

Sarah Edwards | @iamevtwin | oompa@csh.rit.edu | mac4n6.com

Ubiquity Forensics: Your iCloud and You

whoami

By Day – Test Engineer at Parsons Corporation

By Night – SANS Author & Instructor

- FOR518 – Mac Forensic Analysis (sans.org/course/mac-forensic-analysis)
- Upcoming classes:
 - October – Singapore
 - November – San Francisco
 - February – Anaheim
 - Anytime - OnDemand

At All Times - Mac Fan Girl

The latest and greatest version of this presentation is available at: mac4n6.com

Scope

iCloud Basics

Storage and Acquisition of iCloud Data

Synced Preferences

Application Data

iCloud Basics

iCloud Basics

Ubiquity = “Everything Everywhere”

What is “Everything”?

- Documents
- Email
- Contacts
- Preference Configurations
- Photos
- Calendar
- Notes
- Reminders
- and more!



iCloud Basics

Ubiquity = “Everything Everywhere” - OS X & iOS

The image displays two side-by-side screenshots of the iCloud settings interface.

OS X iCloud Settings:

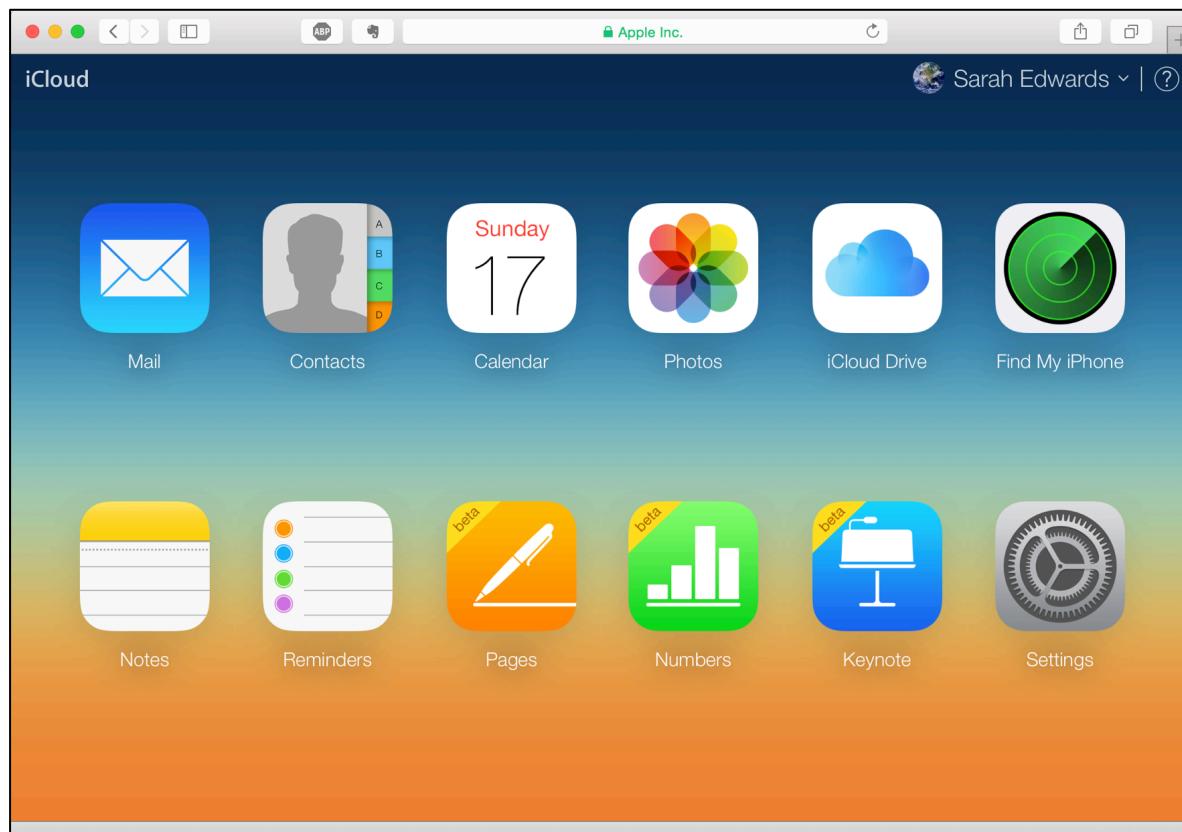
- User Profile:** Shows a circular profile picture of Earth and the account details "Sarah Edwards" and "oompa@csh.rit.edu".
- Services:** A list of services with checkboxes:
 - iCloud Drive (checked)
 - Photos (checked)
 - Mail (checked)
 - Contacts (checked)
 - Calendars (checked)
 - Reminders (checked)
 - Safari (checked)
 - Notes (checked)
- Storage:** Displays "You have 5 GB of iCloud storage." with a progress bar showing "1.43 GB" used.
- Buttons:** "Sign Out", "Photos and Videos", "Backup", and "Manage...".

iOS iCloud Settings:

- Header:** Shows signal strength, battery level (97%), and the time (6:31 PM).
- User Profile:** Shows the same account details as the OS X version.
- Services:** A list of services with toggle switches:
 - iCloud Drive (On)
 - Photos (On)
 - Mail (Off)
 - Contacts (On)
 - Calendars (On)
 - Reminders (On)
 - Safari (On)

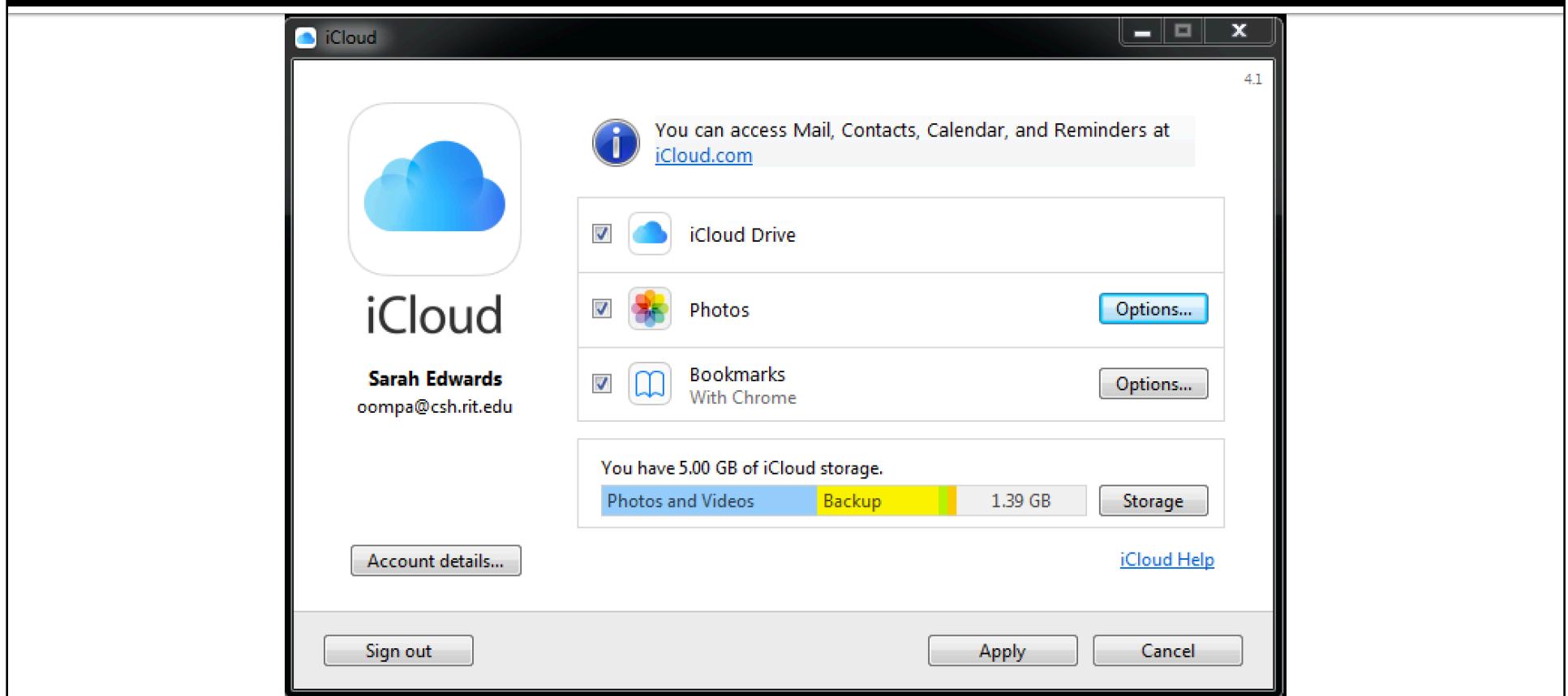
iCloud Basics

Ubiquity = “Everything Everywhere” – iCloud.com



iCloud Basics

Ubiquity = “Everything Everywhere” - Windows



iCloud Basics

iCloud Accounts

- Email: Apple ID
- Numeric: iCloud “Person ID”
- Vetted Account Aliases
 - Email Addresses
 - Phone Numbers
- Credentials
 - Password
 - Two-factor
 - Token
- Storage
 - 5GB Data Free
 - Can purchase up to 1TB

iCloud Basics System Configuration

OS X

- ~/Library/Application Support/iCloud/Accounts

iOS

- /private/var/mobile/Library/Preferences/com.apple.udb.plist

Windows

- HKEY_CURRENT_USER\Software\Apple Inc.\Internet Services

Getting to the iCloud Data

Getting to the iCloud Data – Storage

On Disk

- OS X - Disk Image
- Windows - Disk Image
- iOS
 - Physical Acquisition - Jailbreak required for iPhone4S generations and newer.
 - or SSH
 - or “Physical Logical” (Elcomsoft EIFT, “save user files to .tar archive”)

iCloud.com

- Various Download Tools

Downloadable Storage Types

- iCloud Backups (iTunes-ish Backups)
- iCloud Data (Mobile Documents, Photos, Synced Preferences, etc)

Getting to the iCloud Data - iCloud Backup Download Tools

Sketchy

- **iPhone Backup Extractor** - <http://www.iphonebackupextractor.com/>
- **iPhone Data Recovery** - <http://www.iskysoft.com/data-recovery/how-to-download-icloud-backup.html>

Slightly Less Sketchy?

- **iLoot** - <https://github.com/hackappcom/iloot>

Forensic

- **Elcomsoft Phone Breaker (EPPB)** - <https://www.elcomsoft.com/eppb.html>

Getting to the iCloud Data

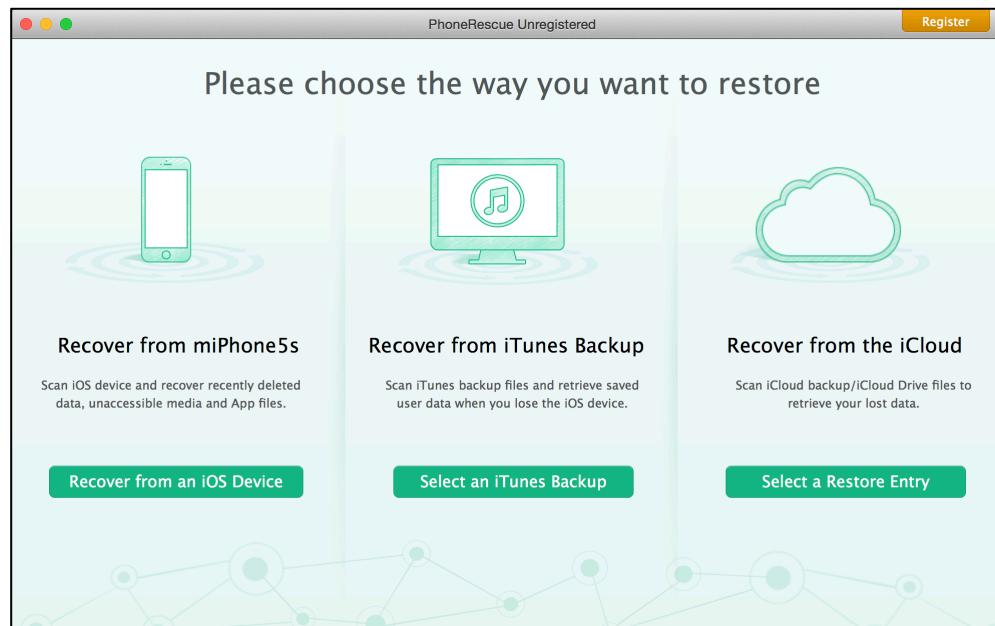
iCloud Backup Download Tools

- iPhone Backup Extractor – Download Software
 - Apple ID Required
 - No Two-factor Support
 - Choice of Mac or Windows
 - Choice of Home or Pro Versions
 - \$30, \$70

The screenshot shows the iPhone Backup Extractor website. At the top, there's a navigation bar with links for Product tour, Free download, Buy now, Help & support, and a language switcher. Below the navigation is a section for "Free iPhone Backup Extractor download" with a "Free download" button. To the right, there are two pricing options: "Home Edition" at \$29.95 and "Pro Edition" at \$69.95, both offering 1 year of support and upgrades included. A comparison table highlights features like recovering files from iTunes and iCloud backups, CSV export, encrypted backup support, and access to expert support. The table shows the Home Edition has limited support for some features, while the Pro Edition offers full support. Below the table, three steps are outlined: 1. Allow iPhone Backup Extractor to be installed to your computer (User Account Control dialog). 2. Follow the setup wizard to install the software (Phone Device Installer dialog). 3. iPhone Backup Extractor reads iTunes and iCloud backups on your PC (Software interface showing file lists). On the right side, there's a "Thank you for downloading our software!" message, social sharing icons (Facebook, Twitter, LinkedIn), and a "Hey, We're" contact button. The footer includes a "100% MONEY BACK GUARANTEE" badge and payment method logos (RapidSSL, PayPal).

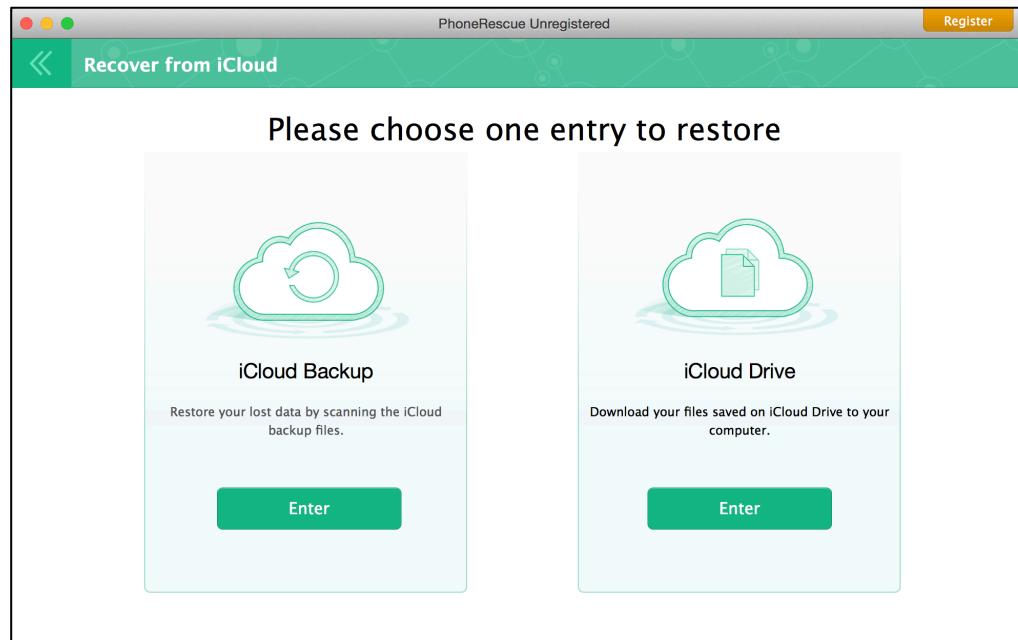
Getting to the iCloud Data iCloud Backup Download Tools

- iPhone Backup Extractor – “Recover from the iCloud”



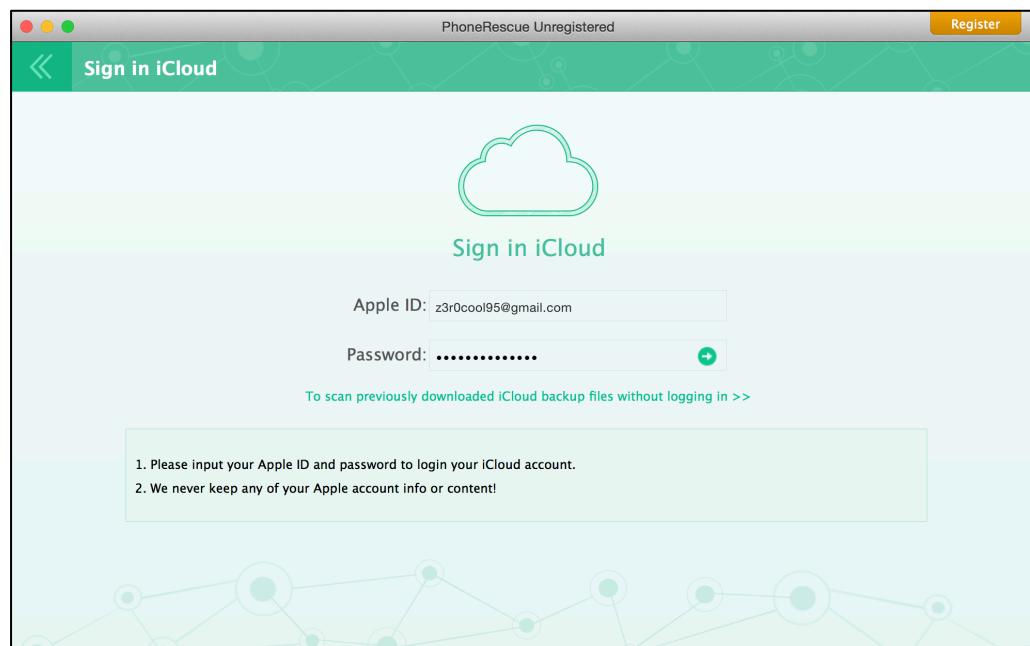
Getting to the iCloud Data iCloud Backup Download Tools

- iPhone Backup Extractor – iCloud Backup or iCloud Drive?



