Sarah Edwards | @iamevltwin | 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

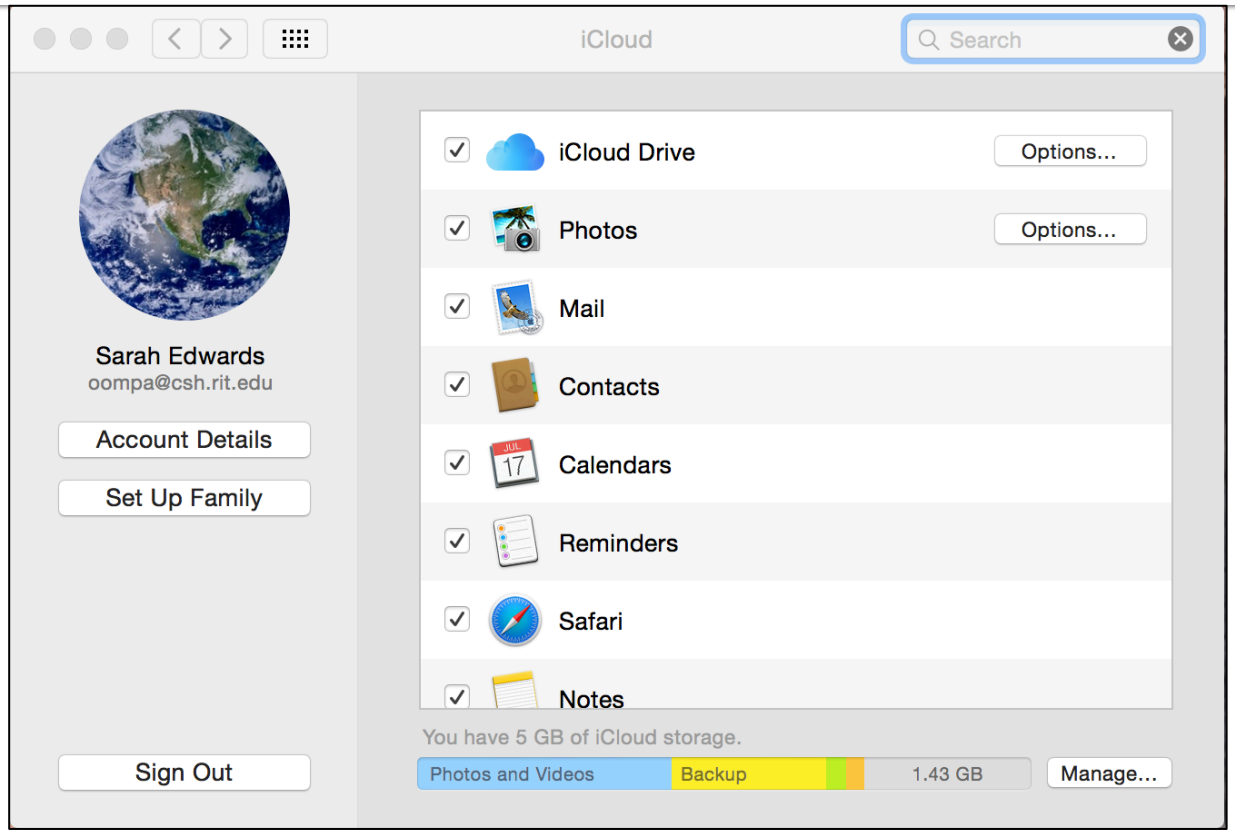
iCloud Basics
Ubiquity = "Everything Everywhere"

What is "Everything"?

