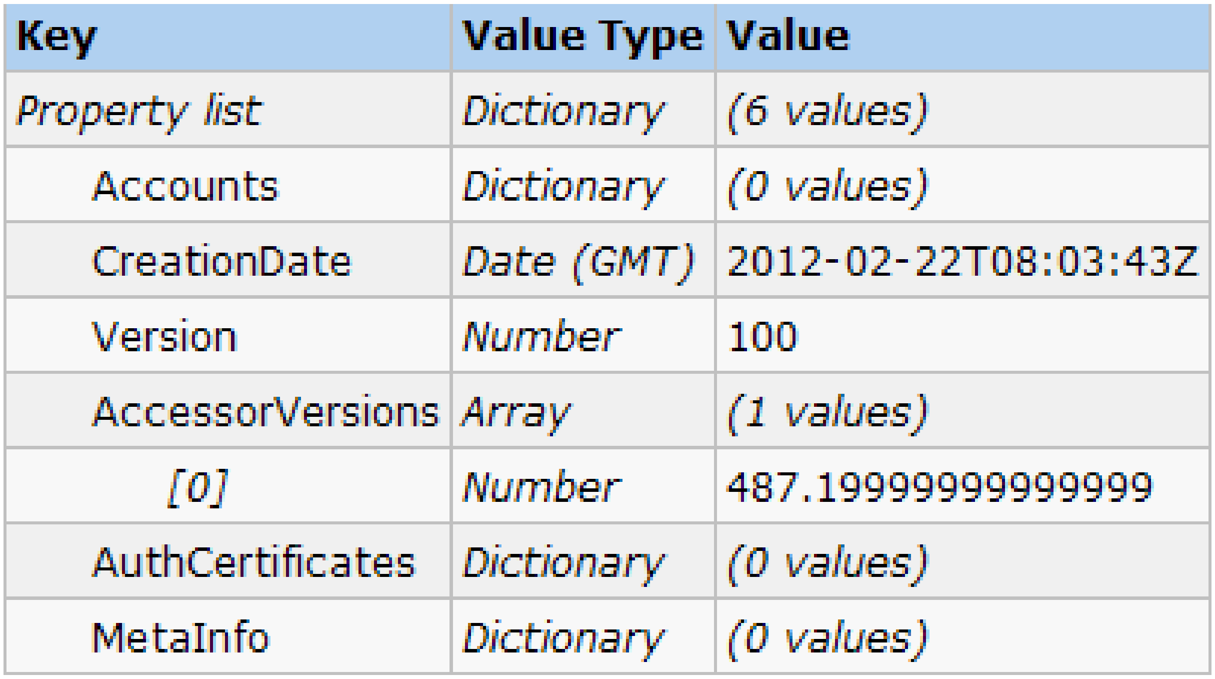
Table 16. Data Comparison of iPod Images

Type of File/Keyword	Before iTunes and iCloud	After iTunes and Before iCloud	After iTunes and iCloud
Plist	1940	1954	2047
Database	56	59	74
iCloud	5711 hits in 786 files	5711 hits in 786 files	6885 hits in 866 files
Castle	37 hits in 16 files	37 hits in 16 files	37 hits in 16 files
John.MarshallFS	0 hits in 0 files	0 hits in 0 files	73 hits in 26 files

Table 17. Data Comparison of MacBook Phases

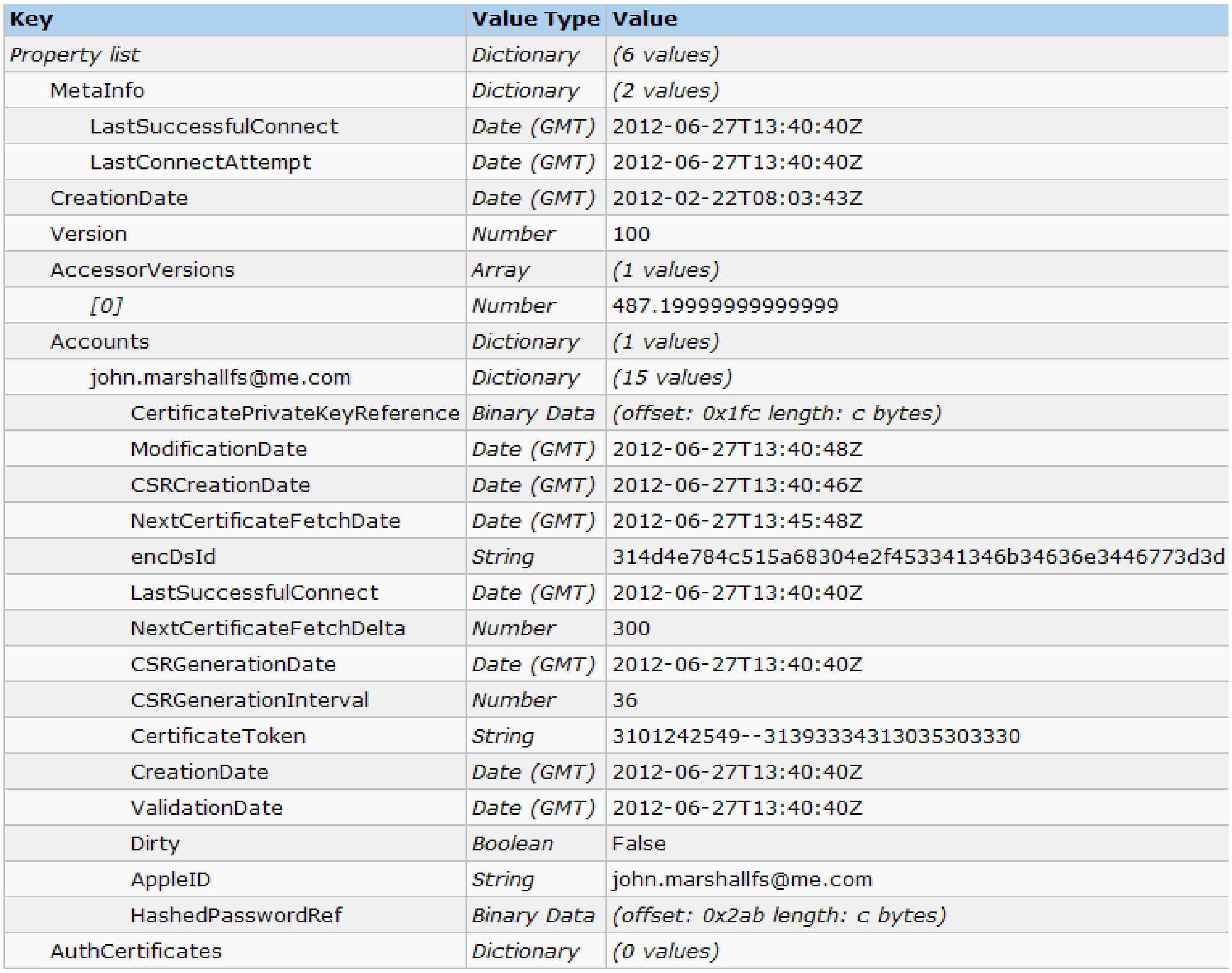
Type of File/Keyword	Before iCloud	After iCloud
Plist	19407	19490
Database	385	406
iCloud	24789 hits in 2521 files	28547 hits in 2623 files
Castle	2541 hits in 768 files	3018 hits in 779 files
John.MarshallFS	0 hits in 0 files	586 hits in 70 files

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



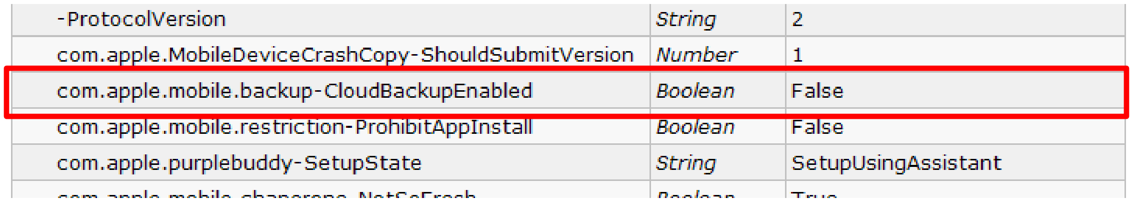
Key	Value Type	Value
Property list	*Dictionary*	*(6 values)*
Accounts	*Dictionary*	*(0 values)*
CreationDate	*Date (GMT)*	2012-02-22T08:03:43Z
Version	*Number*	100
AccessorVersions	*Array*	*(1 values)*
[0]	*Number*	487.19999999999999
AuthCertificates	*Dictionary*	*(0 values)*
MetaInfo	*Dictionary*	*(0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

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



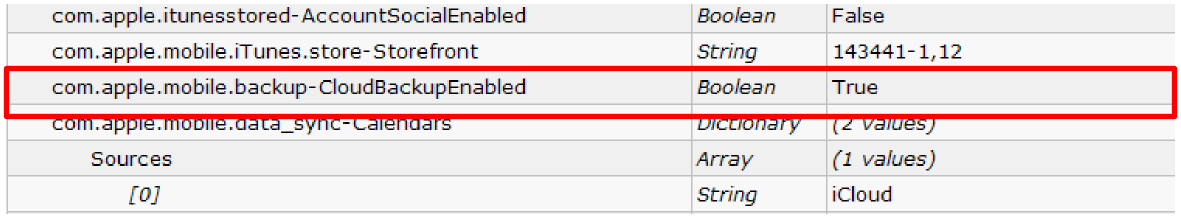
Key	Value Type	Value
Property list	*Dictionary*	*(6 values)*
MetaInfo	*Dictionary*	*(2 values)*
LastSuccessfulConnect	*Date (GMT)*	2012-06-27T13:40:40Z
LastConnectAttempt	*Date (GMT)*	2012-06-27T13:40:40Z
CreationDate	*Date (GMT)*	2012-02-22T08:03:43Z
Version	*Number*	100
AccessorVersions	*Array*	*(1 values)*
[0]	*Number*	487.19999999999999
Accounts	*Dictionary*	*(1 values)*
john.marshallfs@me.com	*Dictionary*	*(15 values)*
CertificatePrivateKeyReference	*Binary Data*	*(offset: 0x1fc length: c bytes)*
ModificationDate	*Date (GMT)*	2012-06-27T13:40:48Z
CSRCreationDate	*Date (GMT)*	2012-06-27T13:40:46Z
NextCertificateFetchDate	*Date (GMT)*	2012-06-27T13:45:48Z
encDsId	*String*	314d4e784c515a68304e2f453341346b34636e3446773d3d
LastSuccessfulConnect	*Date (GMT)*	2012-06-27T13:40:40Z
NextCertificateFetchDelta	*Number*	300
CSRGenerationDate	*Date (GMT)*	2012-06-27T13:40:40Z
CSRGenerationInterval	*Number*	36
CertificateToken	*String*	3101242549--31393334313035303330
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.