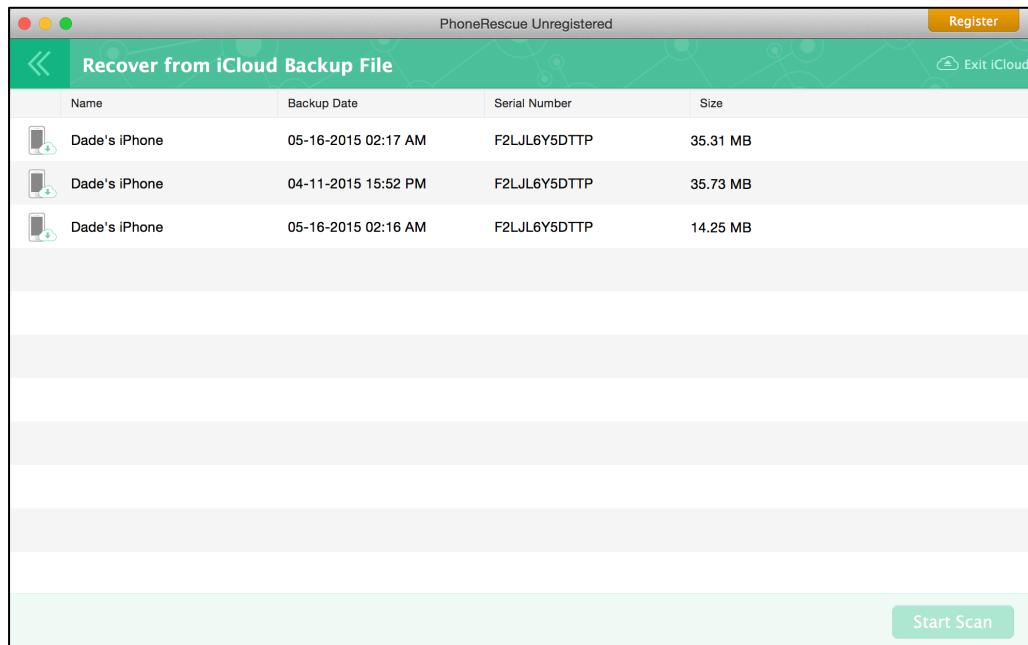
Getting to the iCloud Data iCloud Backup Download Tools

- iPhone Backup Extractor – Login Apple ID (iCloud) Credentials



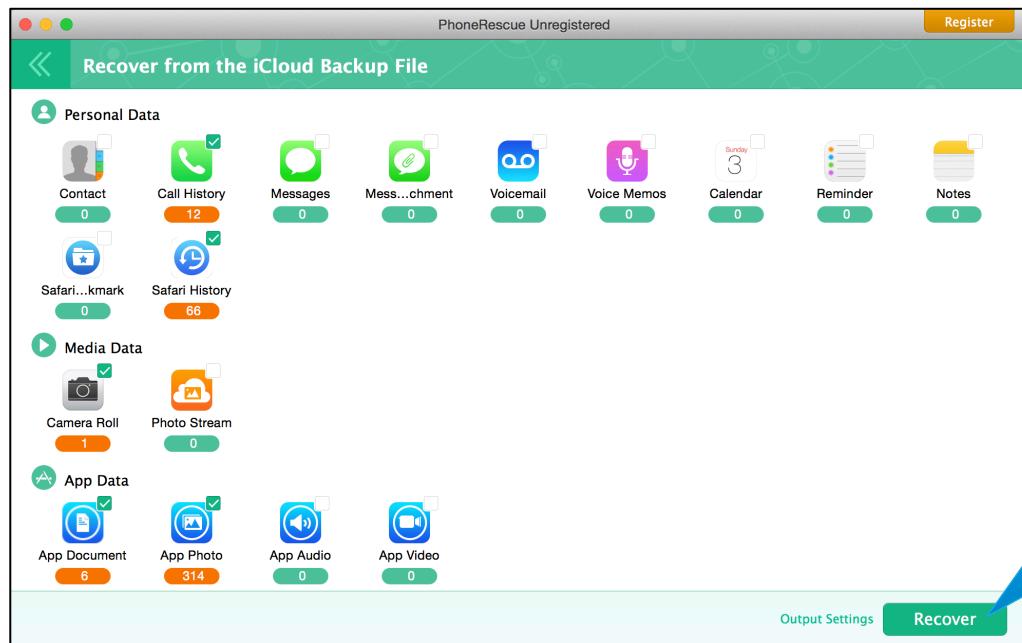
Getting to the iCloud Data iCloud Backup Download Tools

- iPhone Backup Extractor – Multiple iCloud Backups Available



Getting to the iCloud Data iCloud Backup Download Tools

- iPhone Backup Extractor – Downloaded! Now what?



What a
tease...Press to
give them \$\$\$!
:(

Getting to the iCloud Data

iCloud Backup Download Tools

- iLoot:
 - Apple ID Required
 - No Two-factor Support
 - Python! Run Anywhere
 - Command-line Only
 - Open Source
 - Free!

```
word:iloot-master oompa$ python iloot.py -h
usage: iloot [-h] [--threads THREADS] [--output OUTPUT] [--combined]
              [--snapshot SNAPSHOT] [--itunes-style]
              [--item-types ITEM_TYPES [ITEM_TYPES ...]] [--domain DOMAIN]
              apple_id password

positional arguments:
  apple_id            Apple ID
  password           Password

optional arguments:
  -h, --help          show this help message and exit
  --threads THREADS   Download thread pool size
  --output OUTPUT      Output Directory
  --combined          Do not separate each snapshot into its own folder
  --snapshot SNAPSHOT  Only download data the snapshot with the specified ID.
                       Negative numbers will indicate relative position from
                       newest backup, with -1 being the newest, -2 second,
                       etc.
  --itunes-style       Save the files in a flat iTunes-style backup, with
                      mangled names
  --item-types ITEM_TYPES [ITEM_TYPES ...], -t ITEM_TYPES [ITEM_TYPES ...]
                      Only download the specified item types. Options
                      include address_book, calendar, sms, call_history,
                      voicemails, movies and photos. E.g., --types sms
                      voicemail
  --domain DOMAIN, -d DOMAIN
                      Limit files to those within a specific application
                      domain
```

Getting to the iCloud Data iCloud Backup Download Tools

- iLoot – Support for multiple snapshots (backups)

```
word:iloot-master oompa$ python iloot.py z3r0cool95@gmail.com [REDACTED]
Working with z3r0cool95@gmail.com :
Output directory : output
Available Devices: 1
===[ 0 ]===
    UDID: 1d6929153d69581341badb0ac1d1765dd8bdf10d
    Device: iPhone 5
    Size: 40M
    LastUpdate: 2015-05-16 01:16:58
Downloading backup 1d6929153d69581341badb0ac1d1765dd8bdf10d to output/1d6929153d69581341badb0ac1d1765dd8bdf10d
Got OTA Keybag
Available Snapshots: 17
Listing snapshot 1...
    Shifting offset: 5000
Files in snapshot 1604
Downloading 1604 files due to filter
    HomeDomain      output/1d6929153d69581341badb0ac1d1765dd8bdf10d/snapshot_1/HomeDomain/Library/Preferences/com.apple.AppSupport.plist
    HomeDomain      output/1d6929153d69581341badb0ac1d1765dd8bdf10d/snapshot_1/HomeDomain/Library/Preferences/com.apple.certui.plist
    HomeDomain      output/1d6929153d69581341badb0ac1d1765dd8bdf10d/snapshot_1/HomeDomain/Library/Preferences/com.apple.iapd.plist
    HomeDomain      output/1d6929153d69581341badb0ac1d1765dd8bdf10d/snapshot_1/HomeDomain/Library/Preferences/com.apple.keyboard.plist
    HomeDomain      output/1d6929153d69581341badb0ac1d1765dd8bdf10d/snapshot_1/HomeDomain/Library/Preferences/com.appleUIKit.plist
```

Getting to the iCloud Data

iCloud Backup Download Tools

- iLoot – Analysis
 - Saved by Device UDID
 - Each Snapshot (Backup) is named
 - Snapshots may be full or incremental (1 full, 16 & 17 incremental)
 - Analysis is similar to iTunes Backups, may also choose iTunes Backup format for iCloud Backups

```
word:1d6929153d69581341badb0ac1d1765dd8bdf10d oompa$ ls -l
total 0
drwxr-xr-x  45 oompa  staff  1530 May 17 20:12 snapshot_1
drwxr-xr-x  20 oompa  staff   680 May 17 20:12 snapshot_16
drwxr-xr-x  14 oompa  staff   476 May 17 20:12 snapshot_17
```

Getting to the iCloud Domain iCloud Backup Download

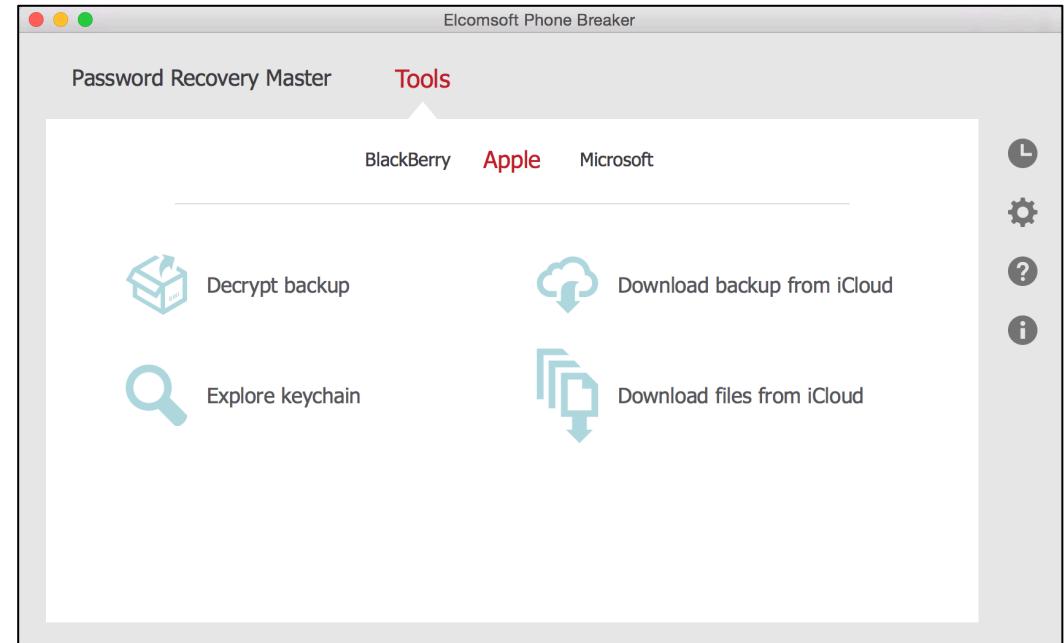
- iLoot – Analysis – Organized by Domain
 - AppDomain
 - CameraRollDomain
 - DatabaseDomain
 - HomeDomain
 - KeyboardDomain
 - KeychainDomain
 - ManagedPreferencesDomain
 - MediaDomain
 - RootDomain
 - SystemPreferencesDomain
 - WirelessDomain

```
word:snapshot_1 oompa$ pwd
/Users/oompa/Documents/iLoot_normaloutput/1d6929153d69581341badb0ac1d1765dd8bdf10d/snapshot_1
word:snapshot_1 oompa$ ls
AppDomain-com.amazon.Amazon
AppDomain-com.apple.Maps
AppDomain-com.apple.mobilemail
AppDomain-com.apple.mobilesafari
AppDomain-com.apple.store.Jolly
AppDomain-com.burbn.instagram
AppDomain-com.fandango.fandango
AppDomain-com.google.Drive
AppDomain-com.google.GoogleMobile
AppDomain-com.mlb.AtTheBallpark
AppDomain-com.newtoyinc.NewWordsWithFriendsFree
AppDomain-com.rei.eCommerce
AppDomain-com.shazam.Shazam
AppDomain-com.united.UnitedCustomerFacingiPhone
AppDomain-com.waze.iphone
AppDomainGroup-group.com.waze.iphone.TodayExtensionSharingDefaults
AppDomainPlaceholder-com.amazon.Amazon
AppDomainPlaceholder-com.apple.store.Jolly
AppDomainPlaceholder-com.burbn.instagram
AppDomainPlaceholder-com.fandango.fandango
AppDomainPlaceholder-com.google.Drive
AppDomainPlaceholder-com.google.GoogleMobile
AppDomainPlaceholder-com.googleMaps
AppDomainPlaceholder-com.mlb.AtTheBallpark
AppDomainPlaceholder-com.newtoyinc.NewWordsWithFriendsFree
AppDomainPlaceholder-com.pandora
AppDomainPlaceholder-com.rei.eCommerce
AppDomainPlaceholder-com.shazam.Shazam
AppDomainPlaceholder-com.toyopagroup.picaboo
AppDomainPlaceholder-com.united.UnitedCustomerFacingiPhone
AppDomainPlaceholder-com.waze.iphone
CameraRollDomain
DatabaseDomain
HealthDomain
HomeDomain
KeyboardDomain
KeychainDomain
ManagedPreferencesDomain
MediaDomain
RootDomain
SystemPreferencesDomain
WirelessDomain
```

Getting to the iCloud Data

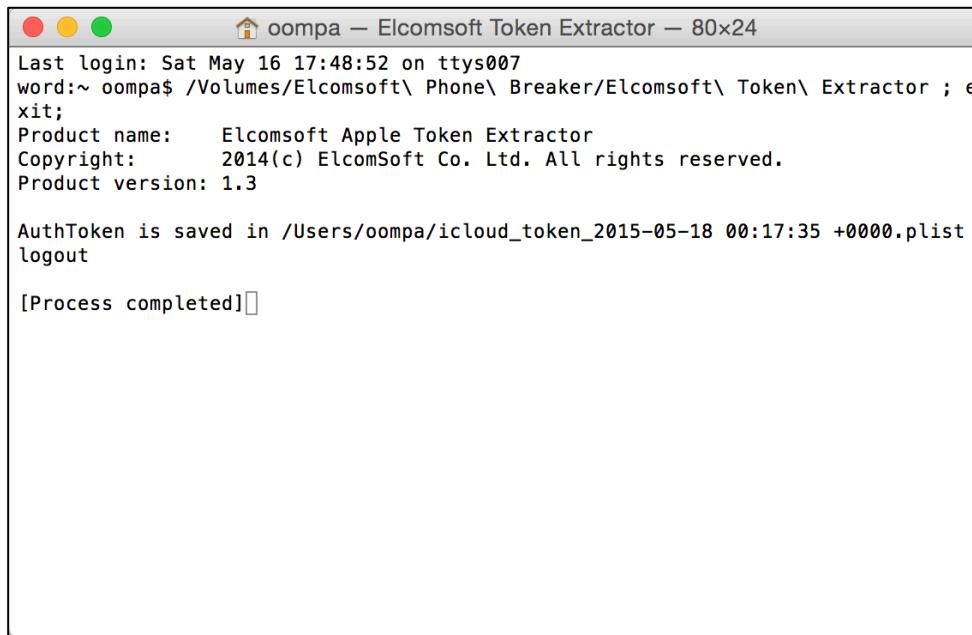
iCloud Backup Download Tools

- Elcomsoft Phone Breaker (EPPB)
 - “Forensic”
 - Apple ID or Authentication Token
 - Support for Two-factor
 - Mac or Windows
 - Professional or Forensic Editions
 - iCloud Backups & iCloud Files (iCloud Drive)
 - \$200, \$800



Getting to the iCloud Data iCloud Backup Download Tools

- Elcomsoft Phone Breaker (EPPB) – Authentication Token Extraction



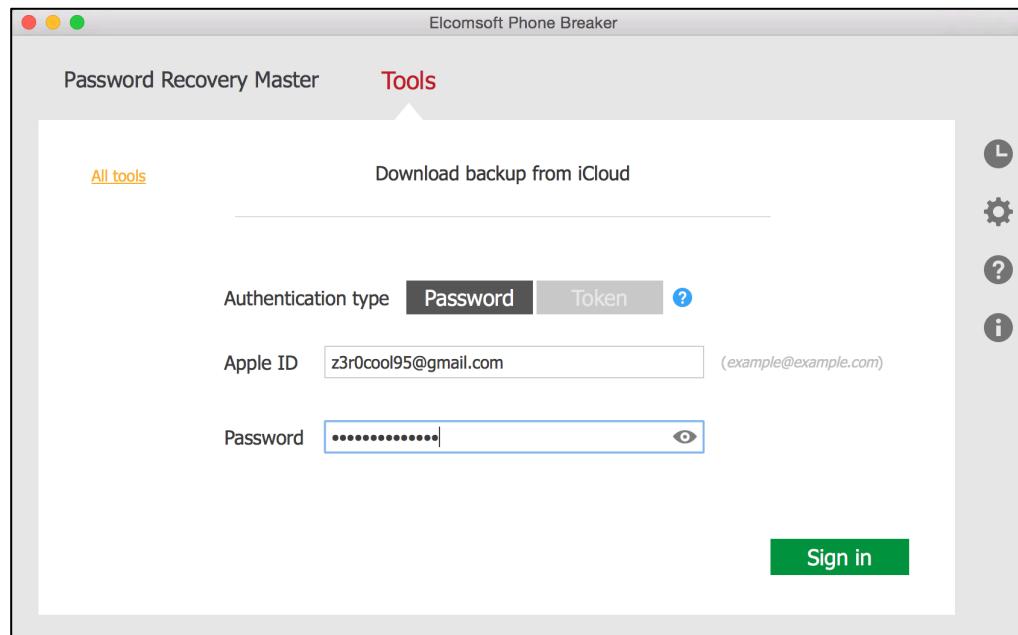
```
Last login: Sat May 16 17:48:52 on ttys007
word:~ oompa$ /Volumes/Elcomsoft\ Phone\ Breaker/Elcomsoft\ Token\ Extractor ; exit;
Product name: Elcomsoft Apple Token Extractor
Copyright: 2014(c) ElcomSoft Co. Ltd. All rights reserved.
Product version: 1.3

AuthToken is saved in /Users/oompa/icloud_token_2015-05-18 00:17:35 +0000.plist
logout

[Process completed]
```

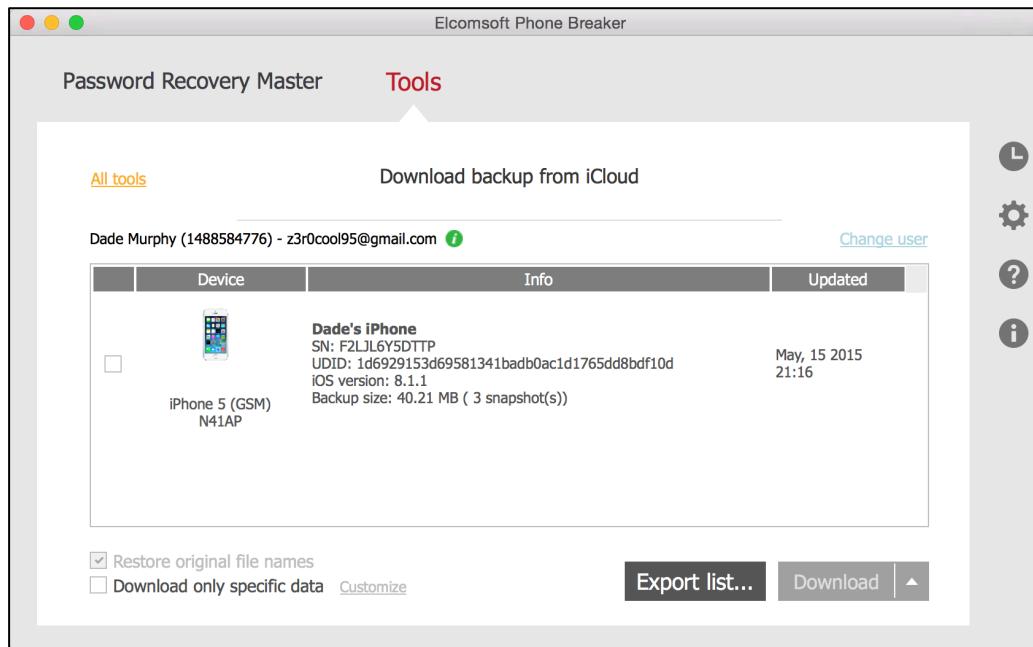
Getting to the iCloud Data iCloud Backup Download Tools

- Elcomsoft Phone Breaker (EPPB) – Apple ID or Authentication Token



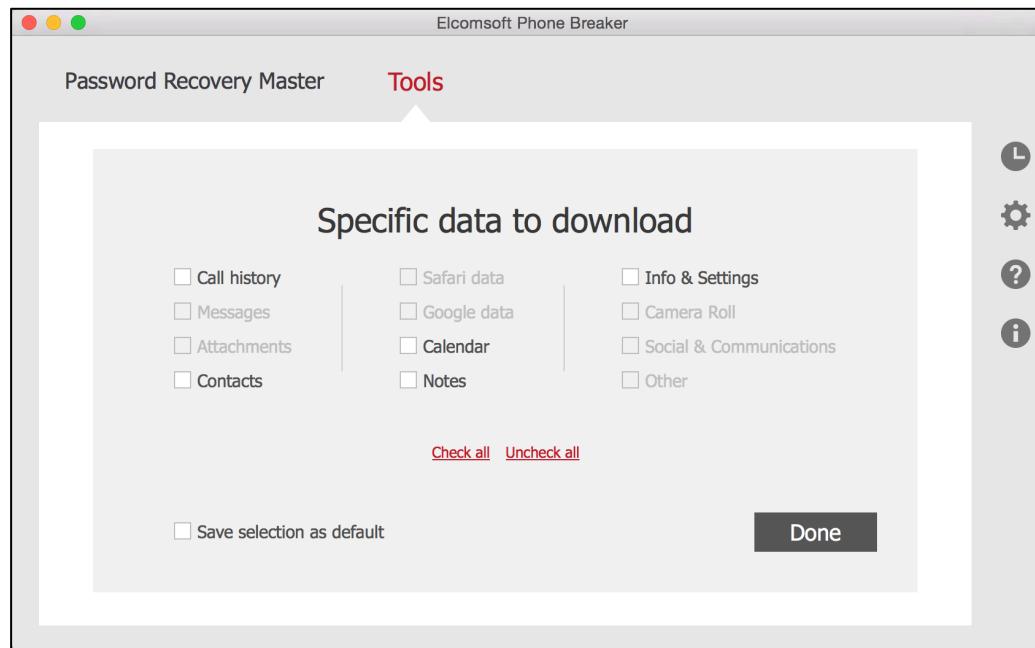
Getting to the iCloud Data iCloud Backup Download Tools