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

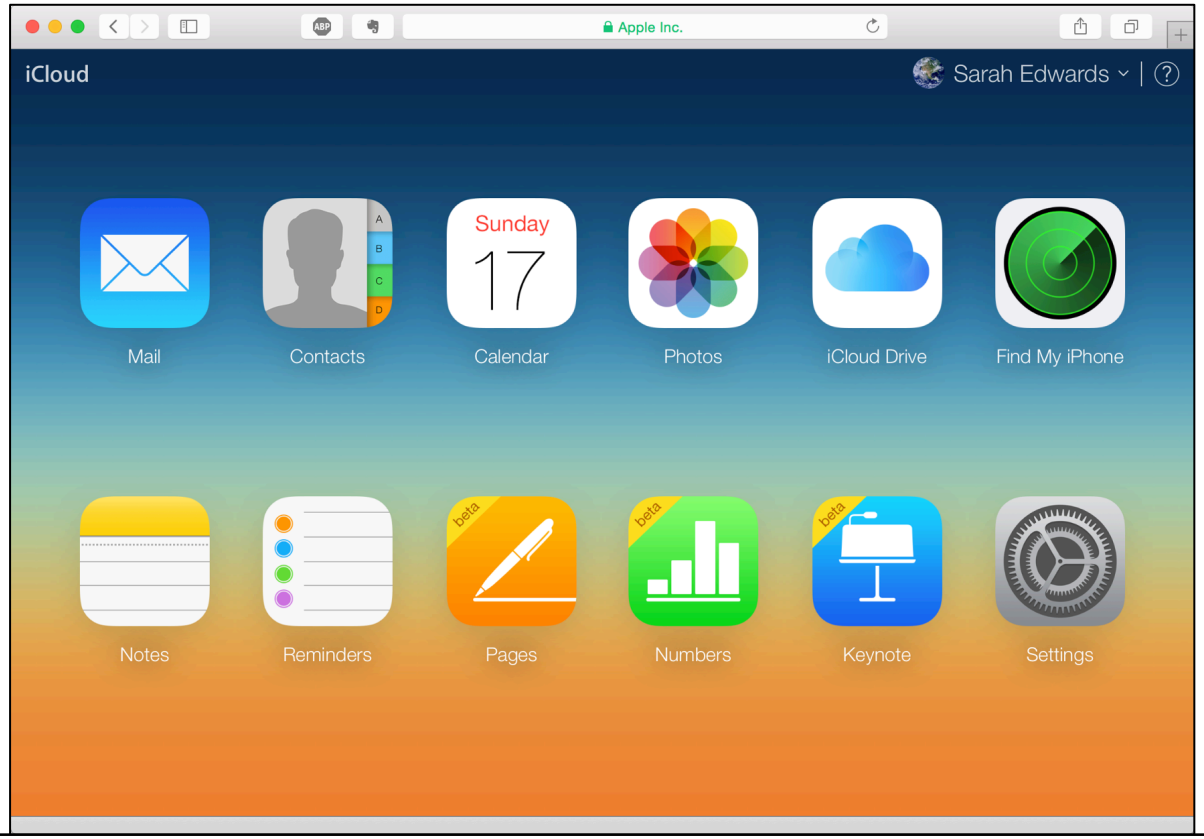
iCloud Basics

Ubiquity = "Everything Everywhere" - OS X & iOS

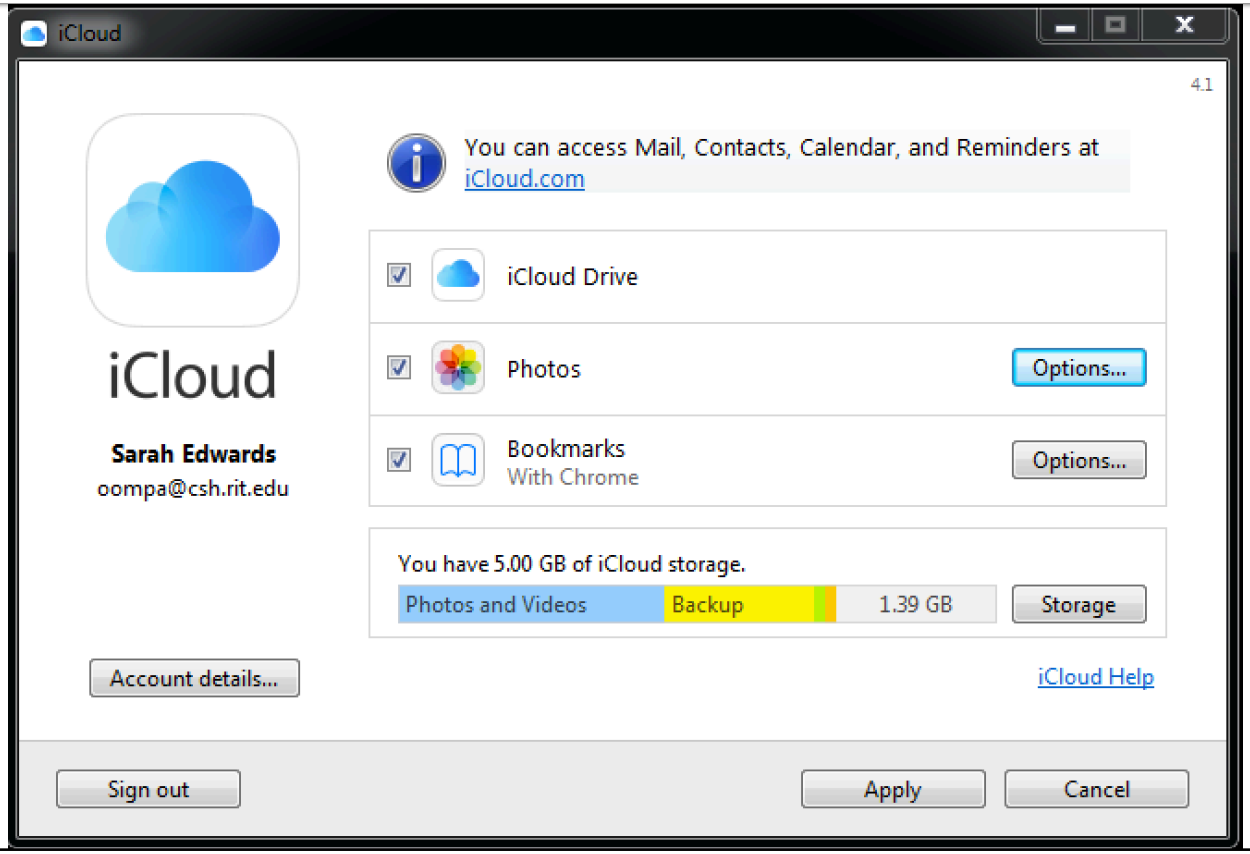


iCloud Basics