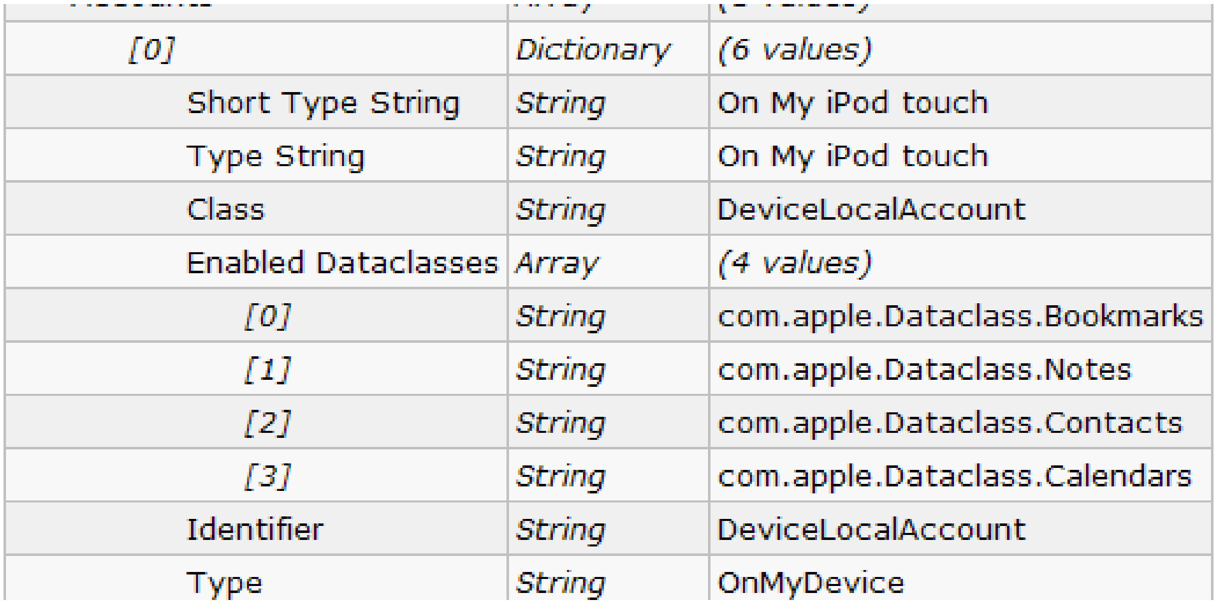
-ProtocolVersion	*String*	2
com.apple.MobileDeviceCrashCopy-ShouldSubmitVersion	*Number*	1
com.apple.mobile.backup-CloudBackupEnabled	*Boolean*	False
com.apple.mobile.restriction-ProhibitAppInstall	*Boolean*	False
com.apple.purplebuddy-SetupState	*String*	SetupUsingAssistant
com.apple.mobile.chaperone-NotSoFresh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

Figure 4. data_ark.plist from iCloud-enabled iPod.



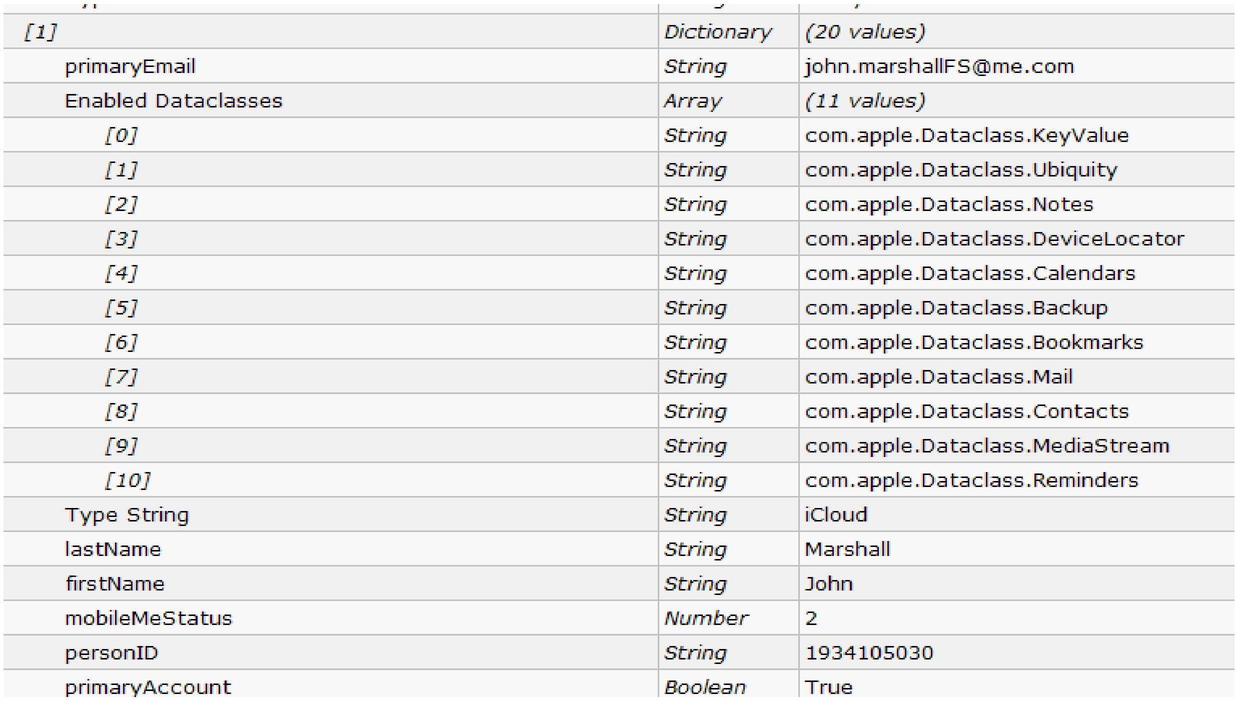
com.apple.itunesstored-AccountSocialEnabled	*Boolean*	False
com.apple.mobile.iTunes.store-Storefront	*String*	143441-1,12
com.apple.mobile.backup-CloudBackupEnabled	*Boolean*	True
com.apple.mobile.data_sync-Calendars	*Dictionary*	*(2 values)*
Sources	*Array*	*(1 values)*
[0]	*String*	iCloud

Figure 5. AccountSettings.plist from iCloud-disabled iPod.



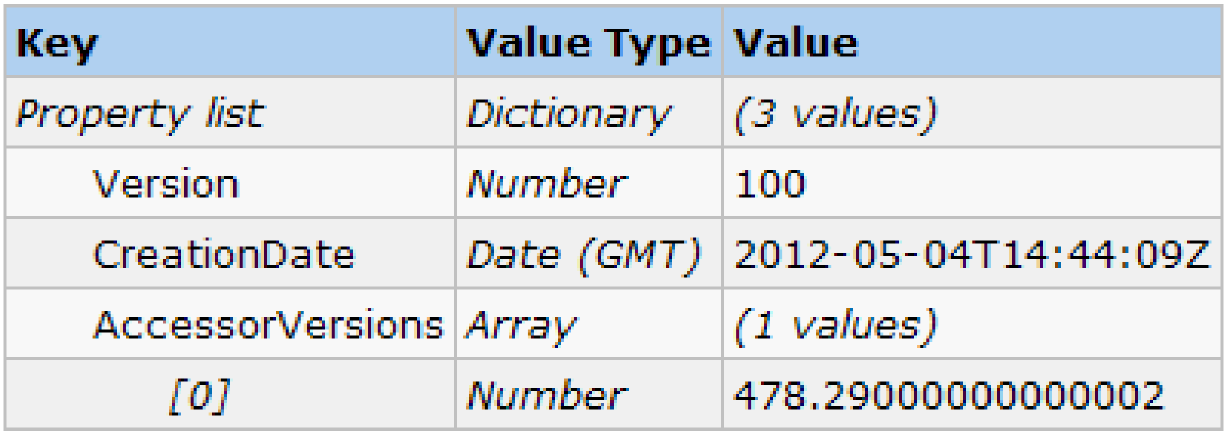
[0]	*Dictionary*	*(6 values)*
Short Type String	*String*	On My iPod touch
Type String	*String*	On My iPod touch
Class	*String*	DeviceLocalAccount
Enabled Dataclasses	*Array*	*(4 values)*
[0]	*String*	com.apple.Dataclass.Bookmarks
[1]	*String*	com.apple.Dataclass.Notes
[2]	*String*	com.apple.Dataclass.Contacts
[3]	*String*	com.apple.Dataclass.Calendars
Identifier	*String*	DeviceLocalAccount
Type	*String*	OnMyDevice