- Elcomsoft Phone Breaker (EPPB) – Choose a Device/Backup



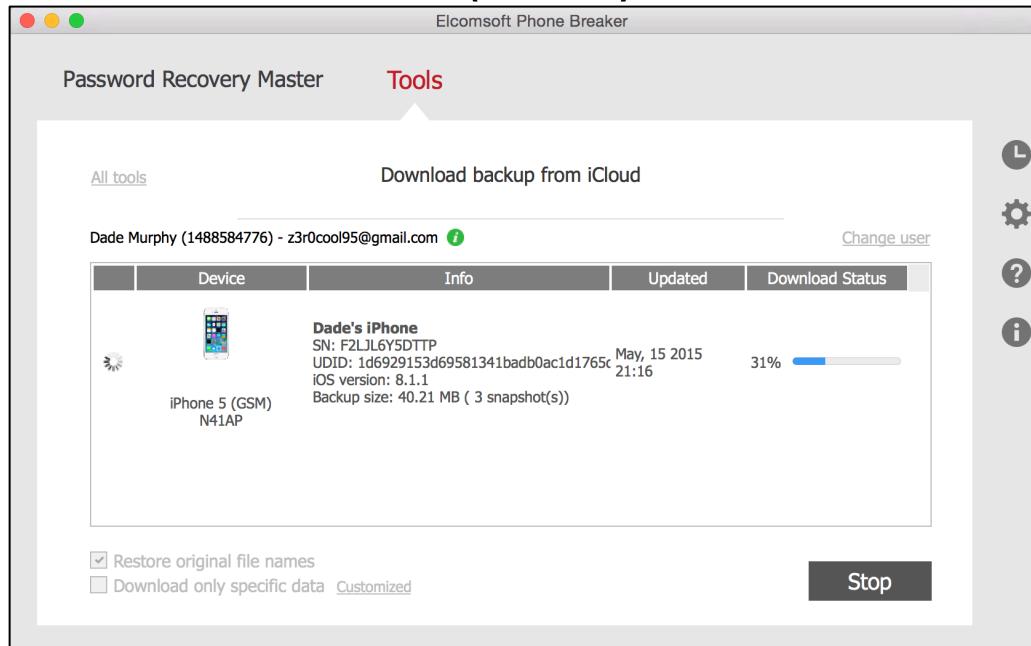
Getting to the iCloud Data iCloud Backup Download Tools

- Elcomsoft Phone Breaker (EPPB) – Choose What to Download (Demo will limit choices)



Getting to the iCloud Data iCloud Backup Download Tools

- Elcomsoft Phone Breaker (EPPB) – Download Progress



Getting to the iCloud Data

iCloud Backup Download Tools

- Elcomsoft Phone Breaker (EPPB) – Analysis
 - Uses Device UDID
 - Backups (1, 16, 17) – Uses iTunes Backup output format
 - Normalized Backups ([01]..., [16]..., [17]...) – Uses Domain-based output

```
word:1d6929153d69581341badb0ac1d1765dd8bdf10d oompa$ ls -l
total 0
drwxr-xr-x 190 oompa  staff  6460 May 17 20:20 1
drwxr-xr-x  55 oompa  staff  1870 May 17 20:20 16
drwxr-xr-x  91 oompa  staff  3094 May 17 20:20 17
drwxr-xr-x   11 oompa  staff    374 May 17 20:22 [01][20150207_105700Z] [R]
drwxr-xr-x   11 oompa  staff    374 May 17 20:22 [16][20150220_202544Z] [R]
drwxr-xr-x   11 oompa  staff    374 May 17 20:22 [17][20150515_211658Z] [R]
```

Synced Preferences

Applications Synced Preferences

- Contains synced preferences for:
 - Email
 - Safari
 - WiFi
 - Maps
 - Stocks
 - Weather
 - Messages
- Legacy & Sandboxed Locations
 - ~/Library/SyncedPreferences/
 - ~/Library/Containers/...

```
word:SyncedPreferences oompa$ pwd
/Users/oompa/Library/SyncedPreferences
word:SyncedPreferences oompa$ ls -1
com.appleMaps-com.appleMapsSupport.bookmarks.plist
com.appleMaps-com.appleMapsSupport.history.plist
com.appleSafari-com.appleSafariUserRequests.plist
com.appleSafari-com.appleSafariWebFeedSubscriptions.plist
com.appleSafari.plist
com.applecmfsyncagent.plist
com.applefinder.plist
com.applemail-com.applemail.vipsenders.plist
com.apple.ncplugin.stocks.plist
com.apple.ncplugin.weather.plist
com.applesbd.plist
com.apple.security.cloudkeychainproxy3.plist
com.apple.syncedpreferences.plist
com.apple.wifi.WiFiAgent.plist
icbaccounts.plist
```

Applications - Synced Preferences

Email – Recent Emails

- **OSX:**
 - ~/Library/SyncedPreferences/com.apple.mail-com.apple.mail.recents.plist
 - ~/Library/Containers/com.apple.corerecents.recentsd/Data/Library/SyncedPreferences/recentsd-com.apple.mail.recents.plist
- **iOS:** /private/var/mobile/Library/SyncedPreferences/com.apple.cloudrecents.CloudRecentsAgent-com.apple.mail.recents.plist

Key	Type	Value
▼ Root	Dictionary	(4 items)
versionid	String	FT=-@RU=d8326b9f-4f49-46cb-8e6f-99bb3e963f9b@S=78594
initialsync	Number	2
changecount	Number	491
▼ values	Dictionary	(680 items) 
▶ GP_D42A57A67E5DF4FDB4BDC67B9FF2D9C7	Dictionary	(3 items)
▶ MR_5DA23DA86B5574B5C862872558D6E2C8	Dictionary	(3 items)
▶ MR_1ABCF8ACFDD90B8EA7A46833DEFAA2F4	Dictionary	(3 items)
▶ MR_9CFDBEF0E4FC5C54D4731E49AF12C323	Dictionary	(3 items)
▶ GP_B643BD5AEA804BE04C1ADF43A7F30311	Dictionary	(3 items)
▶ MR_C9DAFF659EDC27A0FA6E8094787A33A7	Dictionary	(3 items)

Applications - Synced Preferences

Email – Recent Emails

- MR – Single Contact
- GP – Group Email

▼ MR_9CFDBEF0E4FC5C54D4731E49AF12C323	Dictionary	(3 items)
▼ value	Dictionary	(6 items)
S	String	com.apple.mail
v	Number	1
n	String	Heather Mahalik
s	String	oompa@csh.rit.edu
a	String	hmahalik@gmail.com
▼ t	Array	(5 items)
Item 0	Date	May 12, 2015, 9:30:38 PM
Item 1	Date	May 10, 2015, 2:40:35 PM
Item 2	Date	May 10, 2015, 2:23:48 PM
Item 3	Date	May 10, 2015, 12:21:41 PM
Item 4	Date	May 6, 2015, 7:52:22 PM
remotevalue	Data	<0179770f bee0021b 000000
timestamp	Number	453,173,438

▼ GP_B643BD5AEA804BE04C1ADF43A7F30311	Dictionary	(3 items)
▼ value	Dictionary	(8 items)
k	String	gr
t	Array	(3 items)
Item 0	Date	Mar 12, 2015, 9:47:43 PM
Item 1	Date	Jul 28, 2014, 5:44:23 PM
Item 2	Date	Jul 27, 2014, 10:26:47 AM
gK	Number	0
S	String	com.apple.mail
v	Number	1
n	String	Rob Lee
s	String	oompa@csh.rit.edu
▼ mrs	Array	(2 items)
▼ Item 0	Dictionary	(3 items)
n	String	Henri van Goethem
a	String	hvangoethem@sans.org
k	String	email
▼ Item 1	Dictionary	(3 items)
n	String	Rob Lee
a	String	rlee@sans.org
k	String	email
remotevalue	Data	<01196a02 3f9b21a 00000
timestamp	Number	447,904,063

Applications - Synced Preferences Email – VIP Senders

- **OS X:**
 - ~/Library/SyncedPreferences/com.apple.mail-com.apple.mail.vipsenders.plist
 - ~/Library/Containers/com.apple.mail/Data/Library/SyncedPreferences/com.apple.mail-com.apple.mail.vipsenders.plist
- **iOS:**
 - /private/var/mobile/Applications/<GUID>/Library/SyncedPreferences/com.apple.mobilemail-com.apple.mail.vipsenders.plist
 - /private/var/mobile/Containers/Data/Application/<GUID>/Library/SyncedPreferences/com.apple.mobilemail-com.apple.mail.vipsenders.plist

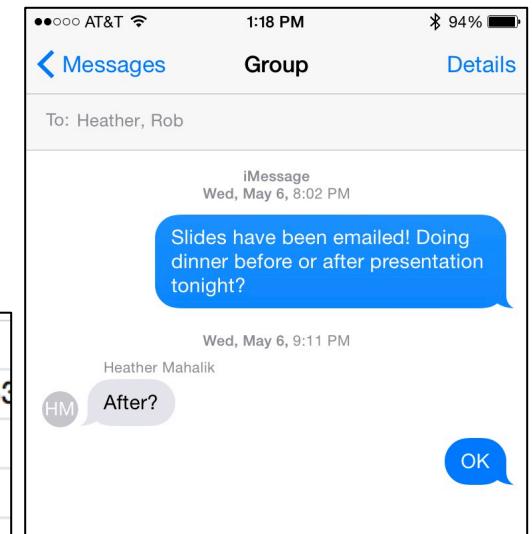
Key	Type	Value
▼ Root	Dictionary	(4 items)
versionid	String	FT--@RU=d8326b9f-4f49-46cb-8e6f-99bb3e963f9b@S=78647
initialsync	Number	4
changecount	Number	7
▼ values	Dictionary	(1 item)
▼ VIP_C23ECE34-264F-4134-9F23-4EA4B80FD2AE	Dictionary	(3 items)
▼ value	Dictionary	(3 items)
n	String	Rob Lee
▼ a	Array	(1 item)
Item 0	String	rlee@sans.org
v	Number	1
remotevalue	Data	<01090809 fc0f081b 00000000 62706c69 73743030 d3010203
timestamp	Number	453,513,212

Applications - Synced Preferences

Messages – “Recent” Messages

- **OS X:** ~/Library/Containers/com.apple.corerecents.recentsd/Data/Library/SyncedPreferences/recentsd-com.apple.messages.recents.plist
- **iOS:** /private/var/mobile/Library/SyncedPreferences/com.apple.cloudrecents.CloudRecentsAgent-com.apple.messages.recents.plist

Root		Dictionary	(4 items)
versionid		String	FT=-@RU=d83
initialsync		Number	2
changeccount		Number	1,227
values		Dictionary	(198 items)
▶ GP_BB031C1D39B13CB975BD2B5D1B704D65		Dictionary	(3 items)
▶ MR_C93D9B19B6118D5D9BF1622CABBE5FE1		Dictionary	(3 items)
▶ MR_434D0C13A43BD98872E495089BFE5CF5		Dictionary	(3 items)
▶ MR_74589F9321BA59AE3DB18194339BD134		Dictionary	(3 items)



Applications - Synced Preferences Messages – “Recent” Messages

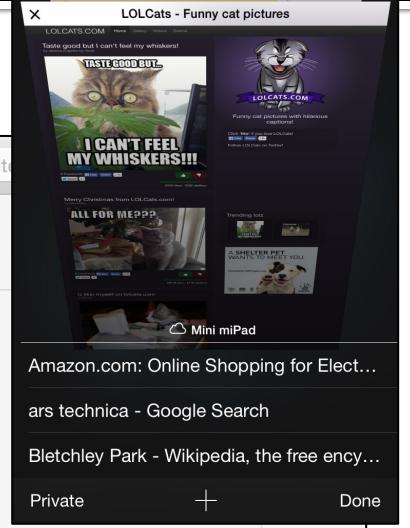
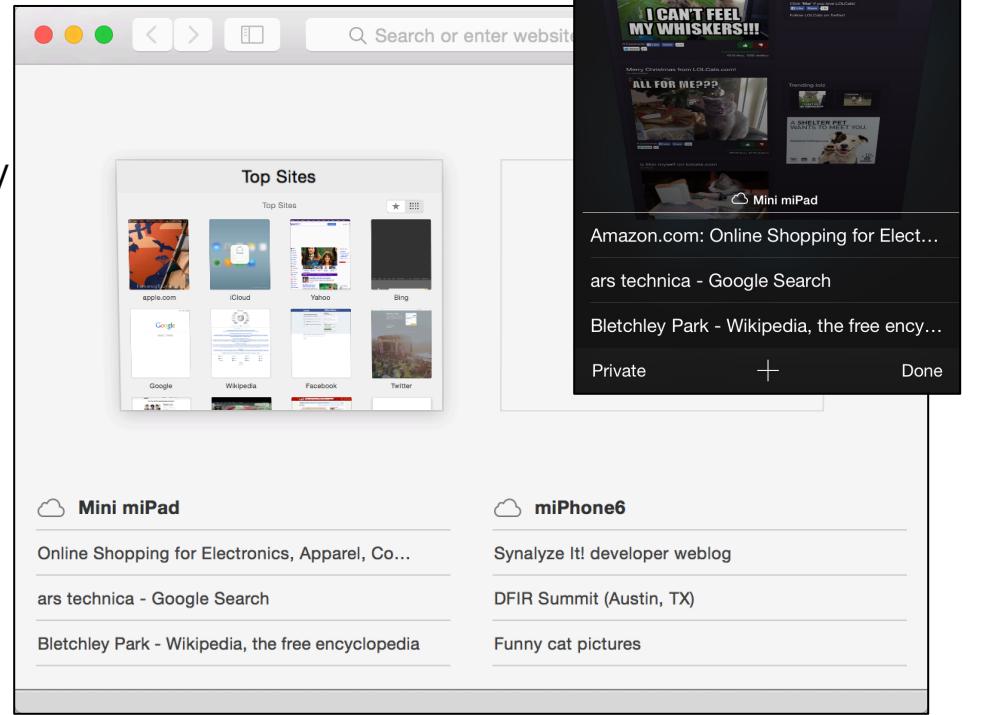
- MR = Single Recipient, GR = Group

▼ MR_39388D82C87706207AB1B3FE1AE5F8F5	Dictionary	(3 items)
▼ value	Dictionary	(7 items)
k	String	p
▼ t	Array	(5 items)
Item 0	Date	Sep 13, 2014, 4:00:19 PM
Item 1	Date	Sep 12, 2014, 11:22:51 AM
Item 2	Date	Sep 12, 2014, 11:21:33 AM
Item 3	Date	Sep 12, 2014, 10:52:41 AM
Item 4	Date	Sep 12, 2014, 10:21:13 AM
S	String	com.apple.MobileSMS
v	Number	1
n	String	Lee Whitfield
a	String	+1 [REDACTED]
s	String	iMessage:oompa@csh.rit.edu
remotevalue	Data	<01394800 d3d9c419 000000
timestamp	Number	432,331,219

▼ GP_5F06D656864AB82329C27640B6781513	Dictionary	(3 items)
▼ value	Dictionary	(6 items)
k	String	gr
gK	Number	0
▼ t	Array	(1 item)
Item 0	Date	May 6, 2015, 8:02:16 PM
mrs	Array	(2 items)
▼ Item 0	Dictionary	(3 items)
n	String	Rob Lee
a	String	+1 [REDACTED]
k	String	phone
▼ Item 1	Dictionary	(3 items)
n	String	Heather Mahalik
a	String	+1 [REDACTED]
k	String	phone
v	Number	1
S	String	com.apple.MobileSMS
remotevalue	Data	<01385300 08e3fa1a 0000
timestamp	Number	452,649,736

Applications - Synced Preferences Safari – Synced Devices

- OS X: ~/Library/SyncedPreferences/com.apple.Safari.plist
- iOS:
 - /private/var/mobile/Applications/<GUID>/Library/SyncedPreferences/com.apple.mobilesafari.plist
 - /private/var/mobile/Containers/Data/Application/<GUID>/Library/SyncedPreferences/com.apple.mobilesafari.plist



Applications - Synced Preferences

Safari – Synced Tabs

▼ Root	Dictionary	(4 items)
versionid	String	FT=-@RU=d8326b9f-4f49-4e
initialsync	Number	1
changecount	Number	3,248
▼ values	Dictionary	(3 items)
▼ CE3B9EB5-CB56-413F-9077-18CB891FFCA2	Dictionary	(3 items)
▼ value	Dictionary	(3 items)
LastModified	Date	May 17, 2015, 10:17:40 AM
DeviceName	String	Mini miPad
► Tabs	Array	(3 items)
remotevalue	Data	<01b98b00 84da081b 00000
timestamp	Number	453,565,060
► 199EC7F7-49FA-405E-8426-F26FF0EF811F	Dictionary	(3 items)
► 3ED4EF04-31B2-44DC-B303-92F29...	+ -	Dictionary ◂ (3 items)

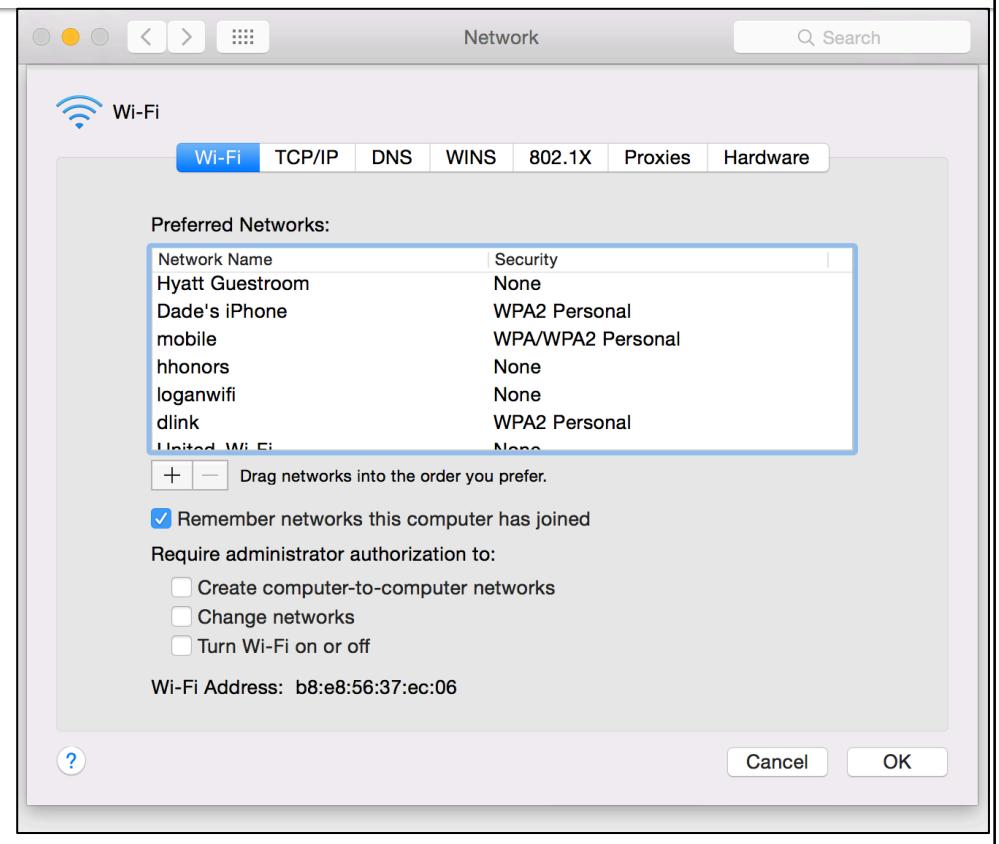
Applications - Synced Preferences

Safari – Synced Tabs

▼ 199EC7F7-49FA-405E-8426-F26FF0EF811F	Dictionary	(3 items)
▼ value	Dictionary	(5 items)
► Capabilities	Dictionary	(1 item)
▼ Tabs	Array	(3 items)
▼ Item 0	Dictionary	(3 items)
Title	String	Synalyze It! developer weblog
URL	String	https://www.synalysis.net/developer-weblog/
UUID	String	81D25DBE-9817-43D9-AB68-A47490EA5D64
▼ Item 1	Dictionary	(3 items)
Title	String	DFIR Summit (Austin, TX)
URL	String	https://www.sans.org/event/digital-forensics-summit-2015
UUID	String	6A911628-65A5-4CCB-8CA3-3128116D6BEA
▼ Item 2	Dictionary	(3 items)
Title	String	LOLCats - Funny cat pictures
URL	String	http://www.lolcats.com/
UUID	String	F7F167CB-BC5B-4CF2-8B10-9A5F82F1F31E
LastModified	Date	May 17, 2015, 10:15:50 AM
DeviceName	String	miPhone6
DictionaryType	String	Device
remotevalue	Data	<01f81b00 16da081b 00000000 62706c69 73743030 d50102
timestamp	Number	453,564,950