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.ubd.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

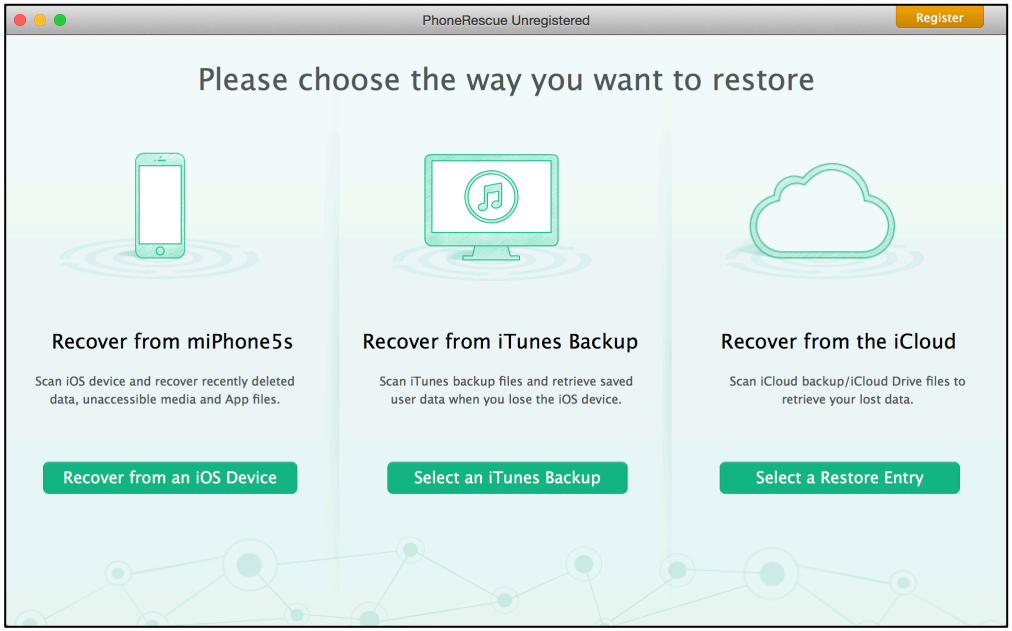
- **Elcomsoft Phone Breaker (EPPB)** - https://www.elcomsoft.com/eppb.html