Figure 6. Account Settings plist from iCloud-enabled iPod



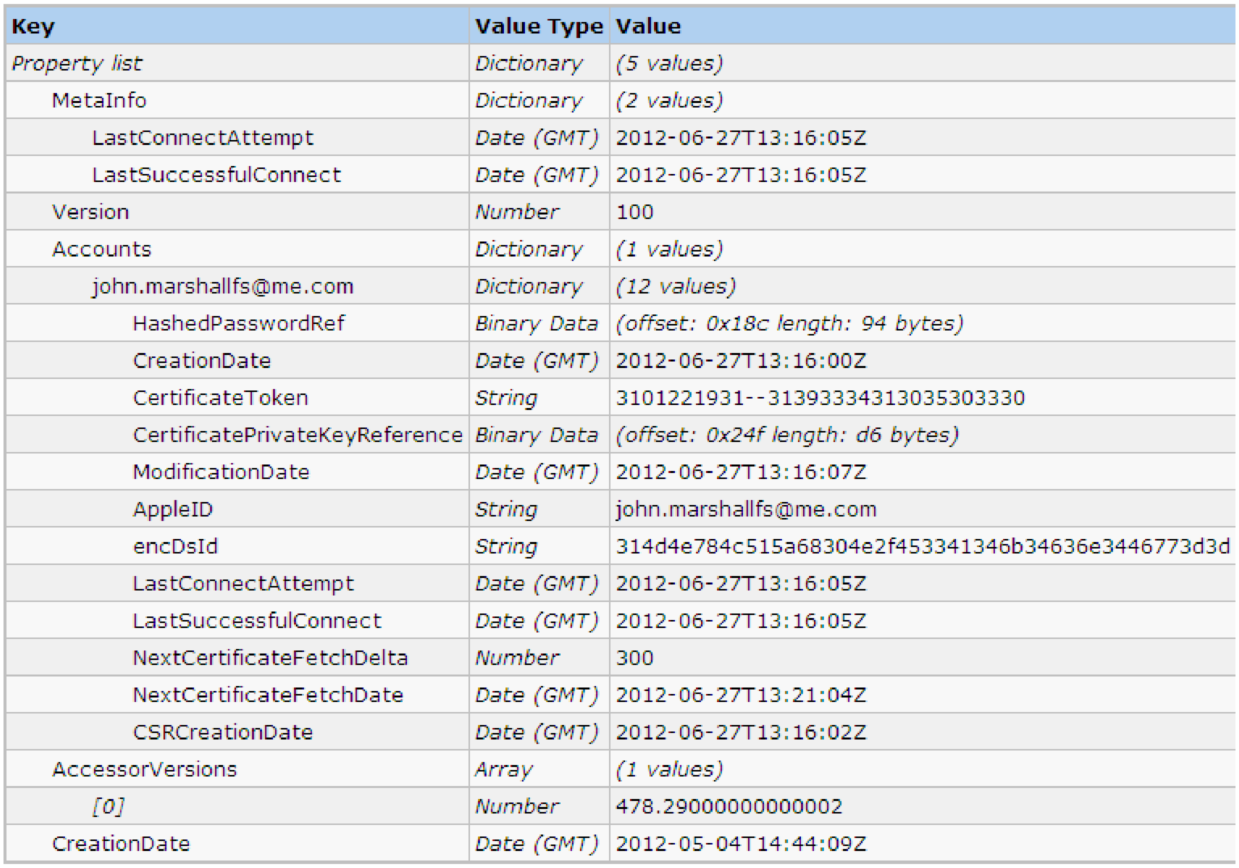
[1]	*Dictionary*	*(20 values)*
primaryEmail	*String*	john.marshallFS@me.com
Enabled Dataclasses	*Array*	*(11 values)*
[0]	*String*	com.apple.Dataclass.KeyValue
[1]	*String*	com.apple.Dataclass.Ubiquity
[2]	*String*	com.apple.Dataclass.Notes
[3]	*String*	com.apple.Dataclass.DeviceLocator
[4]	*String*	com.apple.Dataclass.Calendars
[5]	*String*	com.apple.Dataclass.Backup
[6]	*String*	com.apple.Dataclass.Bookmarks
[7]	*String*	com.apple.Dataclass.Mail
[8]	*String*	com.apple.Dataclass.Contacts
[9]	*String*	com.apple.Dataclass.MediaStream
[10]	*String*	com.apple.Dataclass.Reminders
Type String	*String*	iCloud
lastName	*String*	Marshall
firstName	*String*	John
mobileMeStatus	*Number*	2
personID	*String*	1934105030
primaryAccount	*Boolean*	True

Figure 7. Apple ID Authentication Info Plist from iCloud-disabled MacBook



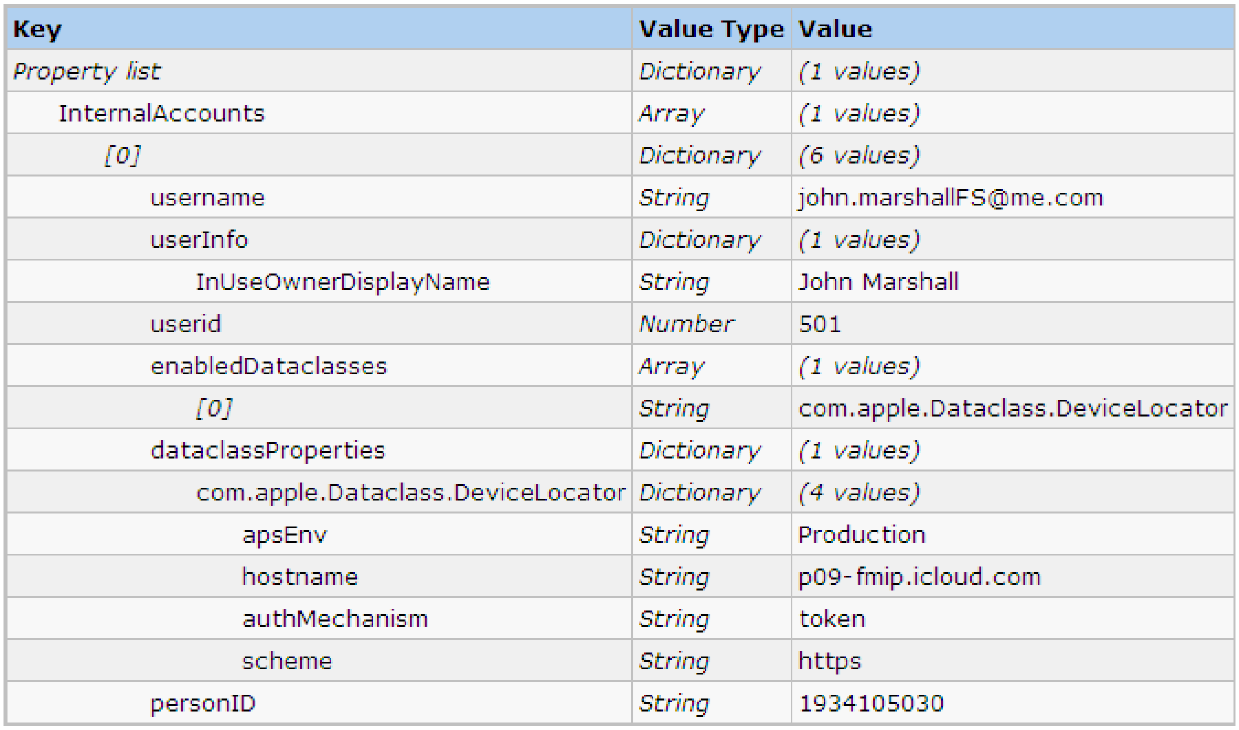
Key	Value Type	Value
Property list	*Dictionary*	*(3 values)*
Version	*Number*	100
CreationDate	*Date (GMT)*	2012-05-04T14:44:09Z
AccessorVersions	*Array*	*(1 values)*
[0]	*Number*	478.29000000000002

Figure 8. Apple ID Authentication Info plist from iCloud-enabled MacBook



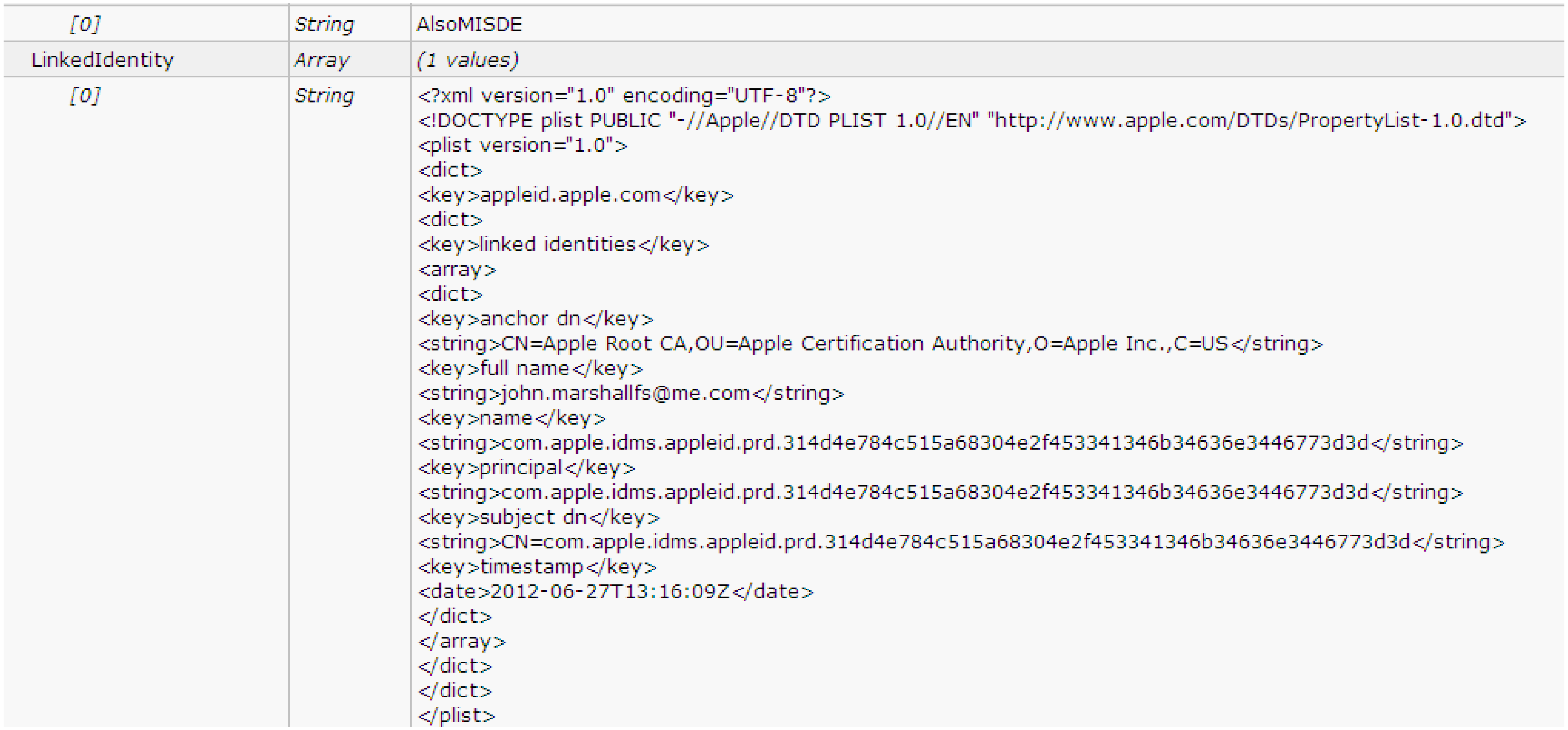
Key	Value Type	Value
Property list	*Dictionary*	*(5 values)*
MetaInfo	*Dictionary*	*(2 values)*
LastConnectAttempt	*Date (GMT)*	2012-06-27T13:16:05Z
LastSuccessfulConnect	*Date (GMT)*	2012-06-27T13:16:05Z
Version	*Number*	100
Accounts	*Dictionary*	*(1 values)*
john.marshallfs@me.com	*Dictionary*	*(12 values)*
HashedPasswordRef	*Binary Data*	*(offset: 0x18c length: 94 bytes)*
CreationDate	*Date (GMT)*	2012-06-27T13:16:00Z
CertificateToken	*String*	3101221931--31393334313035303330
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 9. AOSNotification.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