Applications - Synced Preferences WiFi – Synced Access Points

- **OS X:** ~/Library/SyncedPreferences/com.apple.wifi.WiFiAgent.plist
- **iOS:** /private/var/mobile/Library/SyncedPreferences/com.apple.wifid.plist



Applications - Synced Preferences

WiFi – Synced Access Points

Key	Type	Value
▼ Root	Dictionary	(4 items)
versionid	String	FT=-@RU=0
initialsync	Number	5
changecount	Number	30
▼ values	Dictionary	(27 items)
► FOR518	Dictionary	(3 items)
► Reagan National WiFi	Dictionary	(3 items)
► Parsons_Visitor	Dictionary	(3 items)
► ASUS	Dictionary	(3 items)
► SJ	Dictionary	(3 items)
► RitzCarlton_Guest	Dictionary	(3 items)
► Marriott_GUEST	Dictionary	(3 items)
► Hyatt Lobby	Dictionary	(3 items)
► scandic_easy	Dictionary	(3 items)

▼ Reagan National WiFi	Dictionary	(3 items)
▼ value	Dictionary	(11 items)
WEP	Boolean	NO
enabled	Boolean	YES
UserDirected	Boolean	NO
added_by	String	miPhone5s
SSID_STR	String	Reagan National WiFi
IS_NETWORK_CUSTOMIZED	Boolean	NO
BSSID	String	0:1c:f6:60:45:30
added_at	String	Feb 9 2014 20:25:23
IS_NETWORK_CONFIGURED	Boolean	NO
IS_NETWORK_EAP	Boolean	NO
AP_MODE	Number	2
remotevalue	Data	<01b94900 576fd91a 00000000>
timestamp	Number	450,457,431

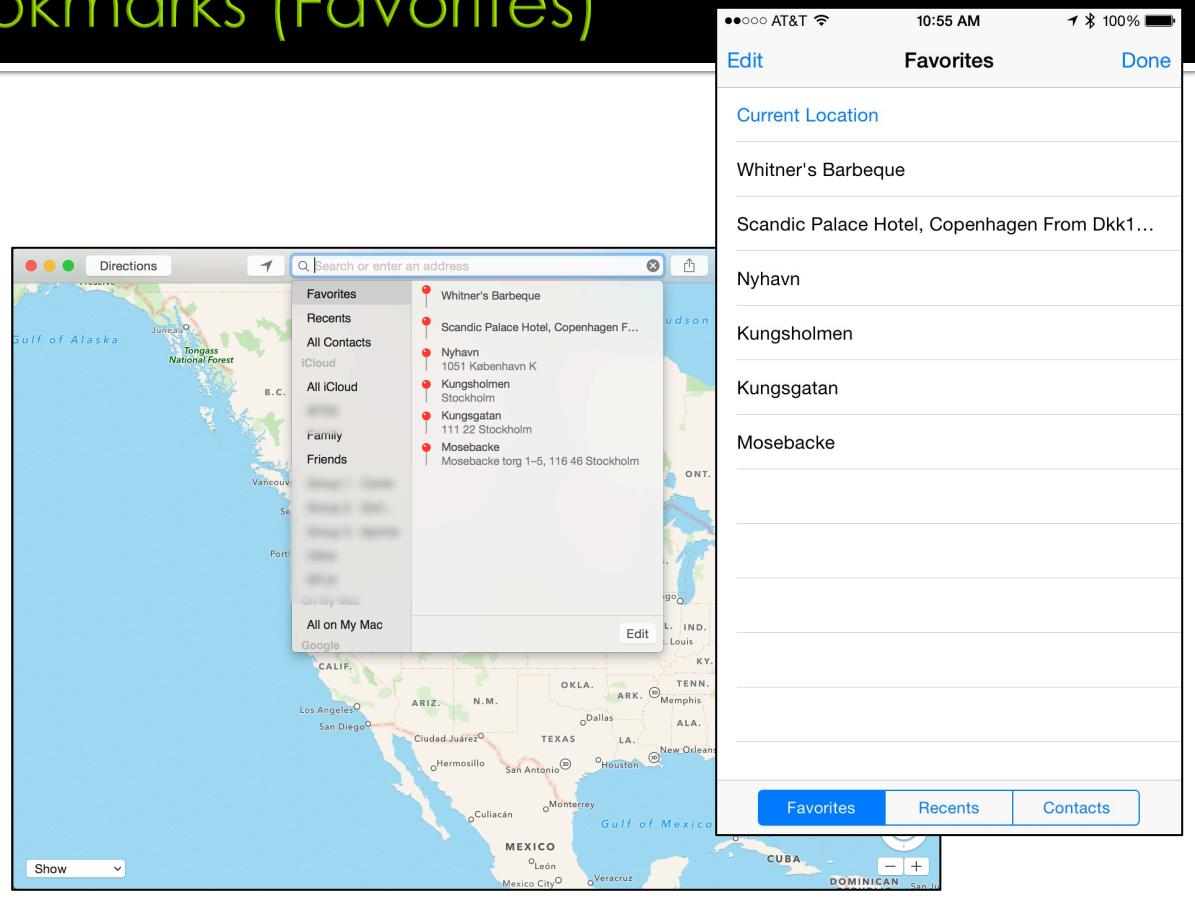
Applications - Synced Preferences Maps – Synced Bookmarks (Favorites)

OS X:

~/Library/SyncedPreferences/
com.appleMaps-
com.appleMapsSupport.bookmarks.plist
~/Library/Containers/com.appleMaps/
Data/Library/SyncedPreferences/
com.appleMaps-
com.appleMapsSupport.bookmarks.plist

iOS:

/private/var/mobile/Library/
SyncedPreferences/com.appleMaps.plist
/private/var/mobile/Containers/Data/
Application/<GUID>/Library/
SyncedPreferences/com.appleMaps-
com.appleMapsSupport.bookmarks.plist



Applications - Synced Preferences Maps – Bookmarks (Favorites)

▼ _sync.bookmarks.item.23D45D96-4D5F-4270-9CE4-38E751F2200A Dictionary (3 items)

 ▼ value

data position remotevalue timestamp	+ - Data Number Data Number	Dictionary (2 items) 400 <01b85000 ce47cf19 00000000 62706c69 73743030 d20 433,014,734
--	--------------------------------------	---

► _sync.bool Untitled

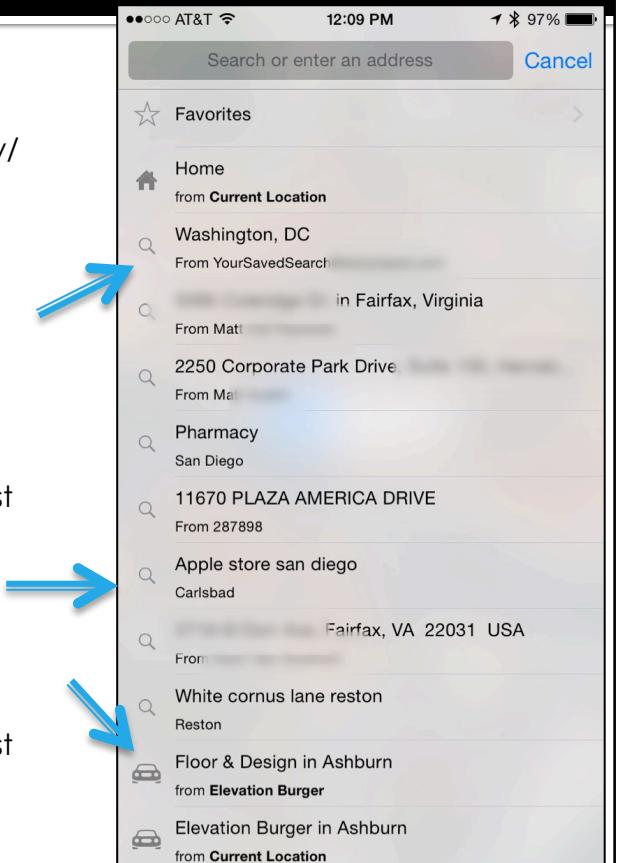
► _sync.vers Go To Offset ↴ Id (Text search)

Save Copy Cut Paste Undo Redo

000 08 01 12 24	32 33 44 34	35 44 39 36	2D 34 44 35	46 2D 34 32	37 30 2D 39	43	...\$23D45D96-4D5F-4270-9C
025 45 34 2D 33	38 45 37 35	31 46 32 32	30 30 41 21	A2 EC 05 F5	A8 7A B9 41	2A	E4-38E751F2200A!.....z.A*
050 A4 02 0A 99	02 12 96 02	18 2D 22 06	4E 79 68 61	76 6E 2A 24	29 A3 EB 2F	F9-".Nyhavn*\$).../.
075 DD D6 4B 40	31 00 00 00	C0 CC 2C 29	40 39 60 22	71 24 24 D7	4B 40 41 00	00	..K@1.....,)@9`"q\$\$..K@A..
100 00 E0 3F 30	29 40 32 AB	01 5A 06 4E	79 68 61 76	6E 5A 11 31	30 35 31 20	4B	..?0)@2..Z.NyhavnZ,1051 K
125 C3 B8 62 65	6E 68 61 76	6E 20 4B 5A	07 44 65 6E	6D 61 72 6B	7A 84 01 0A	07	..benhavn KZ.Denmarkz....
150 44 65 6E 6D	61 72 6B 12	02 44 4B 1A	0E 43 61 70	69 74 61 6C	20 52 65 67	69	Denmark..DK..Capital Regi
175 6F 6E 32 0A	43 6F 70 65	6E 68 61 67	65 6E 3A 04	31 30 35 31	42 07 43 65	6E	on2.Copenhagen:.1051B.Cen
200 74 72 75 6D	72 09 53 6A	C3 A6 6C 6C	61 6E 64 72	06 4E 79 68	61 76 6E 7A	06	trumr.Sj...llandr.Nyhavnz.
225 4E 79 68 61	76 6E 8A 01	0C 4B C3 B8	62 65 6E 68	61 76 6E 20	4B 8A 01 0A	43	Nyhavn...K..benhavn K...C
250 6F 70 65 6E	68 61 67 65	6E 8A 01 08	49 6E 64 72	65 20 42 79	8A 01 07 43	65	openhagen...Indre By...Ce
275 6E 74 72 75	6D 4A 12 09	5A F5 1E FE	01 D7 4B 40	11 9E 59 0C	92 83 2E 29	40	ntrumJ...Z.....K@..Y....)@
300 68 00 70 D9	32 7A 06 4E	79 68 61 76	6E A0 06 E1	81 EA B4 02	CA 0C 05 65	6E	h.p.2z.Nyhavn.....en
325 2D 55 53 D2	0C 05 65 6E	2D 55 53 1A	06 4E 79 68	61 76 6E			-US...en-US..Nyhavn

Applications - Synced Preferences Maps – Recent Addresses & Locations

- **Recent Addresses (Extracted from Mail emails – “From...”)**
 - OS X: ~/Library/Containers/com.apple.corerecents.recentsd/Data/Library/SyncedPreferences/recentsd-com.apple.corerecents.map-locations.plist
 - iOS: /private/var/mobile/Library/SyncedPreferences/com.apple.cloudrecents.CloudRecentsAgent-com.apple.corerecents.map-locations.plist
- **Recent Locations & Searches**
- **OS X:**
 - ~/Library/SyncedPreferences/com.appleMaps-com.appleMapsSupport.history.plist
 - /Users/oompa/Library/Containers/com.appleMaps/Data/Library/SyncedPreferences/com.appleMaps-com.appleMapsSupport.history.plist
- **iOS:**
 - /private/var/mobile/Library/SyncedPreferences/com.appleMaps-com.appleMaps.recents.plist
 - /private/var/mobile/Containers/Data/Application/<GUID>/Library/SyncedPreferences/com.appleMaps-com.appleMaps.recents.plist
 - /private/var/mobile/Containers/Data/Application/<GUID>/Library/SyncedPreferences/com.appleMaps-com.appleMapsSupport.history.plist



Applications - Synced Preferences Maps – Recent Addresses

- Extracted from Mail emails – “From...”

▼ MR_F8EA2DAFA7D6877F5B232D00534B0797558A5D6C	Dictionary	(3 items)
▼ value	Dictionary	(7 items)
k	String	m
▼ t	Array	(4 items)
Item 0	Date	Apr 26, 2015, 9:58:31 AM
Item 1	Date	Apr 26, 2015, 7:25:33 AM
Item 2	Date	Apr 15, 2015, 8:26:02 PM
Item 3	Date	Apr 15, 2015, 7:35:59 PM
▼ m	Dictionary	(4 items)
▼ corerecents:from	Dictionary	(3 items)
kind	String	email
address	String	listings@redfin.com
displayName	String	Redfin
corerecents:event-time	Date	Apr 26, 2015, 7:23:45 AM
corerecents:reference-url	String	message:%3Cdata-listingAlerts-20150424_1041_740ed27991d0e463fd3fc
corerecents:subject	String	Status change on 5035 25TH St SOUTH; New Hot Home on 3103 19TH St
S	String	com.apple.mobilemail
v	Number	1
a	String	5035 25TH St SOUTH
w	Number	5
remotevalue	Data	<01384800 8726ed1a 00000000 62706c69 73743030 d7010203 04050607
timestamp	Number	451,749,511

Applications - Synced Preferences Maps – Recent Locations & Searches

The screenshot shows a debugger interface with a memory dump of a recent location entry. The entry is identified by the key `_sync.history.item.DA2200A8-AC38-4BB3-BFC9-8DE91FA5E914`. The value is a dictionary containing the following fields:

- `data`: Data (hex value: <08011224 44413232 30304138 2d414333 382d3442)
- `position`: Number (decimal value: 452,996,812.218939)
- `remotevalue`: Data (hex value: <01384800 cc2e001b 00000000 62706c69 73743030)
- `timestamp`: Number (decimal value: 452,996,812)

A blue arrow points from the text "Recent Locations & Searches" in the title bar down to the `data` field of the entry.

The memory dump window shows the following data:

Address	Value	Description
000	08 01 12 24 44 41 32 32 30 30 41 38 2D 41 43 33 38 2D 34 42	...\$DA2200A8-AC38-4B
020	42 33 2D 42 46 43 39 2D 38 44 45 39 31 46 41 35 45 39 31 34	B3-BFC9-8DE91FA5E914
040	19 63 0C 38 CC 2E 00 BB 41 21 63 0C 38 CC 2E 00 BB 41 32 3B	.c.8....A!c.8....A2;
060	0A 08 50 68 61 72 6D 61 63 79 12 09 53 61 6E 20 44 69 65 67	..Pharmacy..San Dieg
080	6F 22 24 29 00 00 90 EB DE 58 40 40 31 00 00 4C 38 C8 4A 5D	o"\$).....X@@1..L8.J]
100	C0 39 00 00 AA B2 CC 5C 40 40 41 00 00 8A F5 37 49 5D C0	.9.....\@@A....7I].

Applications - Synced Preferences Weather

- OS X:
 - ~/Library/Containers/com.apple.ncplugin.weather/Data/Library/SyncedPreferences/com.apple.ncplugin.weather.plist
 - ~/Library/SyncedPreferences/com.apple.ncplugin.weather.plist
- iOS:
 - /private/var/mobile/Applications/<GUID>/Library/SyncedPreferences/com.apple.weather.plist
 - /private/var/mobile/Containers/Data/Application/<GUID>/Library/SyncedPreferences/com.apple.weather.plist



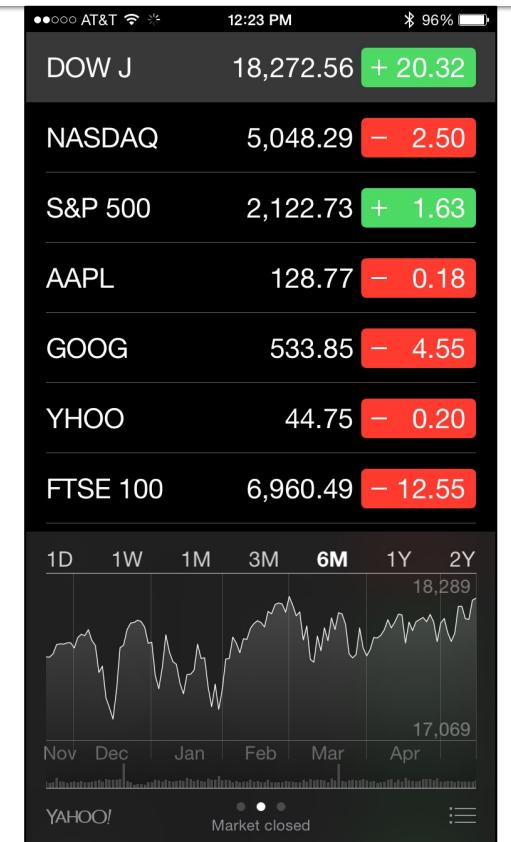
Applications - Synced Preferences Weather – Synced Cities

▼ values		Dictionary	(2 items)
► CloudCities		Dictionary	(3 items)
▼ CloudCities_v2.0		Dictionary	(3 items)
▼ value		Array	(8 items)
► Item 0		Dictionary	(3 items)
▼ Item 1		Dictionary	(3 items)
CityName	String	Gloversville	
Latitude	Number	43.0499992370605	
Longitude	Number	-74.3499984741211	
▼ Item 2		Dictionary	(3 items)
CityName	String	Cleveland	
Latitude	Number	41.5	
Longitude	Number	-81.6900024414062	
▼ Item 3		Dictionary	(3 items)
CityName	String	San Francisco	
Latitude	Number	37.75	
Longitude	Number	-122.440002441406	



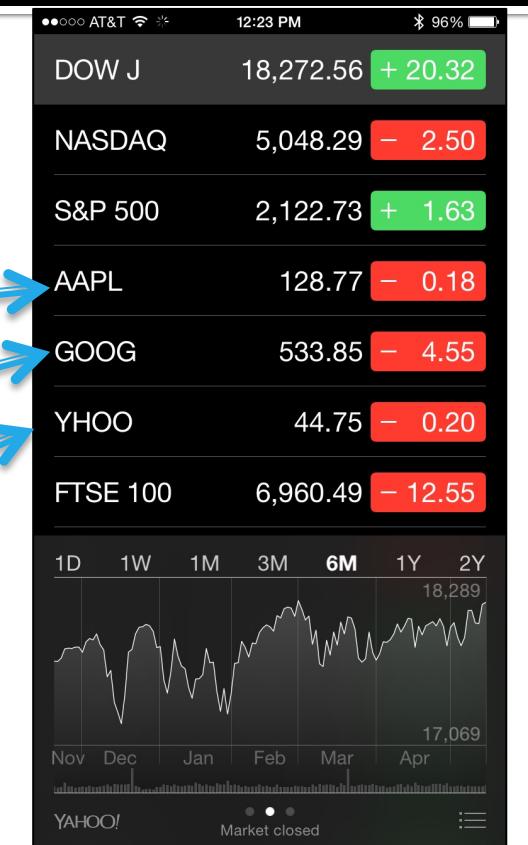
Applications - Synced Preferences Stocks

- OS X:
 - ~/Library/Containers/com.apple.ncplugin.stocks/Data/Library/SyncedPreferences/com.apple.ncplugin.stocks.plist
 - ~/Library/SyncedPreferences/com.apple.ncplugin.stocks.plist
- iOS:
 - /private/var/mobile/Library/SyncedPreferences/com.apple.stocks.plist