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

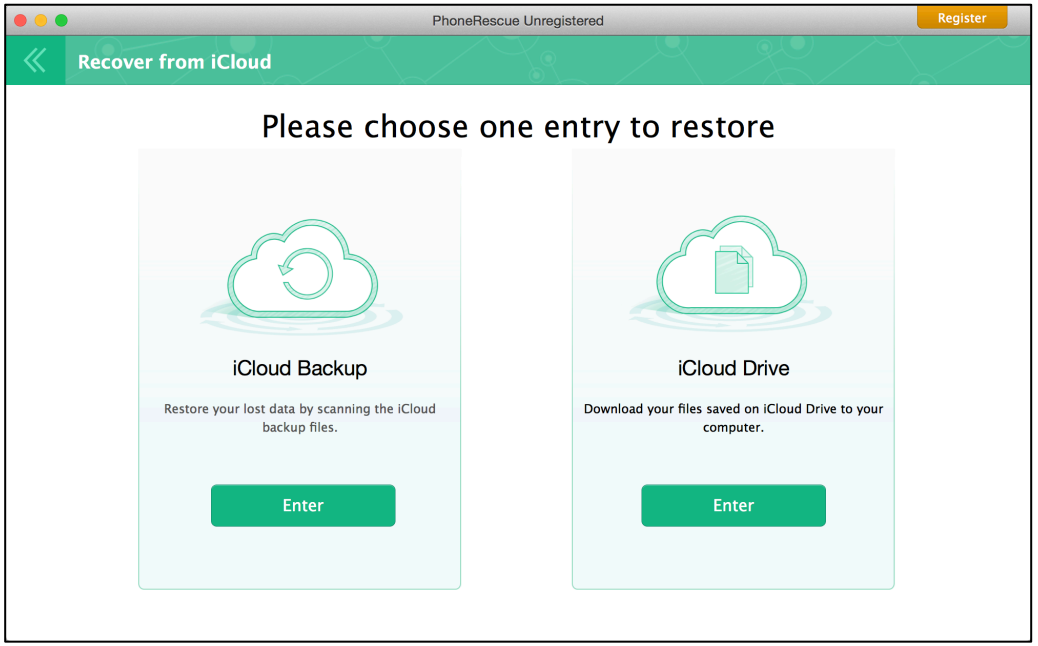
Getting to the iCloud Data
iCloud Backup Download Tools

- iPhone Backup Extractor – "Recover from the iCloud"



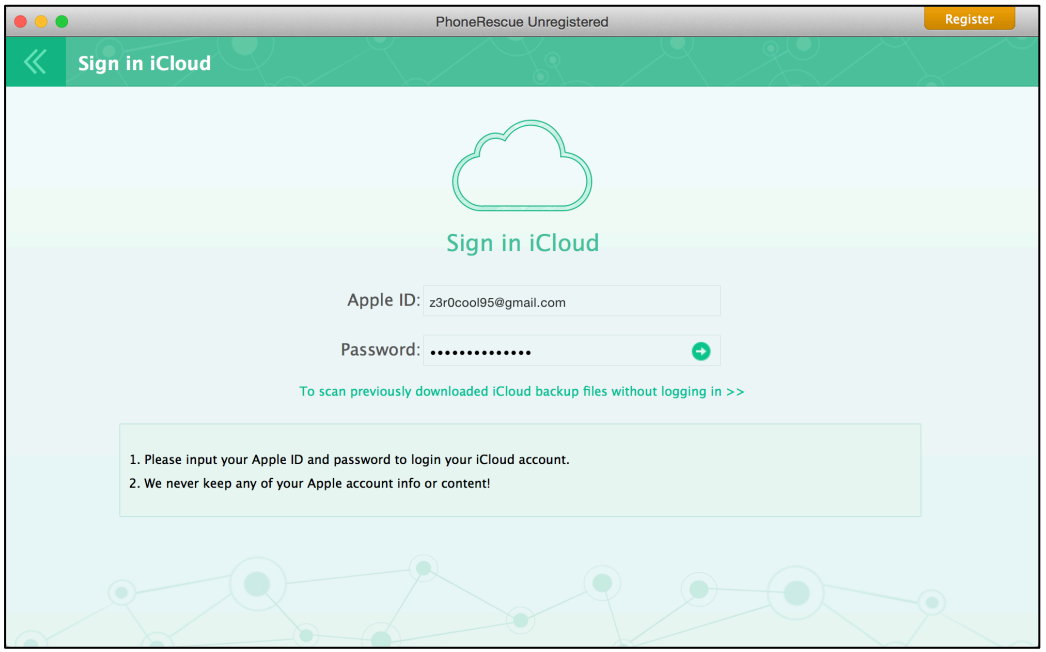
Getting to the iCloud Data
iCloud Backup Download Tools

- iPhone Backup Extractor – iCloud Backup or iCloud Drive?