Figure 10. AlsoMISDE.plist from iCloud-enabled MacBook

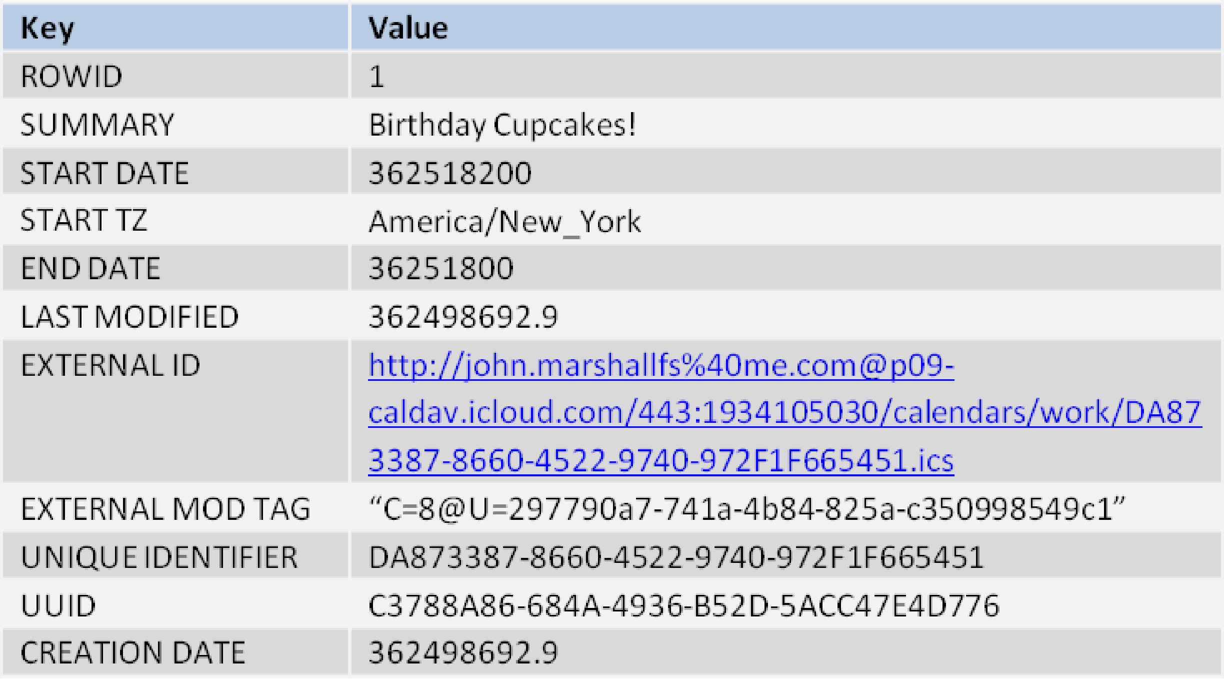


```
      [0]            String    AlsoMISDE
  LinkedIdentity     Array     (1 values)
      [0]            String    <?xml version="1.0" encoding="UTF-8"?>
                               <!DOCTYPE plist PUBLIC "-//Apple//DTD PLIST 1.0//EN" "http://www.apple.com/DTDs/PropertyList-1.0.dtd">
                               <plist version="1.0">
                               <dict>
                               <key>appleid.apple.com</key>
                               <dict>
                               <key>linked identities</key>
                               <array>
                               <dict>
                               <key>anchor dn</key>
                               <string>CN=Apple Root CA,OU=Apple Certification Authority,O=Apple Inc.,C=US</string>
                               <key>full name</key>
                               <string>john.marshallfs@me.com</string>
                               <key>name</key>
                               <string>com.apple.idms.appleid.prd.314d4e784c515a68304e2f453341346b34636e3446773d3d</string>
                               <key>principal</key>
                               <string>com.apple.idms.appleid.prd.314d4e784c515a68304e2f453341346b34636e3446773d3d</string>
                               <key>subject dn</key>
                               <string>CN=com.apple.idms.appleid.prd.314d4e784c515a68304e2f453341346b34636e3446773d3d</string>
                               <key>timestamp</key>
                               <date>2012-06-27T13:16:09Z</date>
                               </dict>
                               </array>
                               </dict>
                               </dict>
                               </plist>
```

Figure 11. Migration log from iCloud-enabled MacBook

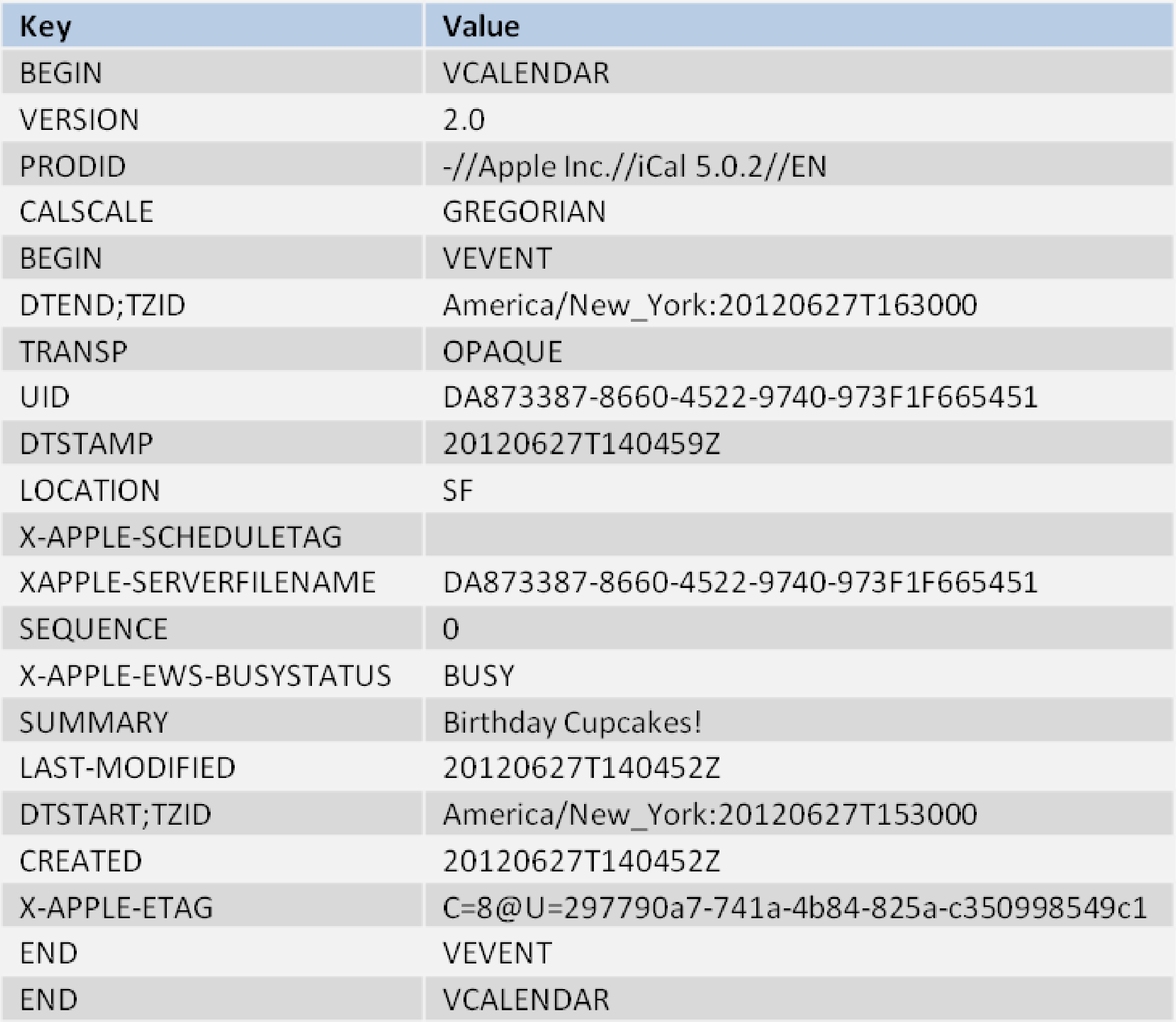
```
;p2012-06-27 09-21-04.860 [884:2303] ### PREPARING MERGER WITH 3 USERS, 0 GROUPS
2012-06-27 09-21-04.863 [884:2303] ### DOWNLOAD FROM
https://john.marshallFS%40me.com@p09-contacts.icloud.com:443/1934105030/carddavhome/card/ ###
2012-06-27 09-21-05.005 [884:2303] ### ------ SUMMARY ------ ###
2012-06-27 09-21-05.007 [884:2303] ### Local People: 3 ###
2012-06-27 09-21-05.009 [884:2303] ### Local Groups: 0 ###
2012-06-27 09-21-05.010 [884:2303] ### Server People: 0 ###
2012-06-27 09-21-05.012 [884:2303] ### Server Groups: 0 ###
2012-06-27 09-21-05.013 [884:2303] ### Merged People: 0 ###
2012-06-27 09-21-05.014 [884:2303] ### Merged Groups: 0 ###
2012-06-27 09-21-05.016 [884:2303] ### Removed People: 0 ###
2012-06-27 09-21-05.018 [884:2303] ### Removed Groups: 0 ###
2012-06-27 09-21-05.020 [884:2303] ### Local People Upload: 3 ###
2012-06-27 09-21-05.023 [884:2303] ### Local Groups Upload: 0 ###
2012-06-27 09-21-05.025 [884:2303] ### --------------------- ###
2012-06-27 09-21-05.027 [884:2303] ### UPLOAD TO https://john.marshallFS%40me.com@p09-
contacts.icloud.com:443/1934105030/carddavhome/card/ ###
2012-06-27 09-21-06.247 [884:2303] ### MIGRATION COMPLETED ###
```

Table 18. Calendar Event from iCloud-enabled iPod.