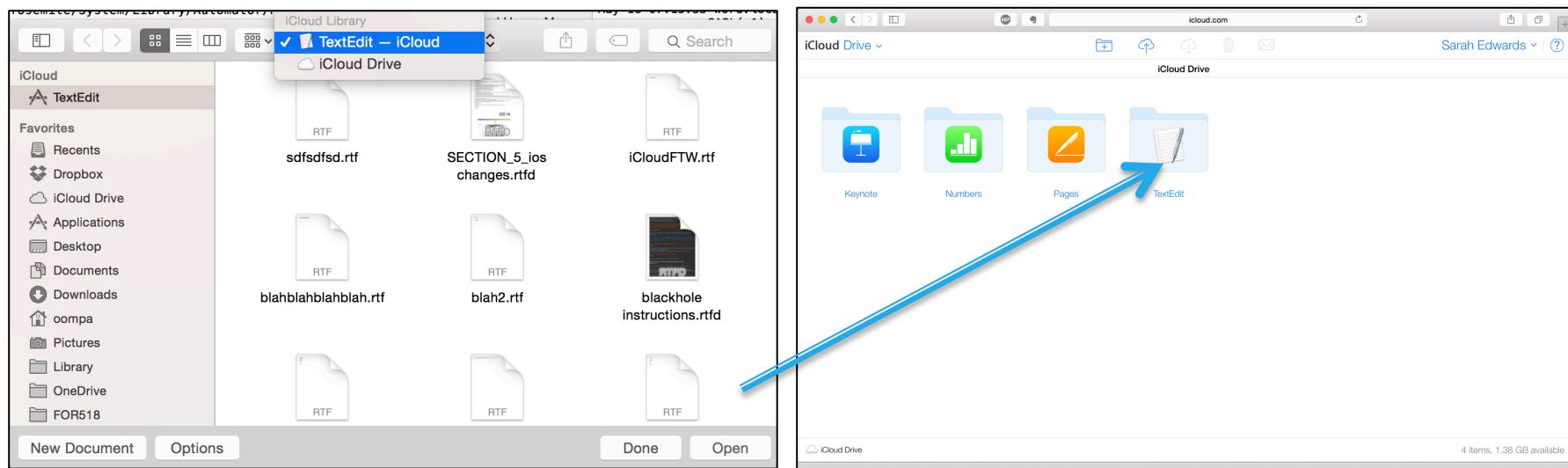
Applications - Synced Preferences Stocks – Synced Stock Symbols

▼ stocks	Dictionary	(3 items)
▼ value	Array	(15 items)
► Item 0	Dictionary	(3 items)
► Item 1	Dictionary	(3 items)
► Item 2	Dictionary	(2 items)
▼ Item 3	Dictionary	(3 items)
symbol	String	AAPL
companyName	String	Apple Inc.
exchange	String	NASDAQ
▼ Item 4	Dictionary	(3 items)
symbol	String	GOOG
companyName	String	Google Inc.
exchange	String	NASDAQ
▼ Item 5	Dictionary	(3 items)
symbol	String	YHOO
companyName	String	Yahoo! Inc.
exchange	String	NASDAQ

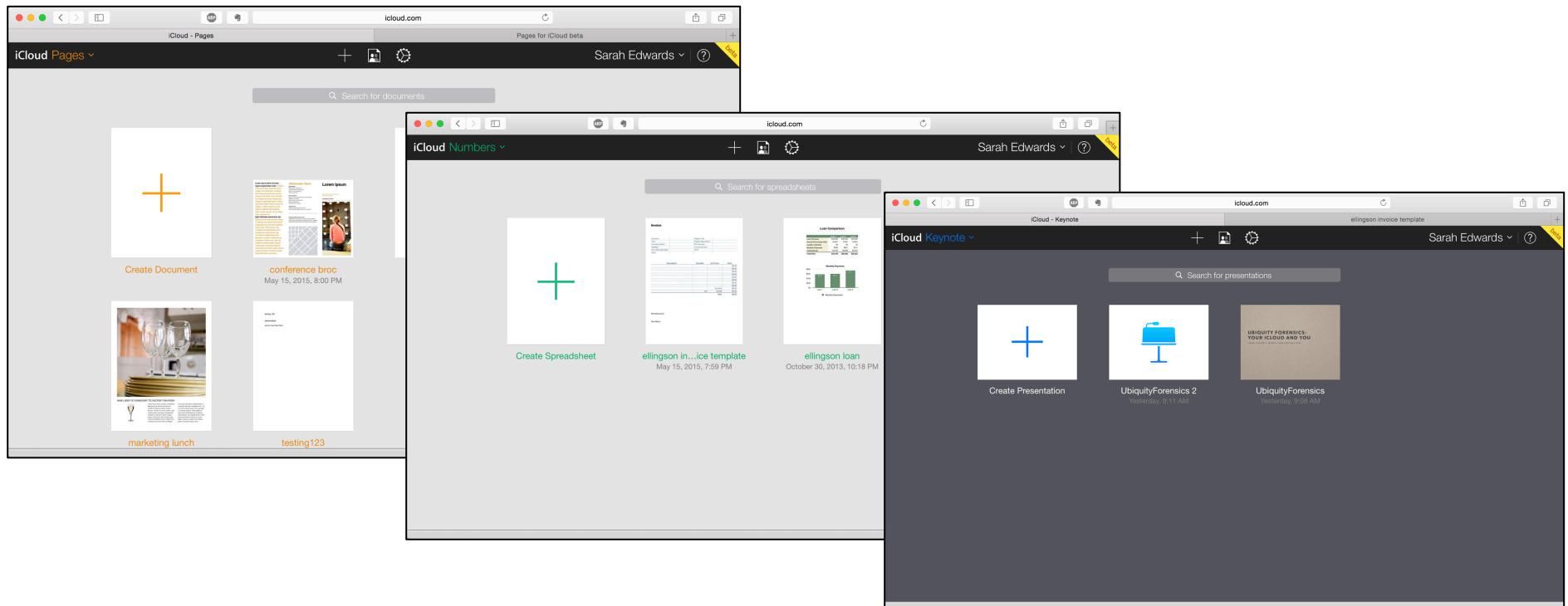


Application Data

Applications Documents



Applications Documents



Applications – Documents iWork & TextEdit – Mobile Documents

Pages

- ~/Library/Mobile Documents/com~apple~Pages/

Keynote

- ~/Library/Mobile Documents/com~apple~Keynote/

Numbers

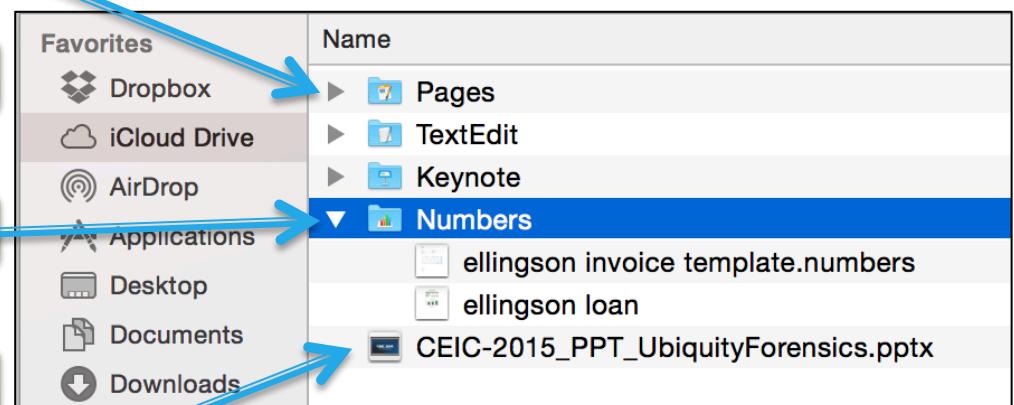
- ~/Library/Mobile Documents/com~apple~Numbers/

TextEdit

- ~/Library/Mobile Documents/com~apple~TextEdit/

Other

- ~/Library/Mobile Documents/com~apple~CloudDocs/



Applications – Documents iWork &TextEdit – Mobile Documents

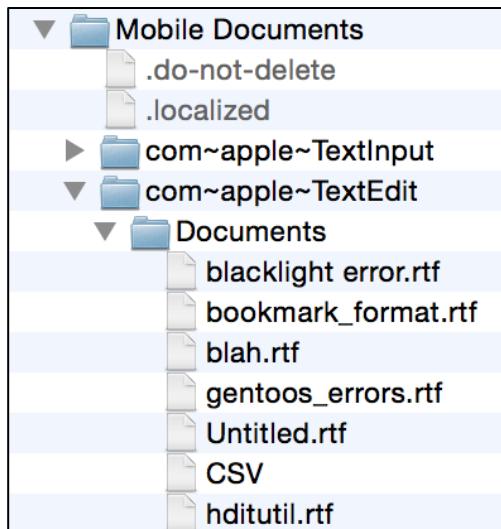
```
word:com~apple~Numbers oompa$ pwd
/Users/oompa/Library/Mobile Documents/com~apple~Numbers
word:com~apple~Numbers oompa$ tree .
.
└── Documents ←
    ├── ellingson invoice template.numbers
    │   ├── Data
    │   ├── Index.zip
    │   ├── Metadata
    │   │   ├── BuildVersionHistory.plist
    │   │   ├── DocumentIdentifier
    │   │   └── Properties.plist
    │   ├── preview-micro.jpg
    │   ├── preview-web.jpg
    │   └── preview.jpg
    ├── ellingson loan.numbers-tef
    │   ├── Previews
    │   │   └── preview.jpg
    │   ├── index.numbers
    │   │   └── 0469B7680B6EC9620097893A00000000.chrtshr
    │   ├── Contents
    │   │   └── PkgInfo
    │   ├── QuickLook
    │   │   └── Thumbnail.jpg
    │   ├── buildVersionHistory.plist
    │   ├── index.xml.gz
    │   ├── preview-micro.jpg
    │   └── preview-web.jpg
    └── iWorkPreviews
        ├── ellingson invoice template.jpg
        └── ellingson loan.jpg
10 directories, 17 files
```

- com~apple~Numbers (& Keynote, Pages, & TextEdit)
 - “Documents” Directory
 - iWorkPreviews Directory (iWork Only)
- com~apple~CloudDocs
 - No “Documents” Directory

```
word:Mobile Documents oompa$ cd com~apple~CloudDocs/
word:com~apple~CloudDocs oompa$ pwd
/Users/oompa/Library/Mobile Documents/com~apple~CloudDocs
word:com~apple~CloudDocs oompa$ tree .
.
└── CEIC-2015_PPT_UbiquityForensics.pptx
0 directories, 1 file
```

Applications – Documents iWork & TextEdit – Mobile Documents on iOS

- iOS: /private/var/mobile/Library/Mobile Documents/



```
miPhone5s:/private/var/mobile/Library/Mobile Documents root# pwd
/private/var/mobile/Library/Mobile Documents
miPhone5s:/private/var/mobile/Library/Mobile Documents root# ls -l
total 0
drwxr-xr-x 3 mobile mobile 102 Nov 16 2013 82J93X7T25~com~apple~mobileiphoto
drwxr-xr-x 3 mobile mobile 102 Feb 19 2014 8YE23NZS57~com~kayak~travel
drwxr-xr-x 3 mobile mobile 102 Dec 10 2013 com~apple~Automator
drwxr-xr-x 4 mobile mobile 204 Feb 18 17:43 com~apple~Keynote
drwxr-xr-x 3 mobile mobile 102 Nov 5 2013 com~apple~Notes
drwxr-xr-x 4 mobile mobile 204 Feb 18 17:43 com~apple~Numbers
drwxr-xr-x 5 mobile mobile 238 Feb 18 17:43 com~apple~Pages
drwxr-xr-x 3 mobile mobile 102 Nov 5 2013 com~apple~Preview
drwxr-xr-x 3 mobile mobile 102 Nov 5 2013 com~apple~TextEdit
drwxr-xr-x 4 mobile mobile 136 Sep 28 2013 com~apple~TextInput
drwxr-xr-x 3 mobile mobile 102 Nov 5 2013 com~apple~finder
drwxr-xr-x 4 mobile mobile 136 Nov 5 2013 com~apple~mail
drwxr-xr-x 4 mobile mobile 136 Nov 5 2013 com~apple~shoebox
drwx----- 3 mobile mobile 102 Nov 5 2013 com~apple~system~spotlight
```

Applications – Documents iWork &TextEdit – Mobile Documents on iOS 8

- Follows same structure
- However...
- Hidden plist files
- <document_name>.icloud
- Theories
 - Files had yet to be downloaded to device?
 - Pointer Records?
 - Image acquired in strange state?

The screenshot shows a file browser interface with a sidebar and a main content area. The sidebar on the left lists categories like 'Mobile Documents' and 'Documents'. The main content area displays a list of files with their names and last modified dates. A blue box highlights a folder named 'Documents' which contains several RTF files. A blue arrow points from this highlighted folder down to a table of metadata at the bottom.

	Type	Value
Root	Dictionary	(3 items)
NSURLFileTypeKey	String	NSURLFileTypeRegular
NSURLFileSizeKey	Number	306
NSURLNameKey	String	testing123.rtf

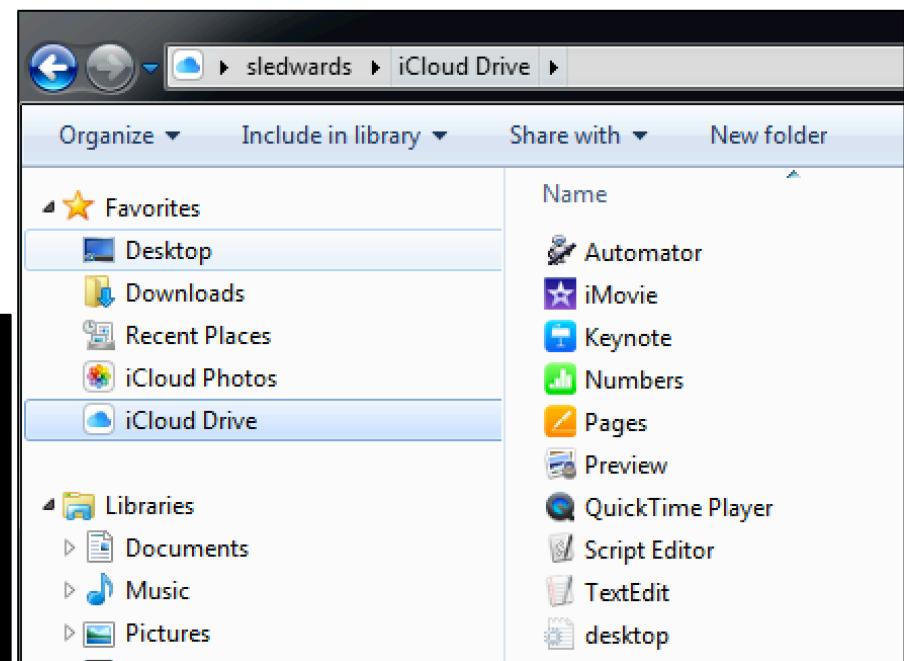
Applications – Documents iWork &TextEdit – Mobile Documents on Windows

- Similar directory structure:
 - com~apple~KeyNote
(Pages, Numbers,
TextEdit)

```
C:\Users\sledwards\iCloudDrive>dir
Volume in drive C has no label.
Volume Serial Number is 6A71-81DC

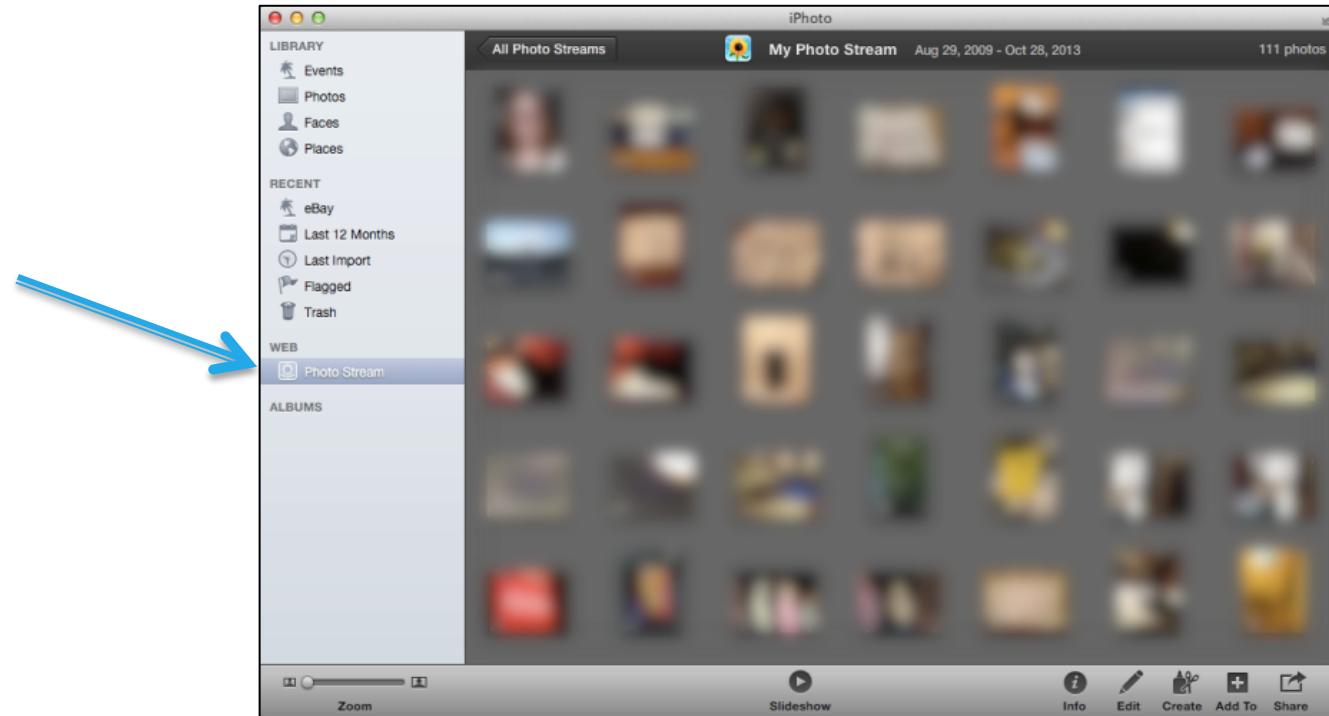
Directory of C:\Users\sledwards\iCloudDrive

05/16/2015  05:02 PM    <DIR>          .
05/16/2015  05:02 PM    <DIR>          ..
05/17/2015  07:56 PM    <DIR>        com~apple~Automator
05/16/2015  05:03 PM    <DIR>        com~apple~Keynote
05/16/2015  05:03 PM    <DIR>        com~apple~Numbers
05/17/2015  08:36 PM    <DIR>        com~apple~Pages
05/17/2015  07:56 PM    <DIR>        com~apple~Preview
05/17/2015  07:56 PM    <DIR>        com~apple~QuickTimePlayerX
05/17/2015  07:56 PM    <DIR>        com~apple~ScriptEditor2
05/16/2015  05:03 PM    <DIR>        com~apple~TextEdit
05/16/2015  05:02 PM    <DIR>        F6266T9T75~com~apple~iMovie
                           0 File(s)              0 bytes
                           11 Dir(s)  32,827,887,616 bytes free
```



Applications Photos – iPhoto (Legacy Application)

- OS X - Legacy Location w/ Old iPhoto App:
- ~/Library/Application Support/iLifeAssetManagement/



Applications Photos – iPhoto (Legacy Application)

- OS X - Legacy Location w/ Old iPhoto App:
 - ~/Library/Application Support/iLifeAssetManagement/
 - Photo Metadata – iLifeAssetManagement.db
 - Only stores data about iCloud related photos.
(Other photo data found in iPhoto Library files.)

```
bash-3.2# pwd
/Users/sledwards/Library/Application Support/iLifeAssetManagement
bash-3.2# tree -L 2 .
.
├── DataModelVersion.plist
├── iLifeAssetManagement.db
└── iLifeAssetManagement.db-journal
.
├── assets
│   ├── pub
│   ├── sub
│   ├── sub-shared
│   └── watch
└── state
    ├── albumshare
    ├── config
    ├── del
    ├── mmcs
    ├── perf
    ├── pub
    ├── share
    └── sub
```

Applications Photos – iPhoto (Legacy Application)