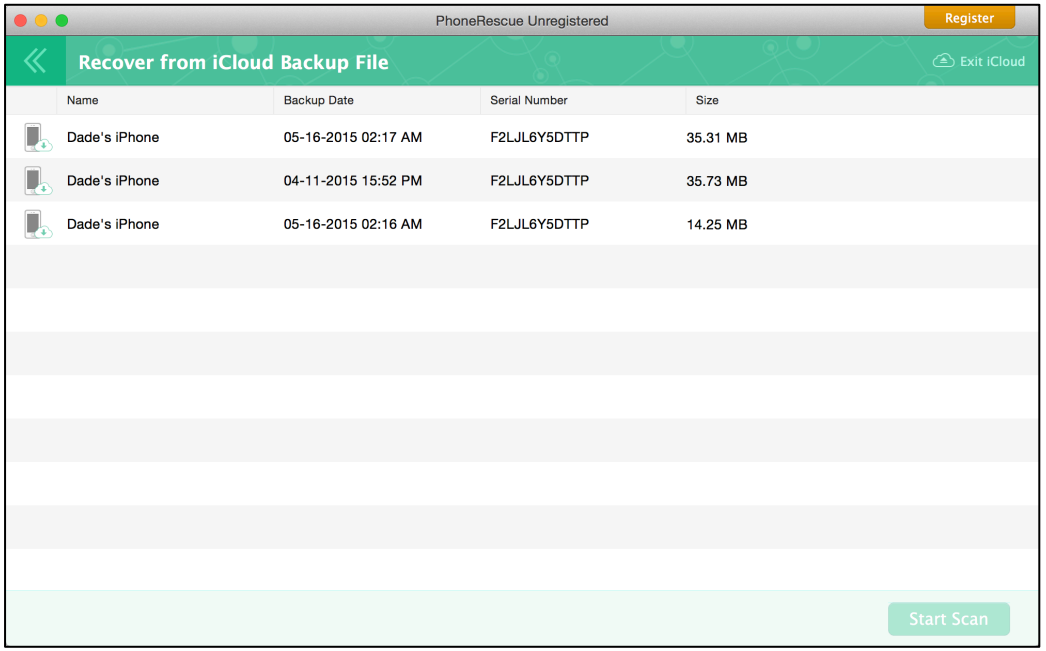
Getting to the iCloud Data
iCloud Backup Download Tools

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



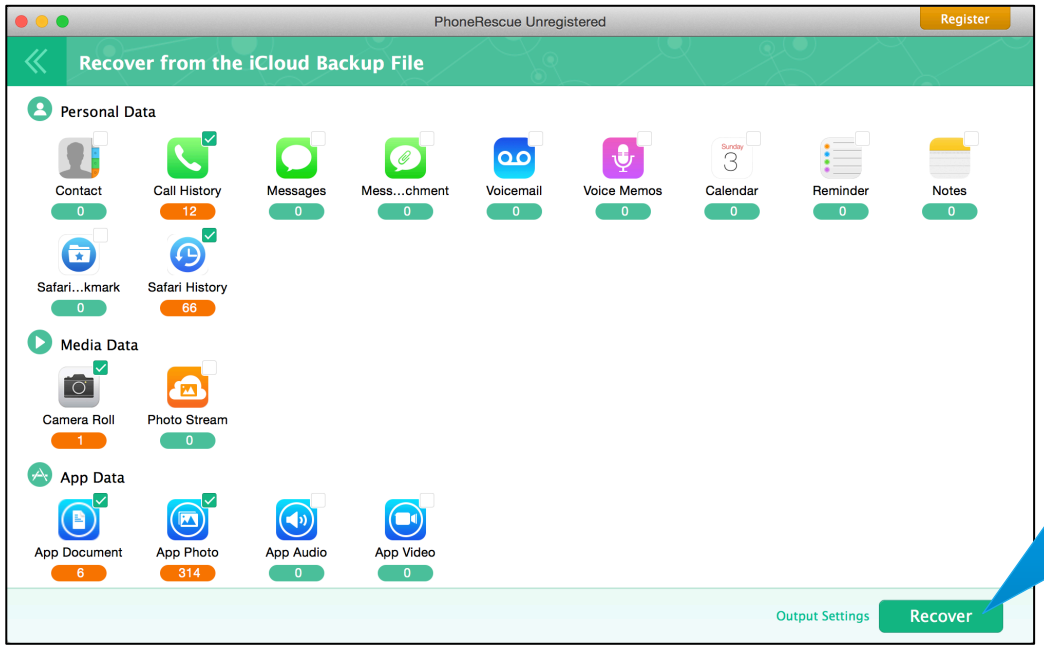
Getting to the iCloud Data
iCloud Backup Download Tools