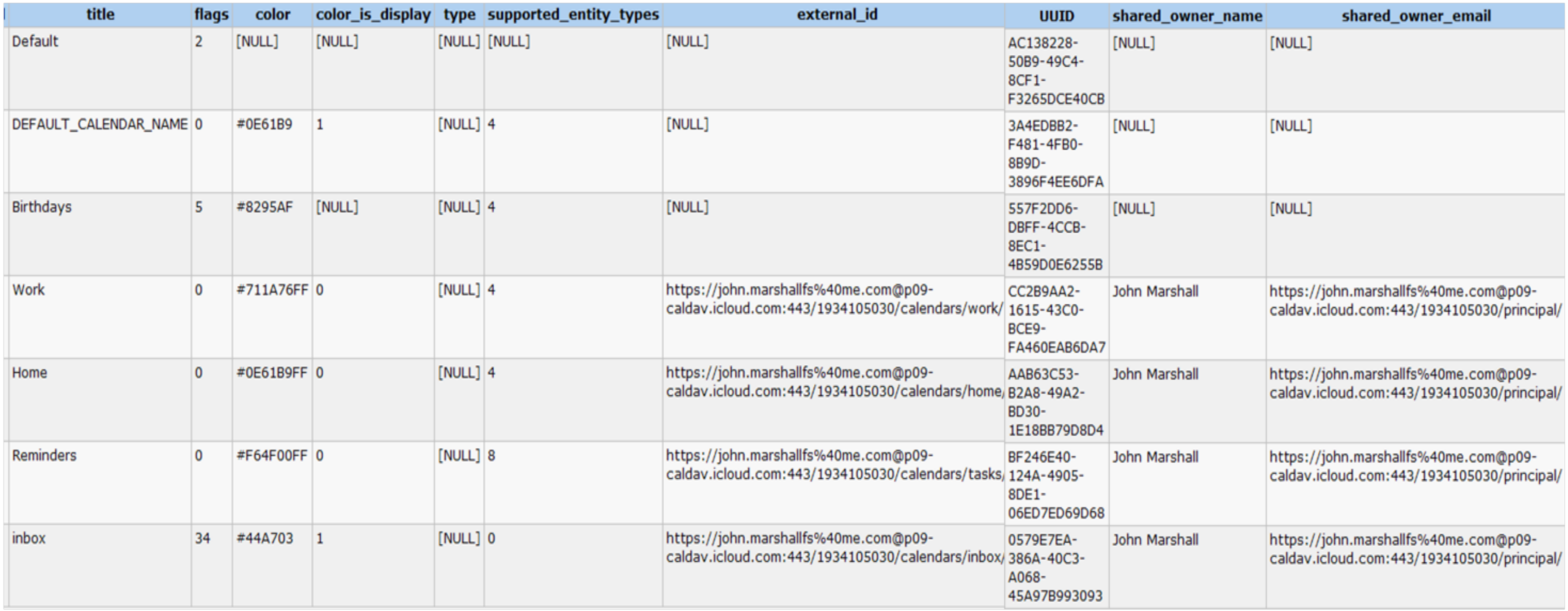
Key	Value
ROWID	1
SUMMARY	Birthday Cupcakes!
START DATE	362518200
START TZ	America/New_York
END DATE	36251800
LAST MODIFIED	362498692.9
EXTERNAL ID	http://john.marshallfs%40me.com@p09-caldav.icloud.com/443:1934105030/calendars/work/DA873387-8660-4522-9740-972F1F665451.ics
EXTERNAL MOD TAG	"C=8@U=297790a7-741a-4b84-825a-c350998549c1"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

Table 19. Calendar Event from iCloud-enabled MacBook.



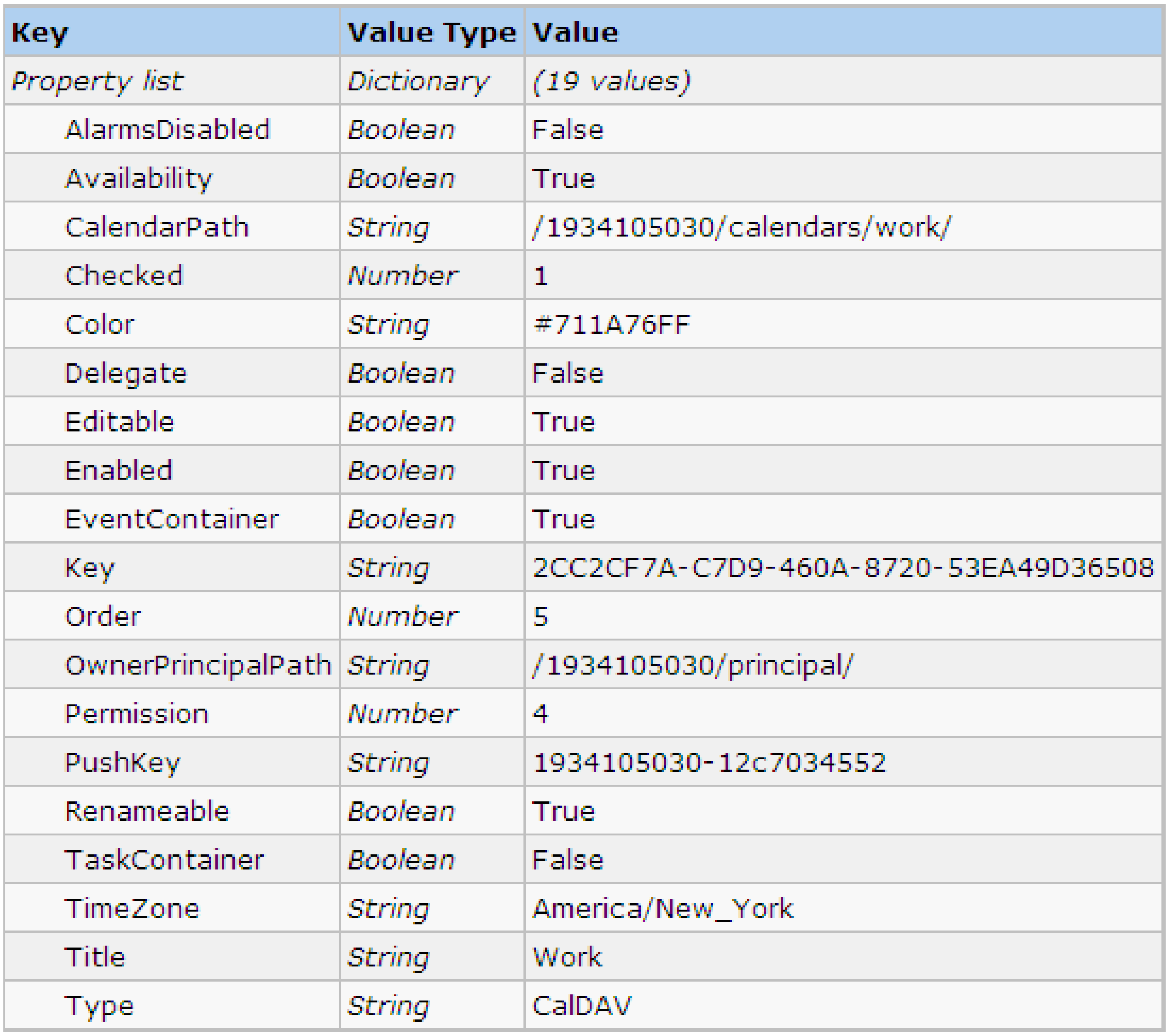
Key	Value
BEGIN	VCALENDAR
VERSION	2.0
PRODID	-//Apple Inc.//iCal 5.0.2//EN
CALSCALE	GREGORIAN
BEGIN	VEVENT
DTEND;TZID	America/New_York:20120627T163000
TRANSP	OPAQUE
UID	DA873387-8660-4522-9740-973F1F665451
DTSTAMP	20120627T140459Z
LOCATION	SF
X-APPLE-SCHEDULETAG	
XAPPLE-SERVERFILENAME	DA873387-8660-4522-9740-973F1F665451
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 12. Calendar List on iCloud-enabled iPod.