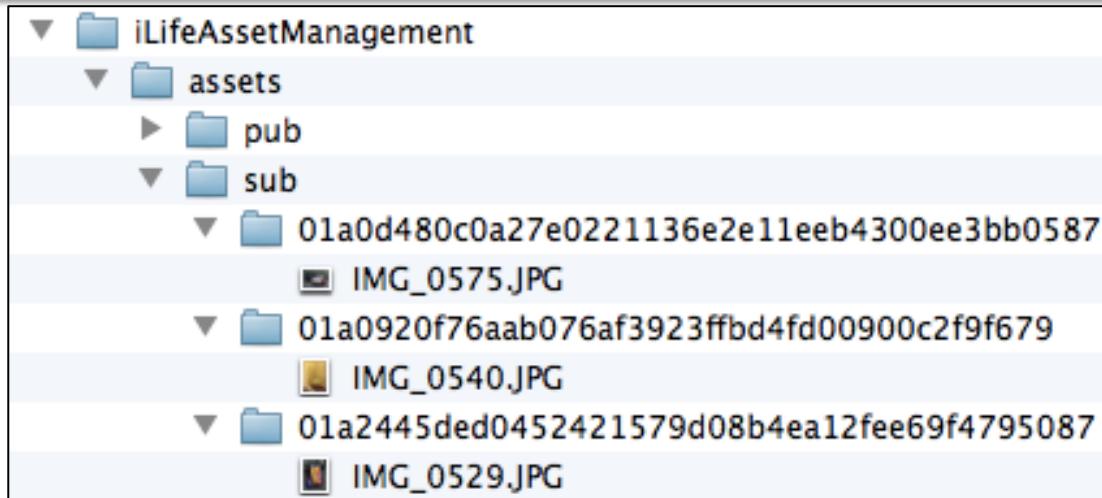
- OS X – iLifeAssetManagement.db
- SQLite Database
- Contains iCloud photo metadata in AMAsset table:
 - Photo UUID
 - iCloud Person ID
 - Timestamps (Downloaded, Modified, Created)
 - Height/Width
 - Filename
 - File Size
 - Device UDID

Enter Field Values	
1. modelId (integer)	9
2. uuid (varchar)	01bff16f98b22720b2a937d606910dfb6d1414b096
3. personId (varchar)	247
4. downloadState (integer)	2
5. downloadDate (timestamp)	392499346.488727
6. height (integer)	2448
7. width (integer)	3264
8. filename (varchar)	IMG_0505.JPG
9. type (varchar)	public.jpeg
10. size (integer)	2381946
11. deviceid (varchar)	d42205699e3962ff2e626649f7a71c91a58165d2
12. modificationDate (timestamp)	391118468
13. creationDate (timestamp)	391118468.461391
14. sourceLibraryId (varchar)	Null
15. sourceUuid (varchar)	Null
16. sha1HashKey (varchar)	Null
17. properties (blob)	Null

Applications Photos – iPhoto (Legacy Application)

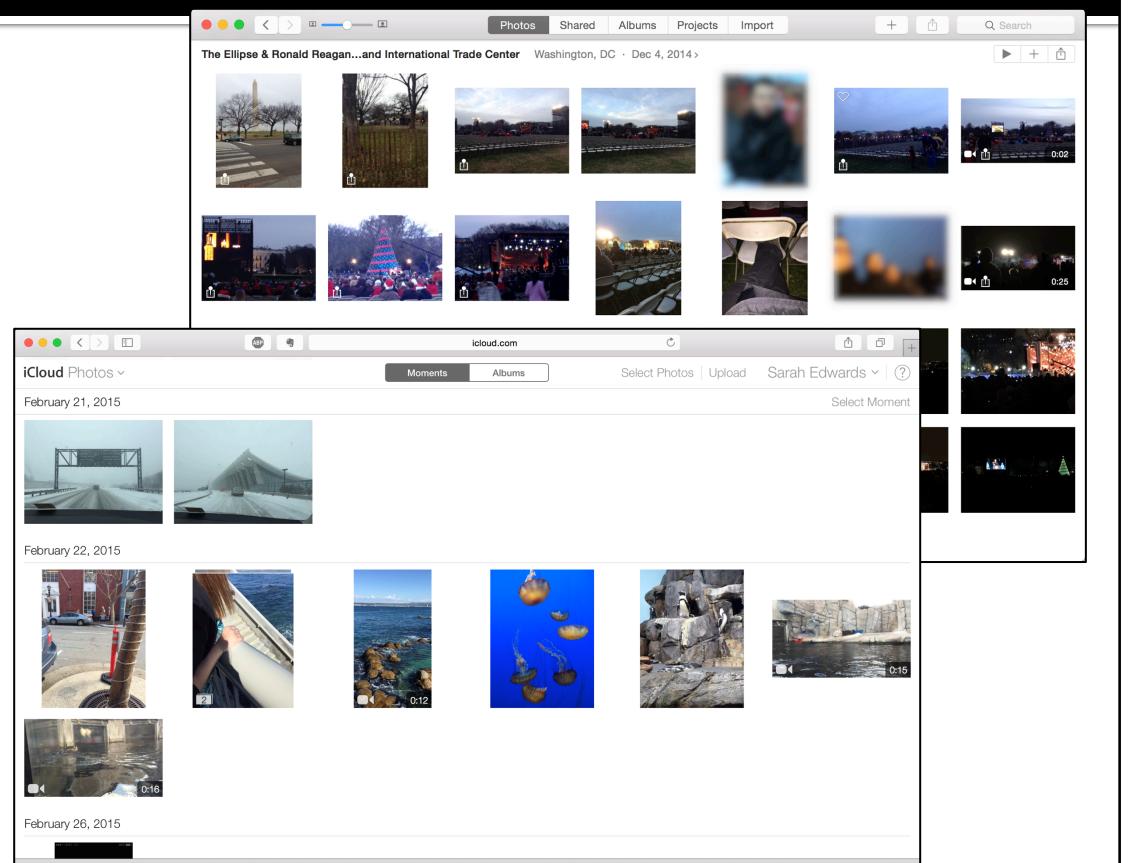
Your Photo Stream Photos - sub/

Shared Photo Stream Photos - sub-shared/



Applications Photos – New Photos Application

- OS X – New Location w/ new OS X Photos App:
 - ~/Pictures/Photos Library.photoslibrary/
 - Local photos and iCloud photos are integrated.



Applications

Photos – New Photos Application

- OS X – New Location w/ new OS X Photos App:
 - ~/Pictures/Photos Library.photoslibrary/

```
word:Photos Library.photoslibrary oompa$ pwd
/Users/oompa/Pictures/Photos Library.photoslibrary
word:Photos Library.photoslibrary oompa$ ls -l
total 1872
drwxr-xr-x  2 oompa  staff      68 May 15 18:21 Attachments
drwxr-xr-x@ 26 oompa  staff    884 May 16 13:39 Database
drwxr-xr-x  2 oompa  staff      68 May 15 18:22 Masks
drwxr-xr-x  4 oompa  staff    136 May 15 18:21 Masters
drwxr-xr-x  2 oompa  staff      68 May 15 18:22 Plugins
drwxr-xr-x  4 oompa  staff    136 May 15 18:21 Previews
-rw-r--r--  1 oompa  staff    341 May 15 18:22 ProjectDBVersion.plist
-rw-r--r--@ 1 oompa  staff  950272 May 15 18:22 Projects.db
drwxr-xr-x  5 oompa  staff    170 May 15 18:22 Thumbnails
drwxr-xr-x  3 oompa  staff    102 May 15 18:21 download
-rw-r--r--@ 1 oompa  staff      1 May  6 08:46 iPhotoLock.data
drwxr-xr-x 10 oompa  staff   340 May 17 07:57 private
drwxr-xr-x  6 oompa  staff    204 May 15 18:22 resources
```

Applications

Photos – New Photos Application

- OS X – New Location w/ new OS X Photos App:
 - ~/Pictures/Photos Library.photoslibrary/
 - Masters Directory: The photos themselves
 - JPG - Photos
 - PNG - Screenshots
 - MOV – Movies
 - Time stamped File Paths
 - Extended Attribute:
com.apple.quarantine = clouddphotosd,
iCloud

```
word:Masters oompa$ pwd  
/Users/oompa/Pictures/Photos Library.photoslibrary/Masters  
word:Masters oompa$ tree -L 4 2015/  
2015/  
├── 01  
│   ├── 11  
│   │   ├── 20150111-174805  
│   │   └── IMG_1629.JPG  
│   └── 20150111-174816  
└── 24  
    ├── 20150124-130736  
    │   ├── IMG_1630.JPG  
    │   └── IMG_1631.JPG  
    └── 20150124-130748  
      └── 02  
        ├── 07  
        │   ├── 20150207-095600  
        │   │   ├── IMG_1632.JPG  
        │   │   ├── IMG_1633.JPG  
        │   │   ├── IMG_1634.JPG  
        │   │   └── IMG_1635.JPG  
        │   └── 20150207-095613  
        └── 11  
          ├── 20150211-205726  
          │   └── IMG_1636.JPG  
          └── 20150211-205737  
            └── 14  
              └── 20150214-235059  
                ├── IMG_1637.MOV  
                ├── IMG_1638.MOV  
                └── IMG_1639.MOV
```

```
word:20150516-225727 oompa$ xattr -xl IMG_1916.PNG  
com.apple.quarantine:  
00000000 30 30 30 32 3B 35 35 35 37 63 64 65 39 3B 63 6C |0002;5557cde9;cll|  
00000010 6F 75 64 70 68 6F 74 6F 73 64 3B |oudphotosd;|  
0000001b
```

Applications Photos – New Photos Application

- OS X – Photos App Metadata
 - ~/Pictures/Photos Library.photoslibrary/Databases/Library.apdb
 - Link to /apdb/Library.apdb
 - SQLite Database

```
word:Database oompa$ pwd
/Users/oompa/Pictures/Photos Library.photoslibrary/Database
word:Database oompa$ ls -l
total 30168
drwxr-xr-x  30 oompa  staff   1020 May 15 18:21 Albums
lrvxr-xr-x@  1 oompa  staff    18 May 15 18:21 BigBlobs.apdb -> apdb/BigBlobs.apdb
-rw-r--r--@  1 oompa  staff   523 May 15 18:23 DataModelVersion.plist
drwxr-xr-x  6 oompa  staff   204 May 15 18:21 Faces
lrvxr-xr-x@  1 oompa  staff   13 May 15 18:21 Faces.db -> apdb/Faces.db
drwxr-xr-x  24 oompa  staff  816 May 15 18:21 Folders
drwxr-xr-x  3 oompa  staff   102 May 15 18:22 History
lrvxr-xr-x@  1 oompa  staff   17 May 15 18:21 History.apdb -> apdb/History.apdb
lrvxr-xr-x@  1 oompa  staff   22 May 15 18:21 ImageProxies.apdb -> apdb/ImageProxies.apdb
-rw-r--r--@  1 oompa  staff  1497 Nov 16 2014 Keywords.plist
lrvxr-xr-x@  1 oompa  staff   17 May 15 18:21 Library.apdb -> apdb/Library.apdb
drwxr-xr-x  2 oompa  staff   68 May 15 18:21 Places
lrvxr-xr-x@  1 oompa  staff   20 May 15 18:21 Properties.apdb -> apdb/Properties.apdb
-rw-r--r--@  1 oompa  staff  8192 May 15 18:23 RKAlbum_name.skindex
-rw-r--r--@  1 oompa  staff  266240 May 18 07:40 RKVersion_searchIndexText.skindex
-rw-r--r--@  1 oompa  staff   42 Mar 22 16:16 SpanCache.plist
drwxr-xr-x  2 oompa  staff   68 May 15 18:21 Vaults
drwxr-xr-x  4 oompa  staff  136 May 15 18:21 Versions
drwxr-xr-x  3 oompa  staff  102 May 15 18:21 Volumes
drwxr-xr-x  15 oompa  staff  510 May 15 18:22 apdb
-rw-r--r--@  1 oompa  staff  3850240 May 17 07:38 metaSchema.db
-rw-r--r--@  1 oompa  staff 11272328 May 18 07:41 metaSchema.db-wal
-rw-r--r--@  1 oompa  staff  453 May 16 13:39 metaSchema.db.lock
-rw-r--r--@  1 oompa  staff  304 May 15 18:22 tmSync.plist
```

Applications

Photos – New Photos Application – Photo Metadata

- OS X – Photos App Metadata – Library.apdb
 - Photo UUID
 - File Name
 - Timestamps (imageDate, Create, Export Image, Export Metadata,
 - Height/Width/Rotation
 - Associated Notes Flag
 - Location Latitude/Longitude
 - Time Zone
 - Reversed Location Blob Data (similar to reverse IP location)
 - More!
- Have not yet found relationship to Device UDID. ☺

Enter Field Values	
1. modelId (integer)	1823
2. uuid (varchar)	obcvjHS1Rw+TIBbEw%gfzQ
3. name (varchar)	Null
4. fileName (varchar)	IMG_1640.JPG
5. versionNumber (integer)	1
6. stackUuid (varchar)	Null
7. masterUuid (varchar)	8XLwuPimQ+KBzn5Ly9HvUA
8. masterId (integer)	912
9. rawMasterUuid (varchar)	Null
10. nonRawMasterUuid (varchar)	8XLwuPimQ+KBzn5Ly9HvUA
11. projectUuid (varchar)	photostream-import-2015-02
12. imageTimeZoneName (varchar)	Null
13. imageDate (timestamp)	445806439.627254
14. mainRating (integer)	0
15. isHidden (integer)	0
16. isFlagged (integer)	0
17. isOriginal (integer)	0
18. isEditable (integer)	1
19. colorLabelIndex (integer)	-1
20. masterHeight (integer)	2448
21. masterWidth (integer)	3264

Applications

Photos – New Photos Application - Photos

- iOS iCloud Photos:
 - Photos: /private/var/mobile/Media/PhotoStreamsData/<iCloud_Person_ID>/1##APPLE/*
 - Metadata: /private/var/mobile/Media/PhotoStreamsData/<iCloud_Person_ID>/.MISC/*

```
iPhone5s:/private/var/mobile/Media/PhotoStreamsData/[REDACTED].MISC root# pwd
/private/var/mobile/Media/PhotoStreamsData/24713276/.MISC
iPhone5s:/private/var/mobile/Media/PhotoStreamsData/[REDACTED].MISC root# plutil -show 01c13f98-f9f7c5d1-f66832d5-8f86e
a71-4cf48493-08
{
    MSAssetMetadataAssetFileTransferUUID = "F42C10FD-A53A-4676-BAB8-4CA37FDEE4E7";
    MSAssetMetadataFileSize = 861366;
    MSAssetMetadataItemID = 2839799380335933883;
    MSAssetMetadataPixelHeight = 1536;
    MSAssetMetadataPixelWidth = 2048;
    MSAssetMetadataStreamIDKey = [REDACTED];
    isDerivedAsset = 1;
    "k-filename" = "IMG_1748.JPG";
    KPLLocalIMSMetadataAssetPLUUIDKey = "42F06193-46C0-47D3-82A1-5A7E2951A54C";
    KPLPhotoStreamAssetCollectionUUID = "861EE924-85E4-492A-B127-B7045E2E1861";
    KPLPhotoStreamDateCreatedKey = 2015-03-21 17:24:46 +0000;
    KPLPhotoStreamDerivedAssetHashKey = <015fc41d 2c0a0ded 478e6d58 9553543a a8057bd0 e8>;
    KPLPhotoStreamMasterAssetHashKey = <01c13f98 f9f7c5d1 f66832d5 8f86ea71 4cf48493 08>;
    KPLPhotoStreamMasterAssetMetadataKey = {
        MSAssetMetadataDateContentCreated = 2015-03-21 17:24:46 +0000;
        MSAssetMetadataDateContentModified = 2015-03-21 17:24:46 +0000;
        MSAssetMetadataDeviceID = eb8c872eb999a2be31801a5b3a6d4ce2a468ccf0;
        MSAssetMetadataFileSize = 1954255;
        MSAssetMetadataPixelHeight = 2448;
        MSAssetMetadataPixelWidth = 3264;
        MSAssetMetadataStreamIDKey = 24713276;
    };
    KPLPhotoStreamModifiedDateKey = 2015-03-21 17:24:46 +0000;
}
```

Applications

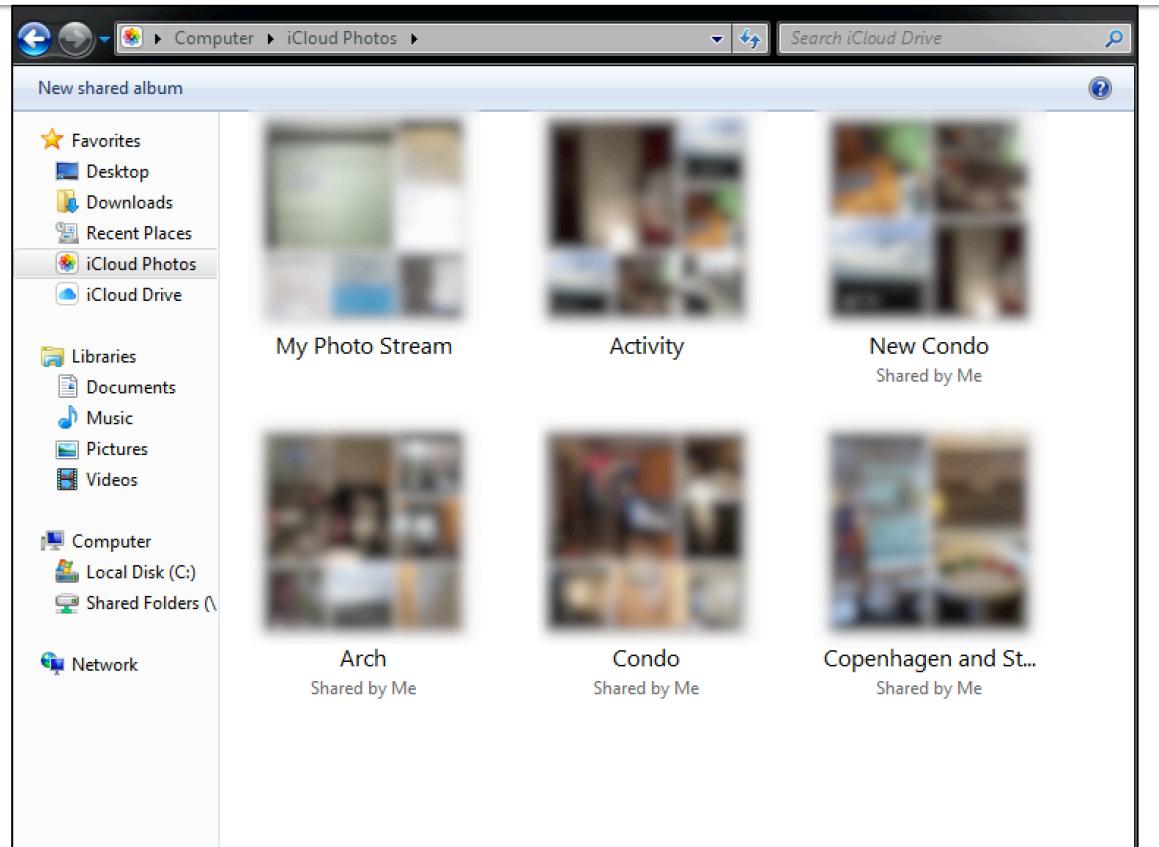
Photos – New Photos Application – Shared Albums

- iOS iCloud Photos – Shared Albums
 - Shared Album Data: /private/var/mobile/Media/PhotoData/PhotoCloudSharingData/<iCloud_Person_ID>/<GUID>/
 - Shared with whom?: ZCLOUDSHAREDALBUMINVINTATIONRECORD Table - /private/var/mobile/Media/PhotoData/Photos.sqlite
 - Correlate the GUIDs
 - iCloud Shared Photo Comments in ZCLOUDSHAREDCOMMENT Table

```
iPhone5s:/private/var/mobile/Media/PhotoData/PhotoCloudSharingData/[REDACTED] root# pwd  
/private/var/mobile/Media/PhotoData/PhotoCloudSharingData/[REDACTED]  
iPhone5s:/private/var/mobile/Media/PhotoData/PhotoCloudSharingData/[REDACTED] root# ls -l  
total 0  
drwxr-xr-x 2 mobile mobile 102 Apr 11 08:03 13836496-E555-4241-8F83-F99700ADA7A9  
drwxr-xr-x 2 mobile mobile 102 Apr 11 08:03 C7482CD5-D258-4E12-82B0-587F7B4EF734  
drwxr-xr-x 2 mobile mobile 102 Apr 11 08:03 D2C210B5-61ED-4534-8145-41274AF31E6F  
drwxr-xr-x 2 mobile mobile 102 Apr 11 08:03 FDB5910C-6C54-4625-8A4B-A9034CA2F291  
iPhone5s:/private/var/mobile/Media/PhotoData/PhotoCloudSharingData/[REDACTED] root# plutil -show 13836496-E555-4241-8F83  
-F99700ADA7A9/Info.plist  
{  
    cloudOwnerEmail = "oompa@csh.rit.edu";  
    cloudOwnerFirstName = Sarah;  
    cloudOwnerHashedPersonID = fbc09[REDACTED]  
    cloudOwnerLastName = Edwards;  
    cloudPublicURLEnabled = 1;  
    cloudRelationshipState = 0;  
    publicURL = "https://www.icloud.com/photostream/#A25[REDACTED]";  
    title = "Copenhagen and Stockholm";  
}
```