- 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, -o 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 : [redacted]
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.apple.UIKit.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
```

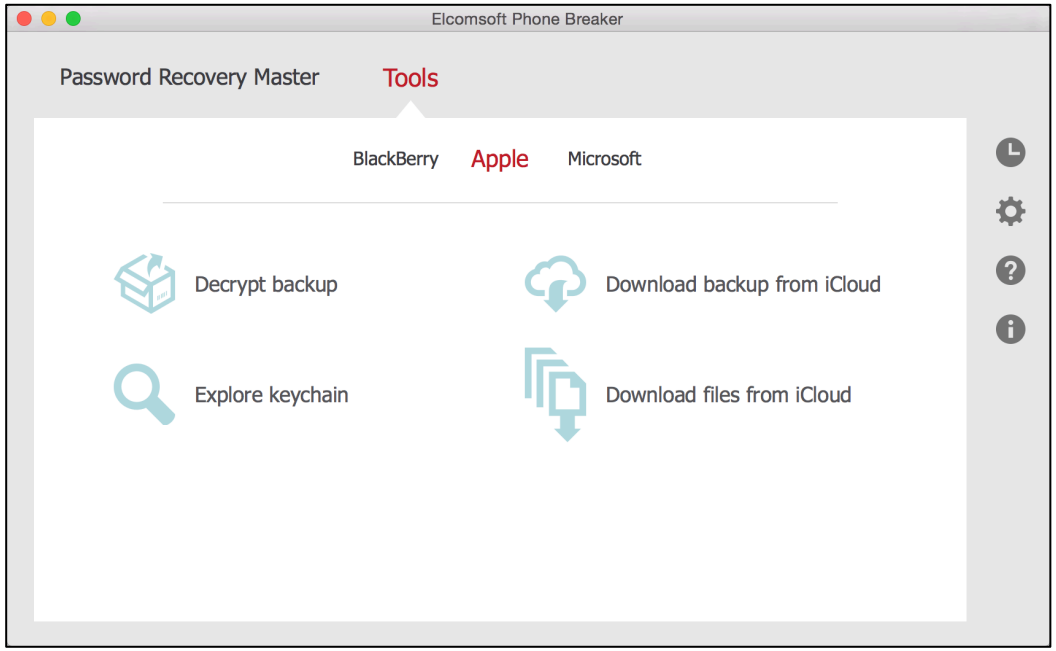
Getting to the iCloud D
iCloud Backup Downlo

- 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.google.Maps
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
```