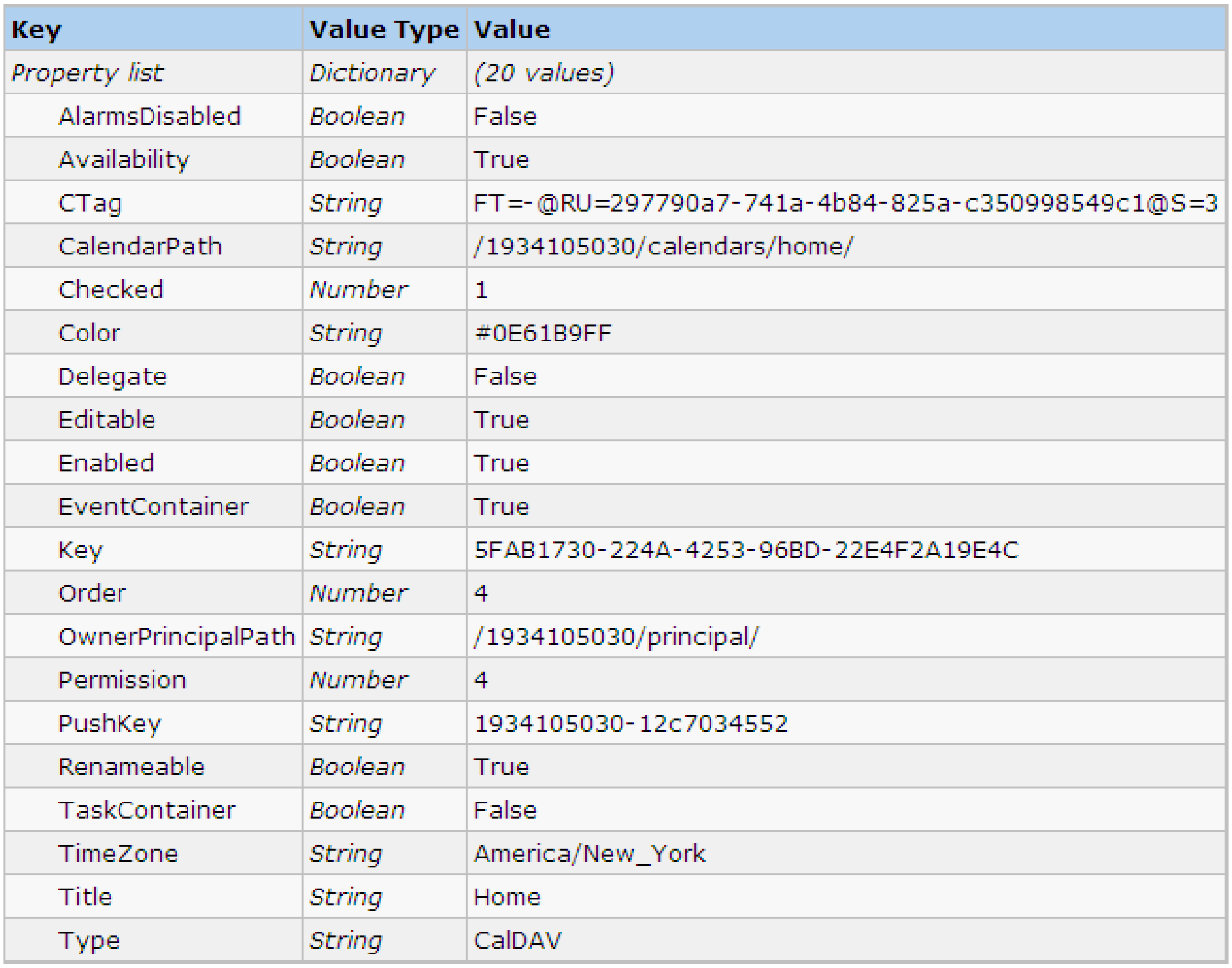
title	flags	color	color_is_display	type	supported_entity_types	external_id	UUID	shared_owner_name	shared_owner_email
Default	2	[NULL]	[NULL]	[NULL]	[NULL]	[NULL]	AC138228-50B9-49C4-8CF1-F3265DCE40CB	[NULL]	[NULL]
DEFAULT_CALENDAR_NAME	0	#0E61B9	1	[NULL]	4	[NULL]	3A4EDBB2-F481-4FB0-8B9D-3896F4EE6DFA	[NULL]	[NULL]
Birthdays	5	#8295AF	[NULL]	[NULL]	4	[NULL]	557F2DD6-DBFF-4CCB-8EC1-4B59D0E6255B	[NULL]	[NULL]
Work	0	#711A76FF	0	[NULL]	4	https://john.marshallfs%40me.com@p09-caldav.icloud.com:443/1934105030/calendars/work/	CC2B9AA2-1615-43C0-BCE9-FA460EAB6DA7	John Marshall	https://john.marshallfs%40me.com@p09-caldav.icloud.com:443/1934105030/principal/
Home	0	#0E61B9FF	0	[NULL]	4	https://john.marshallfs%40me.com@p09-caldav.icloud.com:443/1934105030/calendars/home/	AAB63C53-B2A8-49A2-BD30-1E18BB79D8D4	John Marshall	https://john.marshallfs%40me.com@p09-caldav.icloud.com:443/1934105030/principal/
Reminders	0	#F64F00FF	0	[NULL]	8	https://john.marshallfs%40me.com@p09-caldav.icloud.com:443/1934105030/calendars/tasks/	BF246E40-124A-4905-8DE1-06ED7ED69D68	John Marshall	https://john.marshallfs%40me.com@p09-caldav.icloud.com:443/1934105030/principal/
inbox	34	#44A703	1	[NULL]	0	https://john.marshallfs%40me.com@p09-caldav.icloud.com:443/1934105030/calendars/inbox/	0579E7EA-386A-40C3-A068-45A97B993093	John Marshall	https://john.marshallfs%40me.com@p09-caldav.icloud.com:443/1934105030/principal/

Figure 13. Work Calendar on iCloud-enabled MacBook



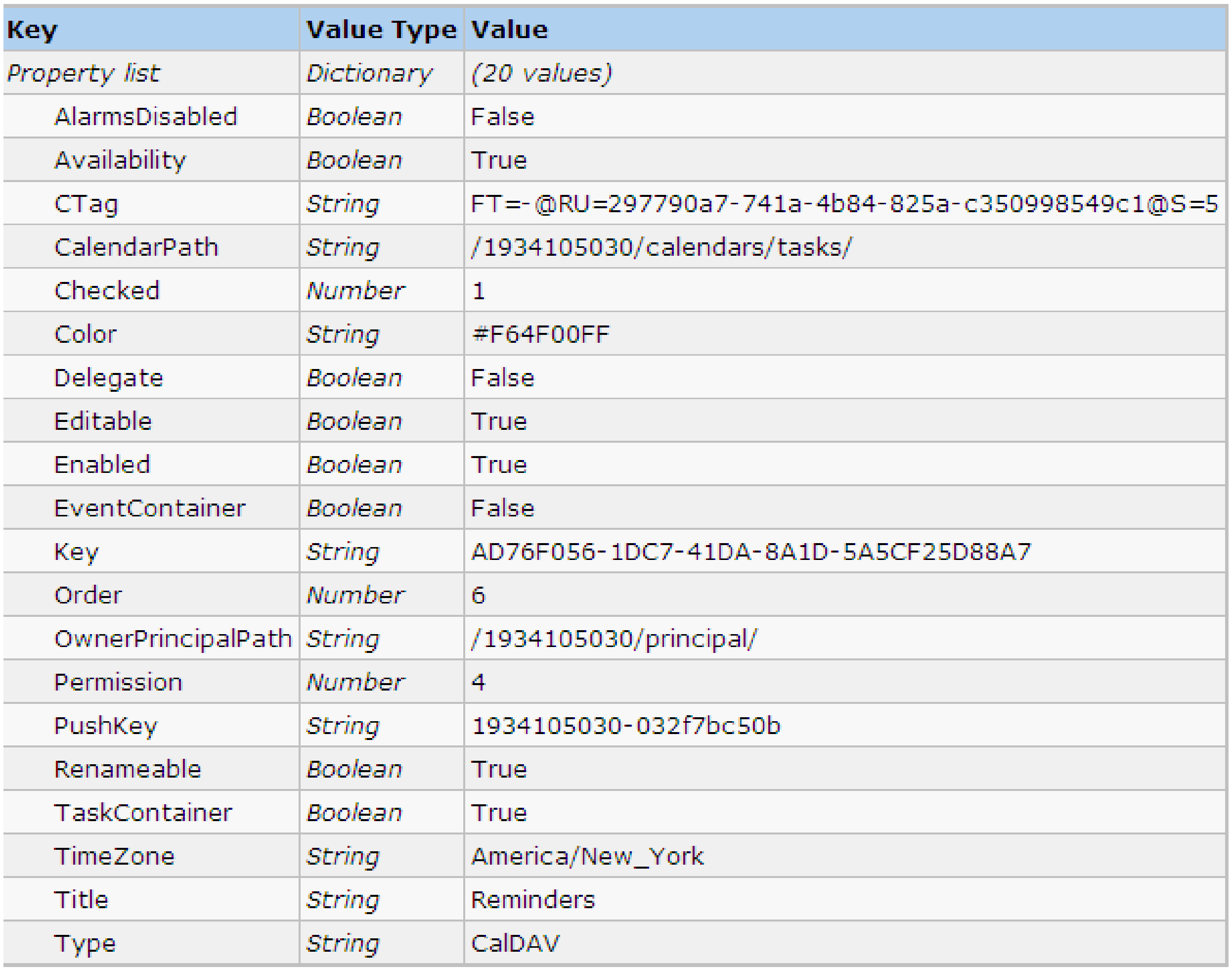
Key	Value Type	Value
Property list	*Dictionary*	*(19 values)*
AlarmsDisabled	*Boolean*	False
Availability	*Boolean*	True
CalendarPath	*String*	/1934105030/calendars/work/
Checked	*Number*	1
Color	*String*	#711A76FF
Delegate	*Boolean*	False
Editable	*Boolean*	True
Enabled	*Boolean*	True
EventContainer	*Boolean*	True
Key	*String*	2CC2CF7A-C7D9-460A-8720-53EA49D36508
Order	*Number*	5
OwnerPrincipalPath	*String*	/1934105030/principal/
Permission	*Number*	4
PushKey	*String*	1934105030-12c7034552
Renameable	*Boolean*	True
TaskContainer	*Boolean*	False
TimeZone	*String*	America/New_York
Title	*String*	Work
Type	*String*	CalDAV

Figure 14. Home Calendar from iCloud-enabled MacBook



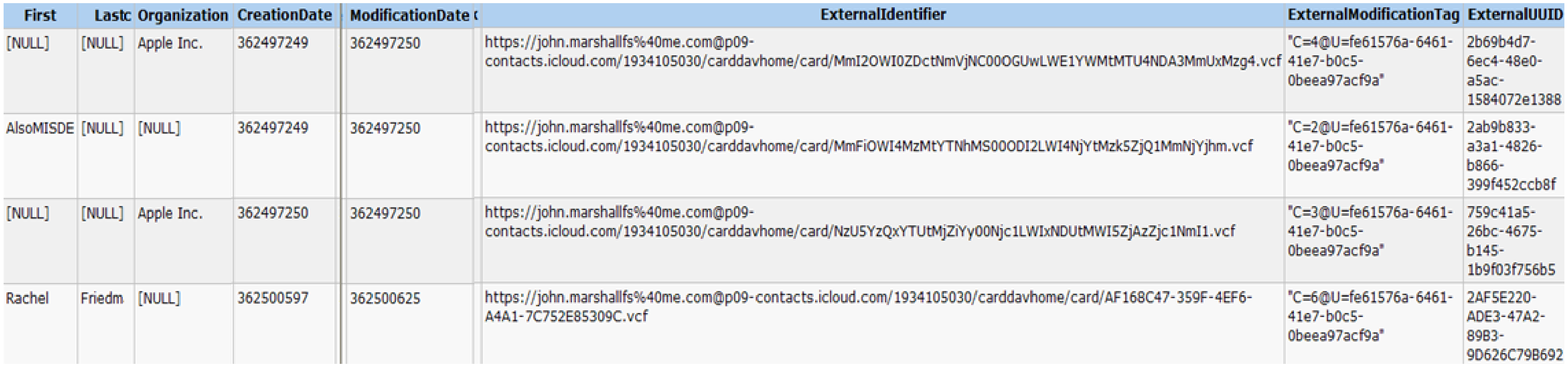
Key	**Value Type**	**Value**
Property list	*Dictionary*	*(20 values)*
AlarmsDisabled	*Boolean*	False
Availability	*Boolean*	True
CTag	*String*	FT=-@RU=297790a7-741a-4b84-825a-c350998549c1@S=3
CalendarPath	*String*	/1934105030/calendars/home/
Checked	*Number*	1
Color	*String*	#0E61B9FF
Delegate	*Boolean*	False
Editable	*Boolean*	True
Enabled	*Boolean*	True
EventContainer	*Boolean*	True
Key	*String*	5FAB1730-224A-4253-96BD-22E4F2A19E4C
Order	*Number*	4
OwnerPrincipalPath	*String*	/1934105030/principal/
Permission	*Number*	4
PushKey	*String*	1934105030-12c7034552
Renameable	*Boolean*	True
TaskContainer	*Boolean*	False
TimeZone	*String*	America/New_York
Title	*String*	Home
Type	*String*	CalDAV