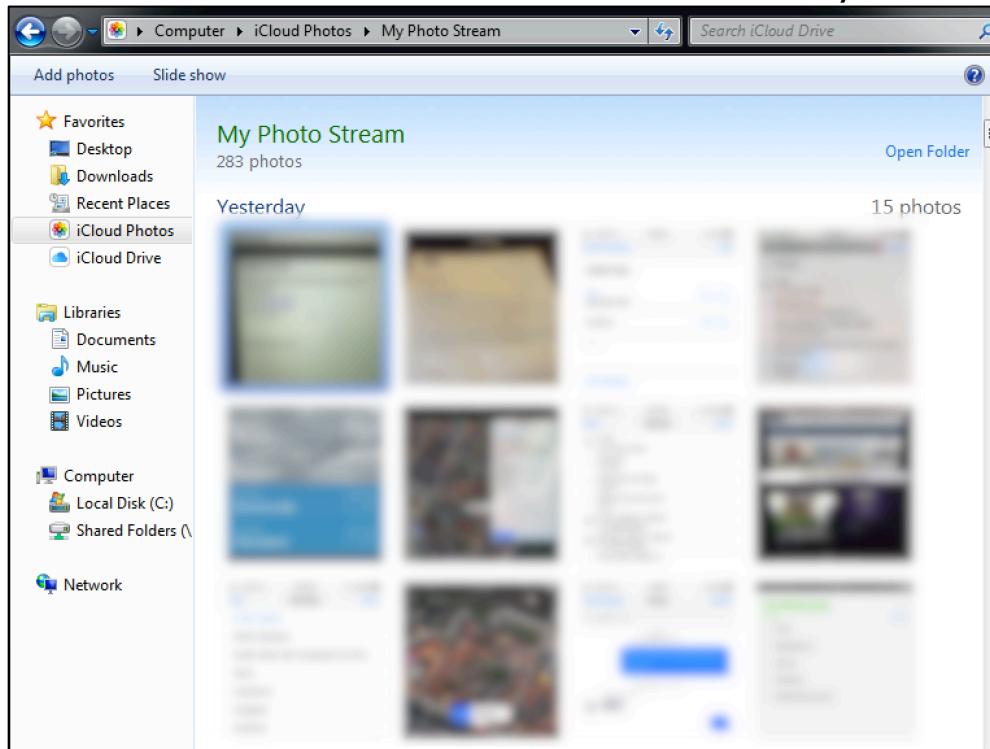
Applications Photos – On Windows – iCloud Photos

- “My Photo Stream”
- “Shared”
 - “New Condo”
 - “Arch”
 - “Condo”
 - “Copenhagen and St...”



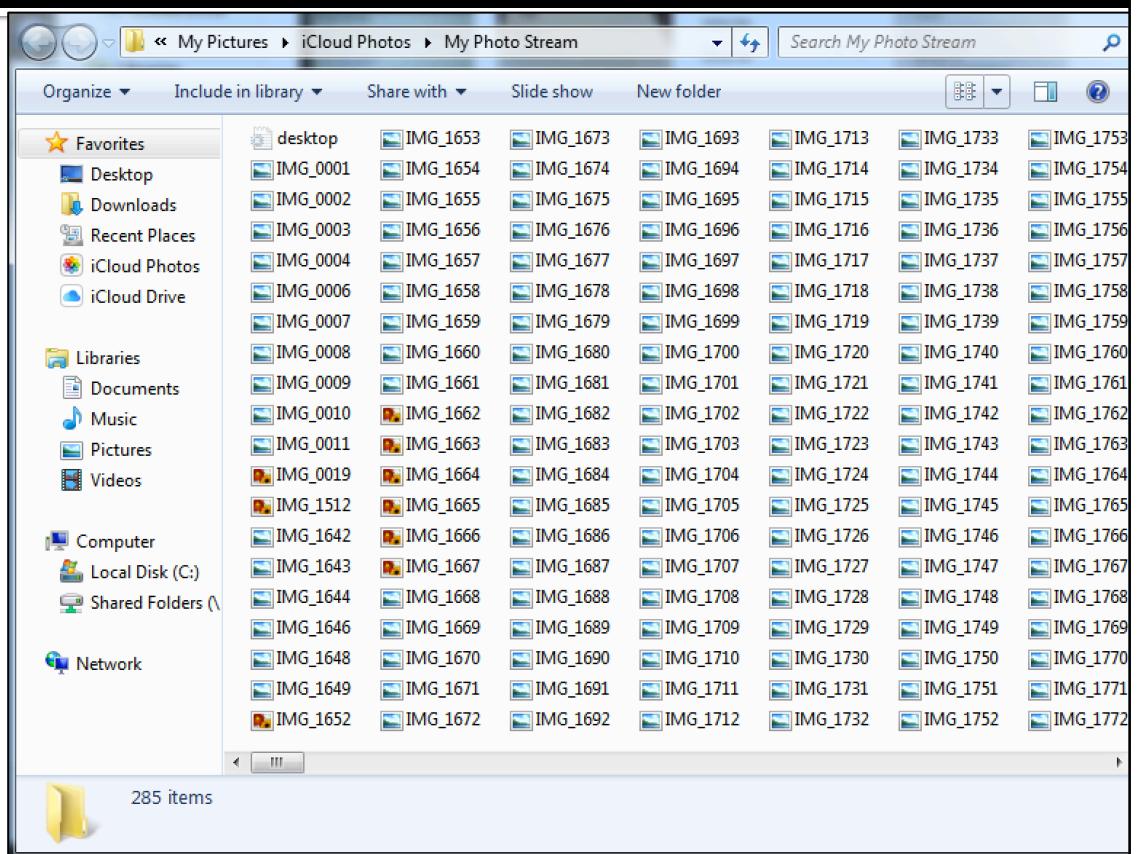
Applications Photos – On Windows – My Photo Stream

- C:\Users\<user>\Pictures\iCloud Photos\My Photo Stream\



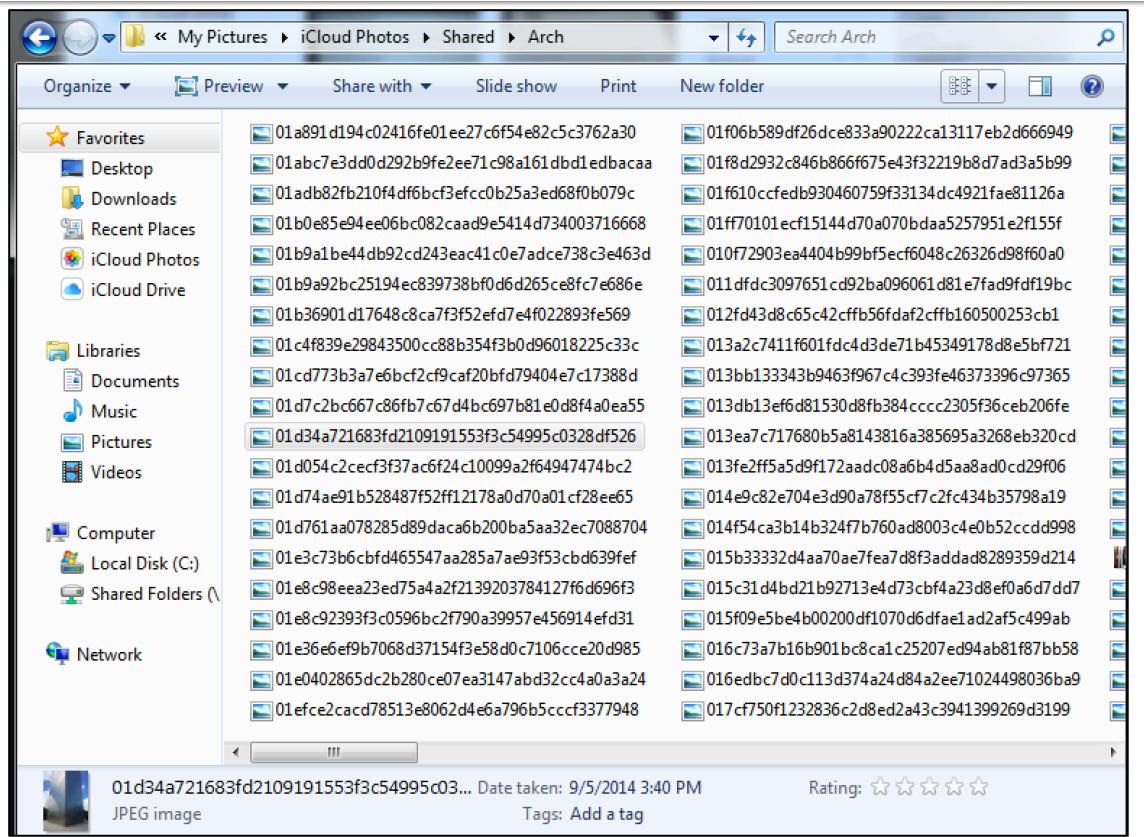
Applications Photos – On Windows – My Photo Stream

- C:\Users\<user>\Pictures\iCloud Photos\My Photo Stream\
 - IMG_####.JPG or PNG



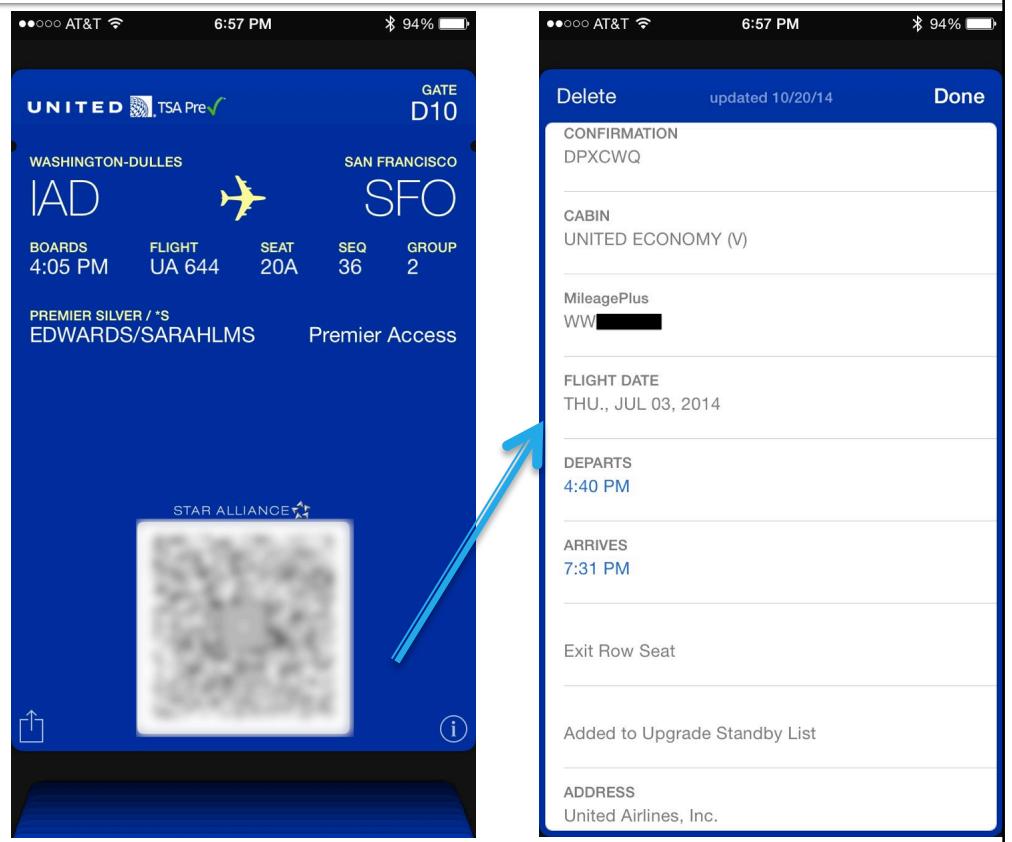
Applications Photos – On Windows – Shared Albums

- C:\Users\<user>\Pictures\iCloud Photos\Shared\
- Directory is Shared Album Name (“Arch”)
- <43_alphanumeric_characters>.JPG or PNG



Applications Passbook Passes

- OS X: ~/Library/Mobile Documents/com~apple~shoebox/UbiqitousCards/
- iOS: /private/var/mobile/Library/Passes/Cards/



Applications Passbook Passes - *.pkpass Files

```
word:UbiquitousCards oompa$ pwd
/Users/oompa/Library/Mobile Documents/com~apple~shoebox/UbiquitousCards
word:UbiquitousCards oompa$ ls -l
total 0
drwxr-xr-x  9 oompa  staff  306 Jul 16  2014 0-cM9ac3eFNA9iCZ0mbkGqaN10E=.pkpass
drwxr-xr-x  9 oompa  staff  306 Jul 26  2014 07DvKQIpN4QMgdtfi5miHNJWHmQ=.pkpass
drwxr-xr-x 12 oompa  staff  408 Aug 10  2014 0cffFcwnrkgt7WihgBX07v4qr7I=.pkpass
drwxr-xr-x 11 oompa  staff  374 Oct 11  2014 1Ky0sMM7V4TVHm8wtU5LSb7GL9k=.pkpass
drwxr-xr-x 12 oompa  staff  408 Jan 14 15:30 3FM0j7C76ZUQaJm01GSeG8dAsfQ=.pkpass
drwxr-xr-x 12 oompa  staff  408 Apr 11 13:34 7v-kNTQz++jc5zN0h1YLoKN1CZk=.pkpass
drwxr-xr-x 12 oompa  staff  408 Apr  2  2014 8D3SZgmt2S5FQ2hS+9ZUTjvqVm8=.pkpass
drwxr-xr-x 12 oompa  staff  408 Nov  8  2014 8x0Nu0B04WA0FfSGlV4cC21bvC8=.pkpass
```

```
miPhone5s:/private/var/mobile/Library/Passes/Cards root# pwd
/private/var/mobile/Library/Passes/Cards
miPhone5s:/private/var/mobile/Library/Passes/Cards root# ls -l
total 0
drwxr-xr-x  2 mobile  mobile  204 Jul 16  2014 0-cM9ac3eFNA9iCZ0mbkGqaN10E=.cache
drwxr-xr-x  2 mobile  mobile  306 Jul 16  2014 0-cM9ac3eFNA9iCZ0mbkGqaN10E=.pkpass
drwxr-xr-x  2 mobile  mobile  204 Jul 26  2014 07DvKQIpN4QMgdtfi5miHNJWHmQ=.cache
drwxr-xr-x  2 mobile  mobile  306 Jul 26  2014 07DvKQIpN4QMgdtfi5miHNJWHmQ=.pkpass
drwxr-xr-x  2 mobile  mobile  204 Aug 10  2014 0cffFcwnrkgt7WihgBX07v4qr7I=.cache
drwxr-xr-x  2 mobile  mobile  408 Aug 10  2014 0cffFcwnrkgt7WihgBX07v4qr7I=.pkpass
drwxr-xr-x  2 mobile  mobile  204 Apr 23  2014 8D3SZgmt2S5FQ2hS+9ZUTjvqVm8=.cache
drwxr-xr-x  2 mobile  mobile  408 Apr  2  2014 8D3SZgmt2S5FQ2hS+9ZUTjvqVm8=.pkpass
```

Applications

Passbook Passes – Pass Info - pass.json Files

- **Pass Information** - pass.json Files

```
{  
  "boardingPass": {  
    "transitType": "PKTransitTypeAir",  
    "auxiliaryFields": [  
      {  
        "label": "BOARDS",  
        "key": "boardingTime",  
        "value": "4:05 PM"  
      },  
      {  
        "label": "FLIGHT",  
        "key": "flight",  
        "value": "UA 644"  
      },  
      {  
        "label": "SEAT",  
        "key": "seat",  
        "value": "20A"  
      },  
      {  
        "label": "SEQ",  
        "key": "seq",  
        "value": "36"  
      },  
      {  
        "label": "GROUP",  
        "key": "group",  
        "value": "2"  
      }  
    ],  
    "headerFields": [  
      {  
        "label": "GATE",  
        "key": "gate",  
        "value": "D10",  
        "changeMessage": "Your gate has changed to %@"  
      }  
    ],  
    "primaryFields": [  
      {  
        "label": "WASHINGTON-DULLES",  
        "key": "origin",  
        "value": "IAD"  
      },  
      {  
        "label": "SAN FRANCISCO",  
        "key": "destination",  
        "value": "SFO"  
      }  
    ]  
  },  
  "xr-x--x 1 oompa staff 11264 Oct 26 2014 Thumbs.db  
  xr-x--x 1 oompa staff 6150 Oct 26 2014 footer.png  
  xr-x--x 1 oompa staff 13133 Oct 26 2014 footer@2x.png  
  xr-x--x 1 oompa staff 2870 Oct 26 2014 icon.png  
  xr-x--x 1 oompa staff 4406 Oct 26 2014 icon@2x.png  
  xr-x--x 1 oompa staff 5467 Oct 26 2014 logo.png  
  xr-x--x 1 oompa staff 8842 Oct 26 2014 logo@2x.png  
  xr-x--x 1 oompa staff 9042 Oct 26 2014 manifest.json  
  xr-x--x 1 oompa staff 9042 Oct 26 2014 pass.json  
  xr-x--x 1 oompa staff 9042 Oct 26 2014 signature  
}
```

```
secondaryFields": [
  {
    "label": "PREMIER SILVER / *$",
    "key": "passenger",
    "value": "EDWARDS/SARAHLMS"
  },
  {
    "key": "status",
    "value": "Premier Access"
  }
],
"backFields": [
  {
    "label": "CONFIRMATION",
    "key": "confirmation",
    "value": "DPXCWQ"
  },
  {
    "label": "CABIN",
    "key": "cabin",
    "value": "UNITED ECONOMY (V)"
  },
  {
    "label": "MileagePlus",
    "key": "mileagePlusNumber",
    "value": "WW [REDACTED]"
  },
  {
    "label": "FLIGHT DATE",
    "key": "flightDate",
    "value": "THU., JUL 03, 2014"
  },
  {
    "label": "DEPARTS",
    "key": "departTime",
    "value": "4:40 PM"
  },
  {
    "label": "ARRIVES",
    "key": "arriveTime",
    "value": "7:31 PM"
  },
  {
    "key": "exitRow",
    "value": "Exit Row Seat"
  }
]
```

Applications Notes

The image displays the Notes application across three platforms: OS X, iOS, and iCloud Notes web interface.

OS X Notes: The main window shows a sidebar with categories: All Notes, iCloud (selected), Notes, New Folder, Google, and accounts (oompa@csh.rit.edu). The main area lists notes: "This is a new iCloud Note." (1:44 PM) and "iCloud preso" (5/10/15).

iOS Notes: A modal view shows a note titled "This is a new iCloud Note." dated 5/17/15, 1:44 PM. The note content is: "This is a new iCloud Note." and "Things to do at conferences:

- Meet new people
- Eat good food
- Present something Apple related!

".

iCloud Notes Web: A screenshot of the iCloud Notes web interface shows the same note and a list of other notes: "iCloud preso" (May 10), "iCloud preso" (May 10), "iCloud preso" (May 10), "Charge Code" (May 8), "Elosoft" (Apr 11), "Marie Smith: 6680 Washingt..." (Apr 6), "Flight Numbers" (Apr 6), "Condo Questions:" (Mar 29), "Condo Updates:" (Mar 22), "Blacklight" (Feb 11), "HACKFORTRESS 2015 - ..." (Jan 17), and "HACKFORTRESS 2014 HIN..." (Jan 4).