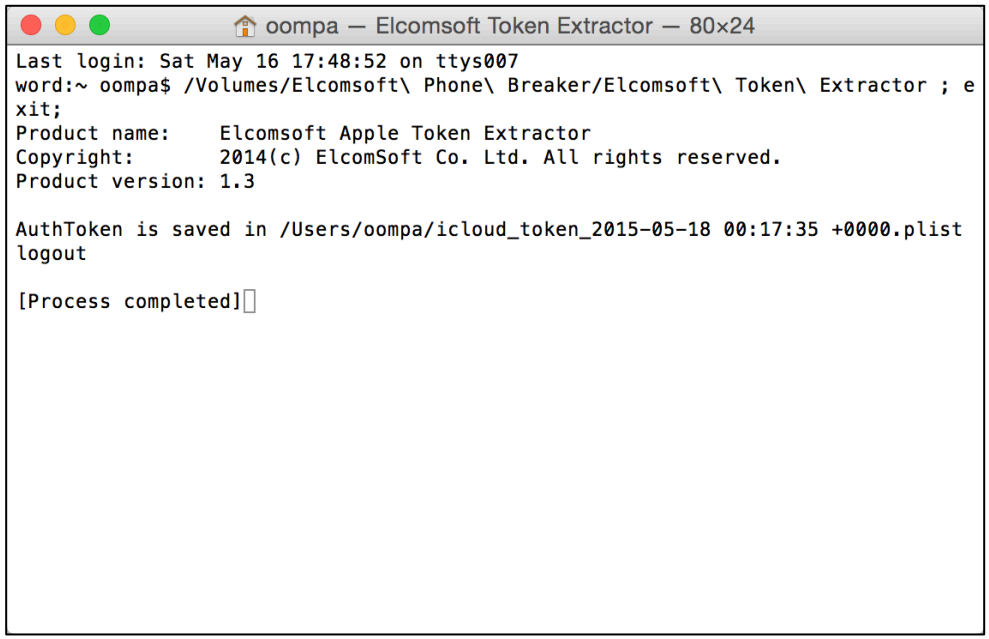
Getting to the iCloud Data
iCloud Backup Download Tools

- 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



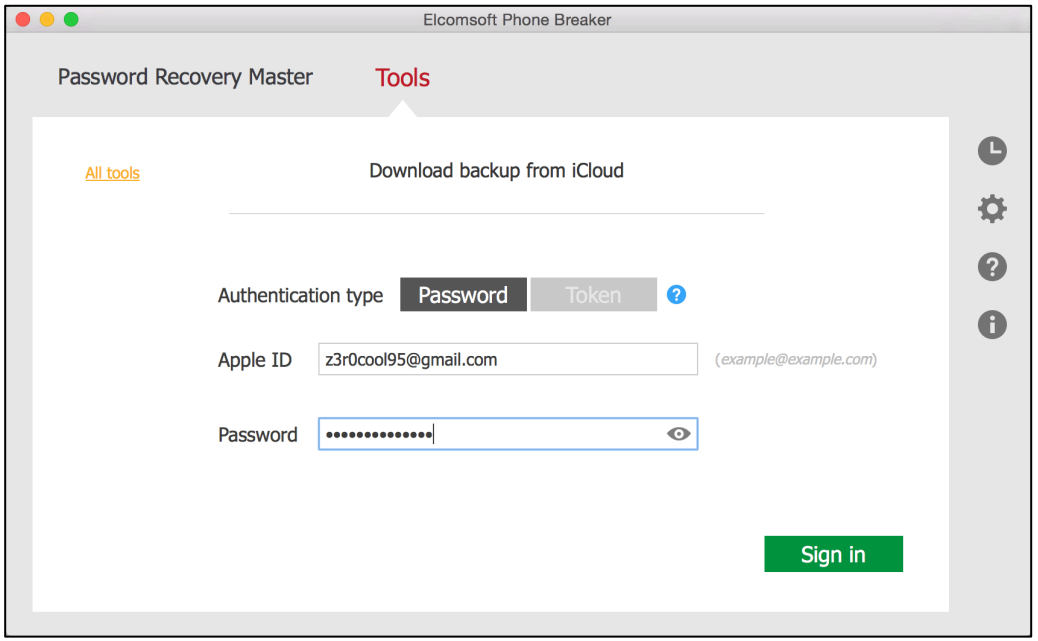
Getting to the iCloud Data
iCloud Backup Download Tools