Figure 15. Reminders Calendar from iCloud-enabled MacBook



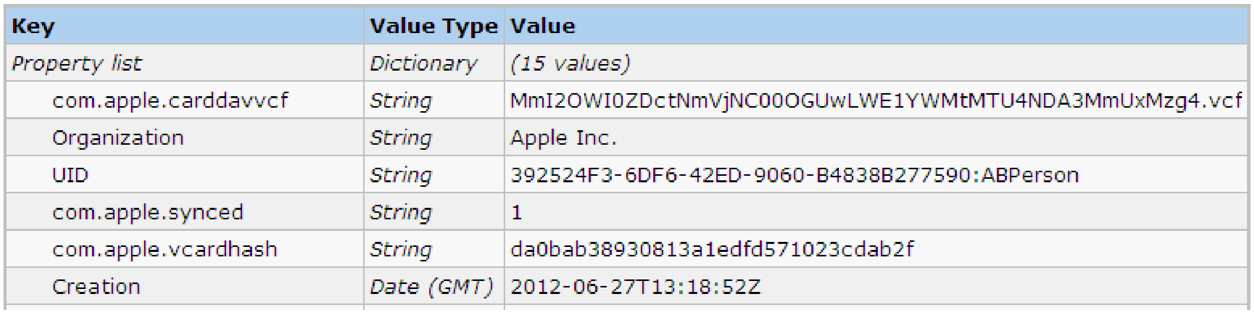
Key	Value Type	Value
Property list	*Dictionary*	*(20 values)*
AlarmsDisabled	*Boolean*	False
Availability	*Boolean*	True
CTag	*String*	FT=-@RU=297790a7-741a-4b84-825a-c350998549c1@S=5
CalendarPath	*String*	/1934105030/calendars/tasks/
Checked	*Number*	1
Color	*String*	#F64F00FF
Delegate	*Boolean*	False
Editable	*Boolean*	True
Enabled	*Boolean*	True
EventContainer	*Boolean*	False
Key	*String*	AD76F056-1DC7-41DA-8A1D-5A5CF25D88A7
Order	*Number*	6
OwnerPrincipalPath	*String*	/1934105030/principal/
Permission	*Number*	4
PushKey	*String*	1934105030-032f7bc50b
Renameable	*Boolean*	True
TaskContainer	*Boolean*	True
TimeZone	*String*	America/New_York
Title	*String*	Reminders
Type	*String*	CalDAV

Figure 16. Contact List from iCloud-enabled iPod



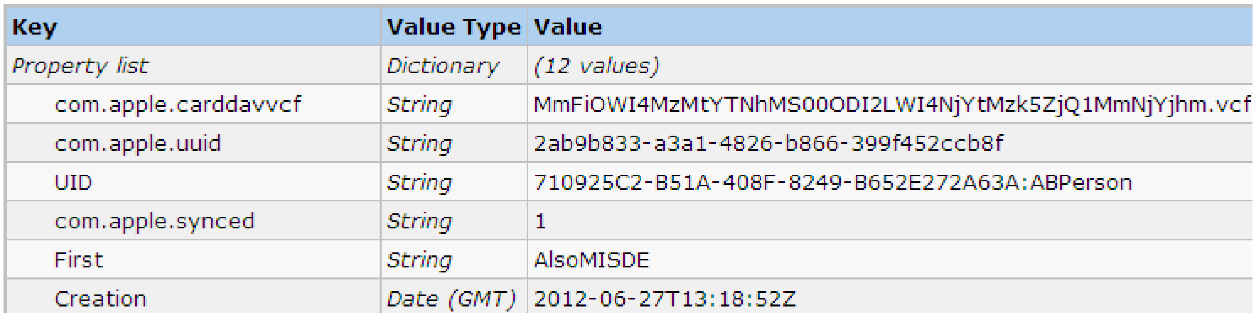
First	Lastc	Organization	CreationDate	ModificationDate	ExternalIdentifier	ExternalModificationTag	ExternalUUID
[NULL]	[NULL]	Apple Inc.	362497249	362497250	https://john.marshallfs%40me.com@p09-contacts.icloud.com/1934105030/carddavhome/card/MmI2OWI0ZDctNmVjNC00OGUwLWE1YWMtMTU4NDA3MmUxMzg4.vcf	"C=4@U=fe61576a-6461-41e7-b0c5-0beea97acf9a"	2b69b4d7-6ec4-48e0-a5ac-1584072e1388
AlsoMISDE	[NULL]	[NULL]	362497249	362497250	https://john.marshallfs%40me.com@p09-contacts.icloud.com/1934105030/carddavhome/card/MmFiOWI4MzMtYTNhMS00ODI2LWI4NjYtMzk5ZjQ1MmNjYjhm.vcf	"C=2@U=fe61576a-6461-41e7-b0c5-0beea97acf9a"	2ab9b833-a3a1-4826-b866-399f452ccb8f
[NULL]	[NULL]	Apple Inc.	362497250	362497250	https://john.marshallfs%40me.com@p09-contacts.icloud.com/1934105030/carddavhome/card/NzU5YzQxYTUtMjZiYy00Njc1LWIxNDUtMWI5ZjAzZjc1NmI1.vcf	"C=3@U=fe61576a-6461-41e7-b0c5-0beea97acf9a"	759c41a5-26bc-4675-b145-1b9f03f756b5
Rachel	Friedm	[NULL]	362500597	362500625	https://john.marshallfs%40me.com@p09-contacts.icloud.com/1934105030/carddavhome/card/AF168C47-359F-4EF6-A4A1-7C752E85309C.vcf	"C=6@U=fe61576a-6461-41e7-b0c5-0beea97acf9a"	2AF5E220-ADE3-47A2-89B3-9D626C79B692

Figure 17. Apple Inc. Contact from iCloud-enabled MacBook



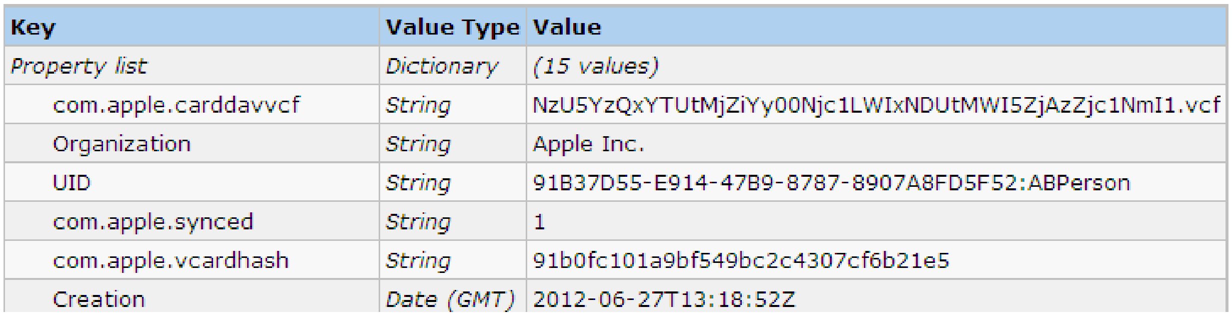
Key	Value Type	Value
Property list	*Dictionary*	*(15 values)*
com.apple.carddavvcf	*String*	MmI2OWI0ZDctNmVjNC00OGUwLWE1YWMtMTU4NDA3MmUxMzg4.vcf
Organization	*String*	Apple Inc.
UID	*String*	392524F3-6DF6-42ED-9060-B4838B277590:ABPerson
com.apple.synced	*String*	1
com.apple.vcardhash	*String*	da0bab38930813a1edfd571023cdab2f
Creation	*Date (GMT)*	2012-06-27T13:18:52Z

Figure 18. AlsoMISDE contact on iCloud-enabled MacBook



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

Figure 19. Apple Inc. Contact from iCloud-enabled MacBook



Key	Value Type	Value
Property list	*Dictionary*	*(15 values)*
com.apple.carddavvcf	*String*	NzU5YzQxYTUtMjZiYy00Njc1LWIxNDUtMWI5ZjAzZjc1NmI1.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

Table 20. Artifacts found in Plists from iCloud-enabled iPod only

Plist Name	Artifact Description	Path	Date of Modification
com.apple.network.identification.plist	IPv4 router information; IP address, timestamp	private\var\preferences\System Configuration	6/27/2012 9:39:50
com_apple_MobileAsset_SoftwareUpdate.xml	List of software updates for Apple devices	private\var\mobile\Library\Assets	6/27/2012 9:39:57
network-constraints.plist	2G, 3G, 4G, Wi-Fi download parameters	private\var\mobile\Library\Caches\com.apple.itunesstored	6/27/2012 9:39:59
com.apple.MobileBackup.plist	Backup account enabled date	private\var\root\Library\Preferences	6/27/2012 9:45:11
chunk_0000.plist	Metadata streaming begins	private\var\mobile\Library\MediaStream\sub\1934105030+1001093892\protocol	6/27/2012 10:03:27
chunk_0001.plist	Metadata streaming ends	private\var\mobile\Library\MediaStream\sub\1934105030+1001093892\protocol	6/27/2012 10:03:27
History.plist	Internet history using Safari	private\var\mobile\Library\Safari	6/27/2012 10:15:57
iTunesMetadata.plist	Manually downloaded application information from iTunes	private\var\mobile\Applications\C94A1625-1DAF-4C8A-89A3-280AD2F80405\	6/27/2012 10:29:30
Metadata.plist	Fetching data specifications	private\var\mobile\Library\Mail	6/27/2012 10:35:51
.mboxCache.plist	Mailbox name and capabilities	private\var\mobile\Library\Mail\iCloud-john.marshallfs	6/27/2012 10:35:51
70_73_cb_9e_e3_86.htm	IP Address, lease start date	private\var\db\dhcpclient\leases\en0-1	6/27/2012 10:41:14
AccountInformation.plist	Data Access information for synced applications (Notes, Calendar, Contacts, Bookmarks)	private\var\mobile\Library\DataAccess\	6/27/2012 10:41:34
rows_0000000_0000000	iCloud account data	private\var\mobile\Library\MusicLibrary\AccountCache.sqlitedb\tables\accounts	n/a