Applications Notes

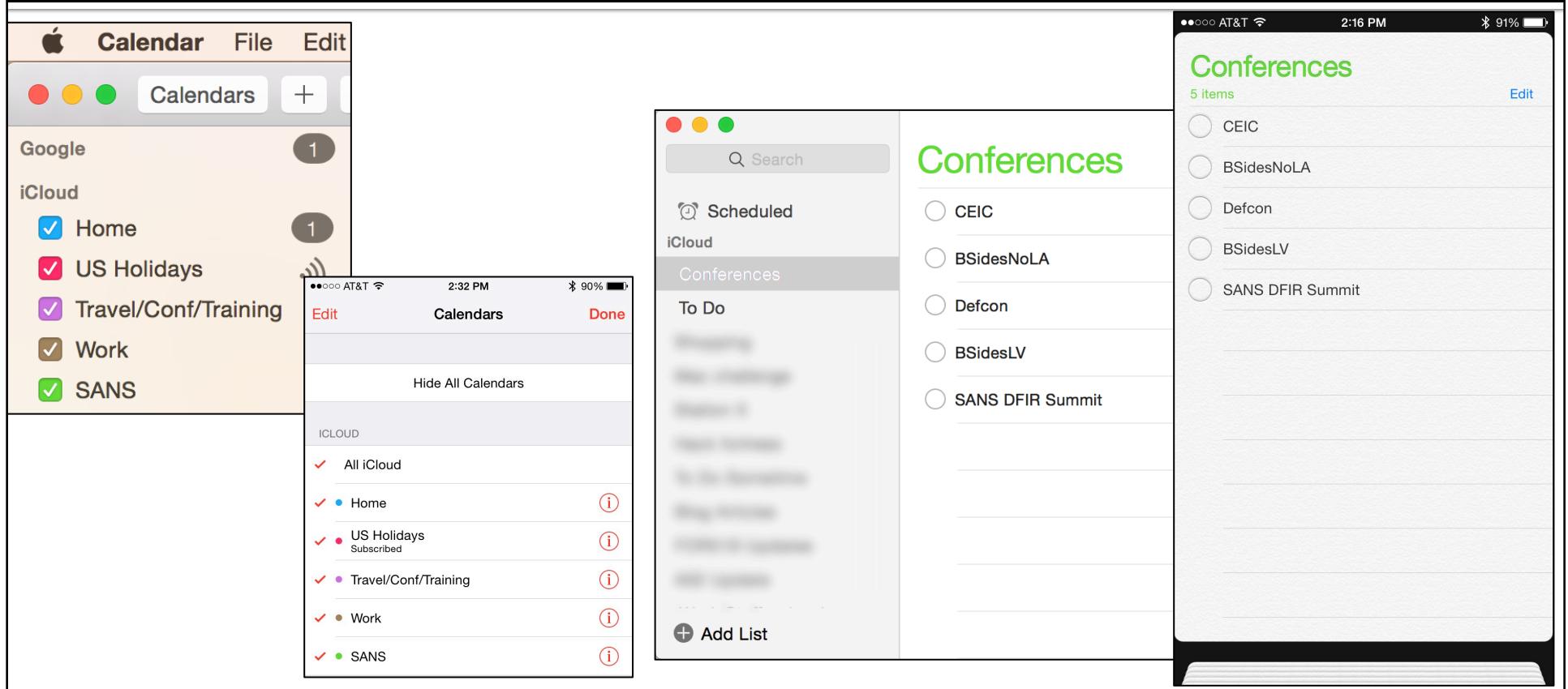
- **OS X:** ~/Library/Containers/com.apple.Notes/Data/Library/Notes/NotesV4.storeddata
- **iOS:** /private/var/mobile/Library/Notes/notes.sqlite
- SQLite Tables: ZNOTE & ZNOTEBODY
 - Note Creation & Edited Time
 - Note Title & Contents

```
1 select ZNOTE.Z_PK,ZDATECREATED,ZDATEEDITED,ZTITLE,ZHTMLSTRING from ZNOTE INNER JOIN ZNOTEBODY  
ON ZNOTE.Z_PK = ZNOTEBODY.Z_PK WHERE ZNOTE.Z_PK=86;
```

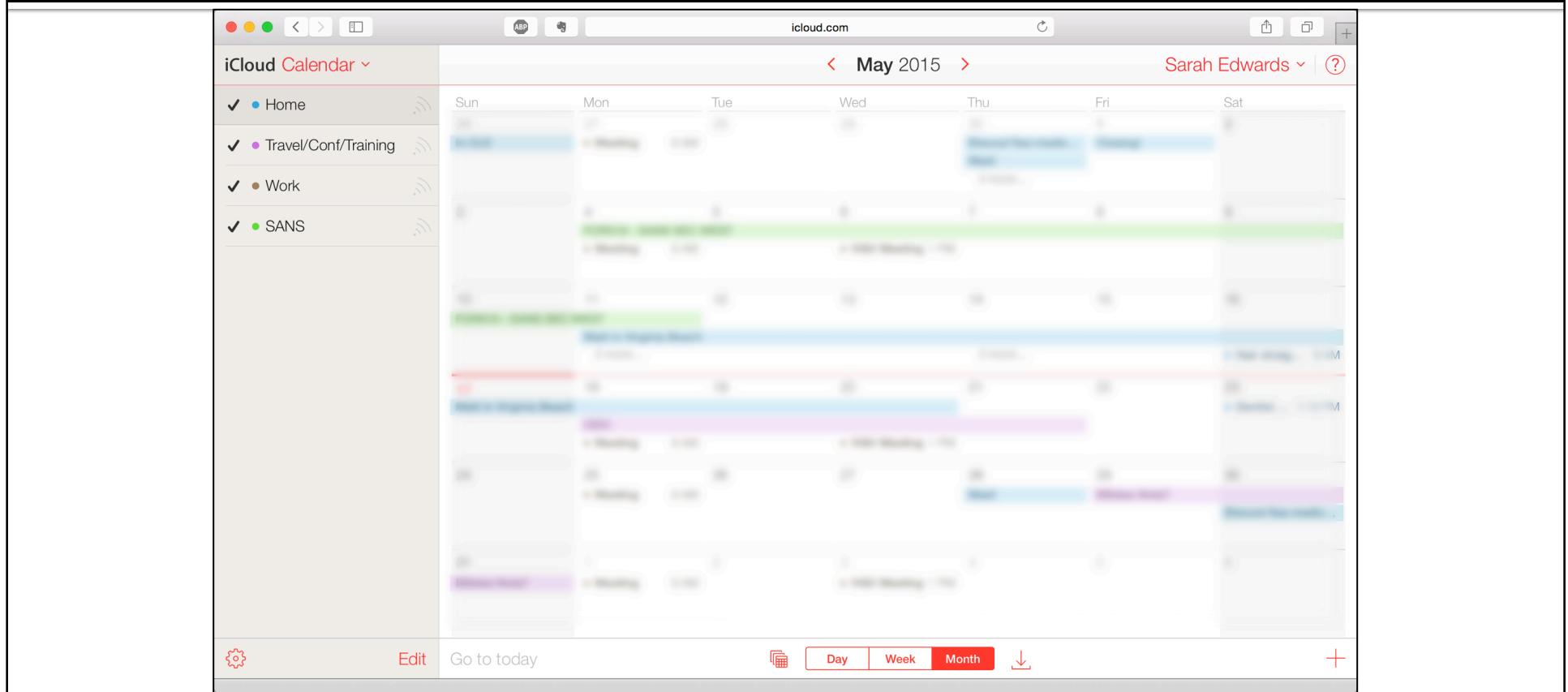
```
2
```

Z_PK	ZDATECREATED	ZDATEEDITED	ZTITLE	ZHTMLSTRING
1 86	453577382.679417	453577442.702202	This is a new iCloud Note.	<html><head></head><body>This is a new iCloud Note.<div> </div><div>Things to do at conferences:</div><div><ul clas...

Applications Calendar & Reminders



Applications Calendar & Reminders



Applications

Calendar & Reminders

- OS X: ~/Library/Calendars/Calendar Cache
- iOS: /private/var/mobile/Library/Calendar/Calendar.sqlitedb
- SQLite Table: ZCALENDARITEM
 - Calendar item creation time and title.

```
1 select Z_PK, ZCREATIONDATE, ZTITLE from ZCALENDARITEM where Z_PK >= 2178 and Z_PK <= 2182;
```

	Z_PK	ZCREATIONDATE	ZTITLE
1	2178	453579293	CEIC
2	2179	453579295	BSidesNoLA
3	2180	453579304	Defcon
4	2181	453579309	BSidesLV
5	2182	453579318	SANS DFIR Summit

Applications Contacts

The image displays three views of contact management:

- Mac Contacts Application:** Shows a sidebar with categories: All Contacts, iCloud, and All iCloud (selected). A search bar at the top right says "Search All iCloud". The main area shows contacts starting with "C": Andrew Case and Chad. Below the contact cards are sections for "note" and "Edit".
- iPhone Screen:** Shows the "All Contacts" screen with a contact for "Andrew Case". It includes fields for "mobile" (redacted), "call", "FaceTime", and "Audio". There are also "other" and "Notes" sections, and a "Send Message" button.
- iCloud Contacts Web View:** Shows the "iCloud.com" interface with a sidebar for "iCloud Contacts". The main area lists contacts starting with "A": Andrew Case, Sarah Edwards, and others. A search bar at the top says "Search All Contacts".

Applications Contacts

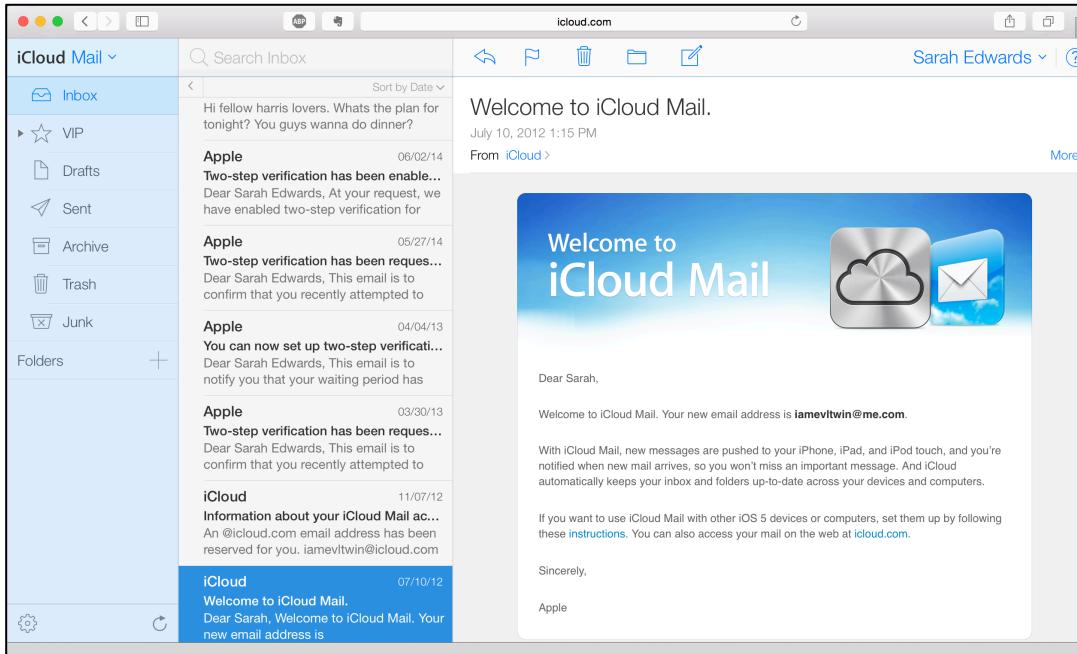
- **OS X:** ~/Library/Application Support/AddressBook/Sources/<GUID>/AddressBook-v22.abcddb
- **iOS:** /private/var/mobile/Library/AddressBook/AddressBook.sqlite
- SQLite Tables: ZABCDRECORD & ZABCDPHONENUMBER
 - Contact Name & Number
 - Contact Creation and Modification Dates

```
1 select ZABCDRECORD.Z_PK, ZCREATIONDATE,  
ZMODIFICATIONDATE, ZFIRSTNAME, ZLASTNAME, ZFULLNUMBER from ZABCDRECORD INNER JOIN  
ZABCDPHONENUMBER ON ZABCDRECORD.Z_PK = ZABCDPHONENUMBER.ZOWNER WHERE  
ZABCDRECORD.Z_PK=12;
```

Z_PK	ZCREATIONDATE	ZMODIFICATIONDATE	ZFIRSTNAME	ZLASTNAME	ZFULLNUMBER
1	12	436038309.237857	436038310.090837	Andrew	Case

Applications Email

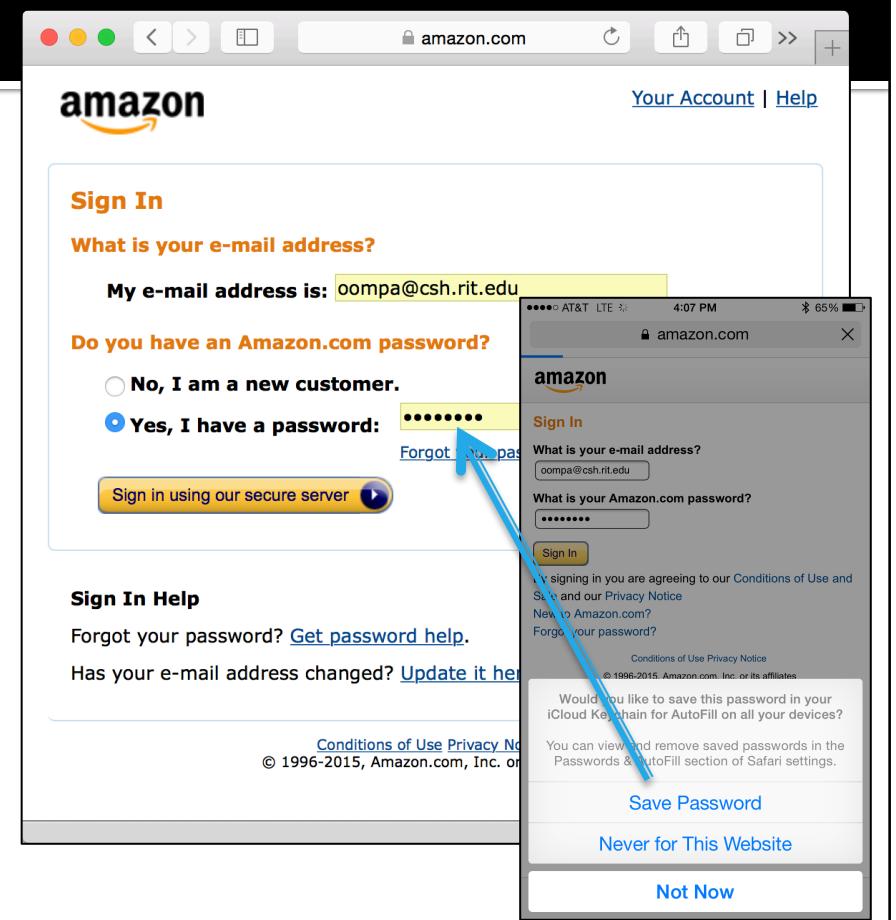
- OS X: ~/Library/Mail/V2/AosIMAP-<username>
- iOS: /private/var/mobile/Library/DataAccess/iCloud-<username>



Applications

iCloud Keychain

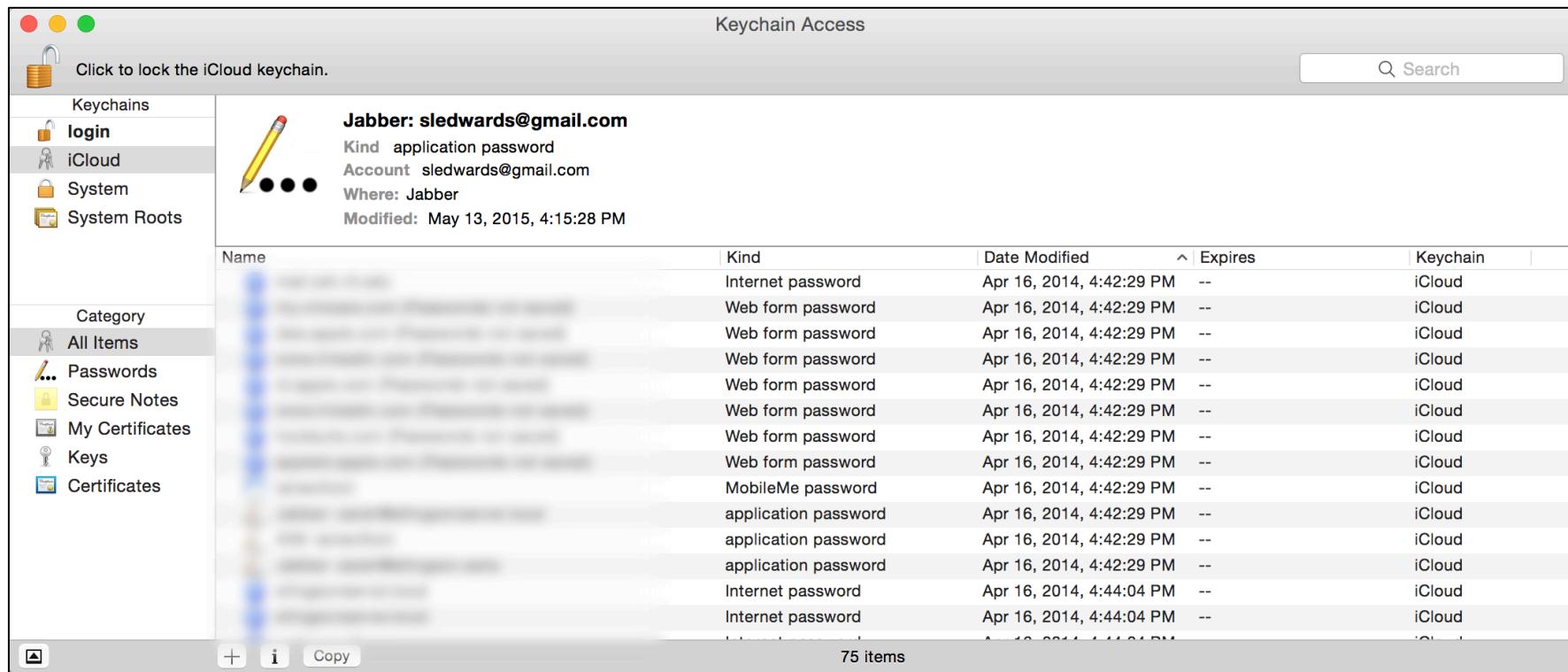
- iCloud Keychain:
 - OS X: ~/Library/Keychains/<GUID>/keychain-2.db (SQLite Database)
 - Accessible via User's Login password
 - iOS: /Library/Keychains/keychain-2.db (SQLite Database)
 - iOS Backup – Encrypted iTunes Backup Only
- May contain passwords for – websites, WiFi, Application Accounts (Chat, Email, Apple), Web Form Data, Credit Cards, etc.



Applications

iCloud Keychain

- iCloud Keychain – Access via OS X Keychain Access.app



Applications

3rd Party Applications

- Microsoft, Google, Dropbox, and other 3rd Party Apps!
- Empty ☹ “Reserved for Future Use”?

```
word:Mobile Documents oompa$ pwd  
/Users/oompa/Library/Mobile Documents  
word:Mobile Documents oompa$ ls  
8YE23NZS57~com~kayak~travel  
A4QBZ46HAP~com~gameloft~UN0Free  
F3LWYJ7GM7~com~apple~mobilegarageband  
F6266T9T75~com~apple~iMovie  
X6UDPZTLVR~Q5CS529KB3~com~velyoo~iDashboard  
com~apple~Automator  
com~apple~CloudDocs  
com~apple~Keynote  
com~apple~Notes  
com~apple~Numbers  
com~apple~Pages  
com~apple~Preview  
com~apple~QuickTimePlayerX  
com~apple~ScriptEditor2  
com~apple~TextEdit  
com~apple~TextInput  
com~apple~mail  
com~apple~shoebox  
com~apple~system~spotlight  
iCloud~com~getdropbox~Dropbox  
iCloud~com~google~container  
iCloud~com~microsoft~Office~PowerPoint  
iCloud~com~microsoft~onenote  
iCloud~com~microsoft~skydrive  
iCloud~com~zenlabs~c25k
```

The Future of iCloud



- Expect more data to be stored in the iCloud
 - Many iCloud related directories empty...but for how long?
- More 3rd Party Application Data
- Expect changes to directory structure and on-disk related data
- Thank You for Coming!
- Slides are available at mac4n6.com
- Contact Me!
 - oompa@csh.rit.edu
 - [@iamevtwin](https://twitter.com/iamevtwin)
 - mac4n6.com
- All icons are owned and are the copyright of Apple, Inc.