Table 21. Artifacts found in Plists shared in iCloud-disabled and iCloud-enabled iPod

Plist Name	Artifact Description	Path	Pre-iCloud Date of Modification	Post-iCloud Date of Modification
com.apple.coreservices.appleidauthenticationinfo.plist	Apple ID authentication information; creation date, Apple ID name	private\var\root\Library\Preferences	2/2/2012 3:03:46	6/27/2012 9:40:51
Sqlite Table Summary	List of properties from AddressBook application	private\var\mobile\Library\AddressBook	2/22/2012 3:10:11	6/27/2012 10:41:52
com.apple.accountsettings.plist	List of accounts on iPod with their enabled data classes	private\var\mobile\Library\Preferences	2/22/2012 3:03:46	6/27/2012 10:07:43
com.apple.mobilecal.plist	Birthday calendar data	private\var\mobile\Library\Preferences	5/30/2012 2:50:07	6/27/2012 10:06:21
Sqlite Table Summary	List of properties from Calendar application	private\var\mobile\Library\Calendar	5/30/2012 3:26:24	6/27/2012 10:41:34
com.apple.timed.plist	Time system sources and specifications	private\var\mobile\Library\Caches	6/5/2012 4:48:18	6/27/2012 9:39:57
data_ark.plist	Non-default information about iPod; last cloud backup date, cloud backup enabled key	private\var\root\Library\Lockdown	6/5/2012 4:55:53	6/27/2012 10:29:31
com.apple.wifi.plist	Wi-Fi properties	private\var\preferences\System Configuration	6/6/2012 11:19:56	6/27/2012 9:39:46

Table 22. Sqlite Databases found in iCloud-enabled iPod

Sqlite Name	Artifact Description	Path	Created Date
Calendar Item	Birthday Cupcakes! Event	private\var\mobile\Library\Calendar\Calendar.sqlitedb\tables\CalendarItem	n/a
Calendar	List of calendars linked to iCloud	private\var\mobile\Library\Calendar\Calendar.sqlitedb\tables\Calendar	n/a
ABStore	Address Book application information	private\var\mobile\Library\AddressBook\AddressBook.sqlitedb\tables\ABStore	n/a
ABPerson	List of contacts linked to iCloud	private\var\mobile\Library\AddressBook\AddressBook.sqlitedb\tables\ABPerson	n/a
Mailboxes	Mail Application information	private\var\mobile\Library\Mail\Envelope Index\tables\mailboxes	n/a

Table 23. Artifacts found in Plists from iCloud-enabled MacBook

Artifact Name	Description	Path	Creation Date	Last Accessed Date	Date Last Modified
Info.plist	Mobile device compatibilities	Macintosh HD\System\Library\CoreServices\CoreTypeBundle\Contents\Library\MobileDevices.bundle\Contents	2/16/2012 3:02:25	6/27/2012 9:03:33	2/16/2012 3:02:25
System Version.plist	MacBook properties	Macintosh HD\System\Library\CoreServices\	2/17/2012 3:10:13	2/17/2012 3:10:13	7/2/2012 5:53:18
13fcec800c483aa9cc21b0f0e731757ac0f2dea9	User assigned device name	Macintosh HD\Users\AlsoMISDE\Library\Application Support\MobileSync\Backup\54df13f7dab5416b349104f22166dd93e936a9ab\13fcec800c483aa9cc21b0f0e731757ac0f2dea9	6/5/2012 4:44:25	6/5/2012 4:44:25	6/5/2012 4:44:25
10c0b06595e6ff4e95ee09e742f9797c5367385e	iOS build	Macintosh HD\Users\AlsoMISDE\Library\Application Support\MobileSync\Backup\54df13f7dab5416b349104f22166dd93e936a9ab\10c0b06595e6ff4e95ee09e742f9797c5367385e	6/5/2012 4:44:25	6/5/2012 4:44:25	6/5/2012 4:44:25
Info.plist	iPod device information: device name, iTunes version, last backup date	Macintosh HD\Users\AlsoMISDE\Library\Application Support\MobileSync\Backup\54df13f7dab5416b349104f22166dd93e936a9ab	6/5/2012 4:44:26	6/5/2012 5:04:32	6/5/2012 4:49:00
com.apple.iPod.plist	iPod activation information: firmware version, serial number	Macintosh HD\Users\AlsoMISDE\Library\Preferences	6/5/2012 4:48:12	6/5/2012 4:48:21	6/5/2012 4:48:21
Manifest.plist	iPod product information: product version, device	Macintosh HD\Users\AlsoMISDE\Library\Application Support\MobileSync\Backup\54df13f7dab5416b349104f22166dd93e936a9ab	6/5/2012 4:49:00	6/5/2012 5:09:32	6/5/2012 4:49:00

	name, build version				
4D68157F-835B-59EF-B4B1-DFBAFF3DB7F6.plist	Apple ID authentication information: creation date, Apple ID name	Macintosh HD\Users\AlsoMISDE\Library\Preferences\ByHost\com.apple.coreservices.appleidauthenticationinfo.4D68157F-835B-59EF-B4B1-DFBAFF3DB7F6.plist	6/27/2012 9:16:07	6/27/2012 9:16:07	6/27/2012 9:16:07
ABPerson.abcdp	Apple Inc. contact	Macintosh HD\Users\AlsoMISDE/Library/Application Support/AddressBook/Sources/b1a97d73-4c47-4768-8ca8-3edf5301ef96/Metadata/91b37d55-e914-47b9-8787-8907a8fd5f52:ABPerson.abcdp	6/27/2012 9:18:52	6/27/2012 9:21:08	6/27/2012 9:21:06
ABPerson.abcdp	Apple Inc. contact	Macintosh HD\Users\AlsoMISDE/Library/Application Support/AddressBook/Sources/b1a97d73-4c47-4768-8ca83edf5301ef96/Metadata/392524f3-6df6-42ed-9060-b4838b277590:ABPerson.abcdp	6/27/2012 9:18:52	6/27/2012 9:21:08	6/27/2012 9:21:06
ABPerson.abcdp	AlsoMISDE contact	Macintosh HD\Users\AlsoMISDE/Library/Application Support/AddressBook/Sources/b1a97d73-4c47-4768-8ca8-3edf5301ef96/Metadata/710925c2-b51a-408f-8249-b652e272a63a:ABPerson.abcdp	6/27/2012 9:18:52	6/27/2012 9:21:23	6/27/2012 9:21:21
Info.plist	Calendar accounts	Macintosh HD\Users\AlsoMISDE\Library\Calendars\E57FCAB7-2DE1-473E-8E98-89A977AFD497.caldav	6/27/2012 9:20:53	6/27/2012 10:16:45	6/27/2012 10:16:43
com.apple.AOSNotification.Accounts.plist	iCloud syncing properties: username, hostname, person ID	Macintosh HD\private\var\root\Library\Preferences	6/27/2012 9:20:53	6/27/2012 9:20:53	6/27/2012 9:20:53
C5F07CFD-0E760-437A-8073-B899CA3ADCEF.plist	Calendar migration properties: title migration	Macintosh HD\Users\AlsoMISDE\Library\Calendars	6/27/2012 9:20:53	6/27/2012 9:20:53	6/27/2012 9:20:53

Info.plist	Work calendar specifications	Macintosh HD\Users\AlsoMISDE\Library\Calendars\E57FCAB7-2DE1-473E-8E98-89A977AFD497.caldav\2CC2F7A-C7D9-460A-8720-53EA49D36508.calendar	6/27/2012 9:20:55	6/27/2012 10:16:45	6/27/2012 10:16:45
Info.plist	Home calendar specifications	Macintosh HD\Users\AlsoMISDE\Library\Calendars\E57FCAB7-2DE1-473E-8E98-89A977AFD497.caldav\5FAB1730-224A-4253-96BD-22E4F2A19E4C.calendar	6/27/2012 9:20:55	6/27/2012 10:16:45	6/27/2012 10:16:43
Info.plist	Tasks calendar specifications	Macintosh HD\Users\AlsoMISDE\Library\Calendars\E57FCAB7-2DE1-473E-8E98-89A977AFD497.caldav\AD76F056-1DC7-41DA-8A1D-5A5CF25D88A7.calendar	6/27/2012 9:20:55	6/27/2012 10:16:45	6/27/2012 10:16:43
Configuration.plist	Address Book synchronization	Macintosh HD\Users\AlsoMISDE\Library\ Application Support\AddressBook\Sources\ B1A97D73-4C47-4768-8CA8-3EDF5301EF96	6/27/2012 9:21:21	6/27/2012 10:17:05	6/27/2012 9:21:21
AlsoMISDE.plist	Linked identities between computer account and Apple ID	Macintosh HD\private\var\db\dslocal\nodes\Default\users	6/27/2012 9:21:21	7/2/2012 5:53:10	6/27/2012 9:21:21
com.apple.iLifePhotoStream.plist	PhotoStream properties	Macintosh HD\Users\AlsoMISDE\Library\Preferences	6/27/2012 9:24:05	6/27/2012 10:17:02	6/27/2012 9:24:05
Accounts.plist	Mailbox properties: account name, date of last sync	Macintosh HD\Users\AlsoMISDE\Library\Mail\V2\MailData	6/27/2012 10:16:43	6/27/2012 10:16:43	6/27/2012 10:16:43
MobileMeAccounts.plist	Apple account and data class (application) properties	Macintosh HD\Users\AlsoMISDE\Library\Preferences	6/27/2012 10:17:06	6/27/2012 10:17:06	6/27/2012 10:17:06

BackupTOC.plist	Table of Contents properties	Macintosh HD\Users\AlsoMISDE\Library\Mail\V2\MailData	6/27/2012 10:17:13	6/27/2012 10:17:13	6/27/2012 10:17:13
com.apple.mail.plist	Mail properties	Macintosh HD\Users\AlsoMISDE\Library\Preferences	6/27/2012 10:21:55	6/27/2012 10:21:55	6/27/2012 10:21:55
ZCALENDARUSERADDRESS	Calendar user identity: Apple ID, person ID	Macintosh HD\Users\AlsoMISDE\Library\Calendars\CalendarCache\tables\ZcalendarUserAddress\rows_0000000_0000002	n/a	n/a	n/a
ZACCOUNT	Calendar account information: server URL string	Macintosh HD\Users\AlsoMISDE\Library\Calendars\CalendarCache\tables\ZACCOUNT\rows_0000000_0000000	n/a	n/a	n/a