- Elcomsoft Phone Breaker (EPPB) – Authentication Token Extraction



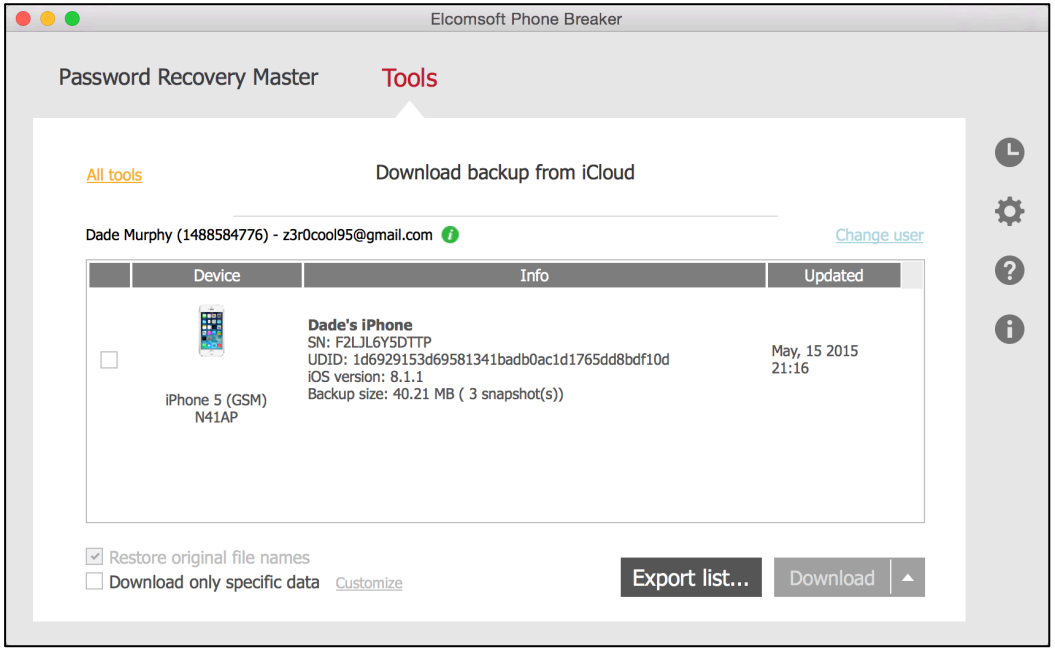
Getting to the iCloud Data
iCloud Backup Download Tools

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



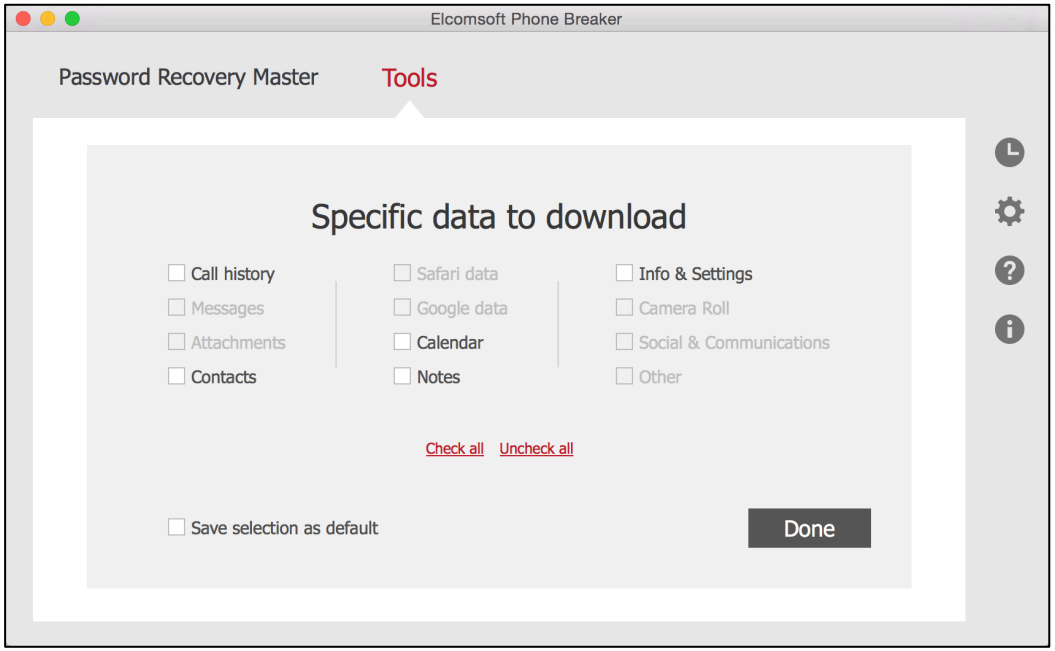
Getting to the iCloud Data
iCloud Backup Download Tools

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



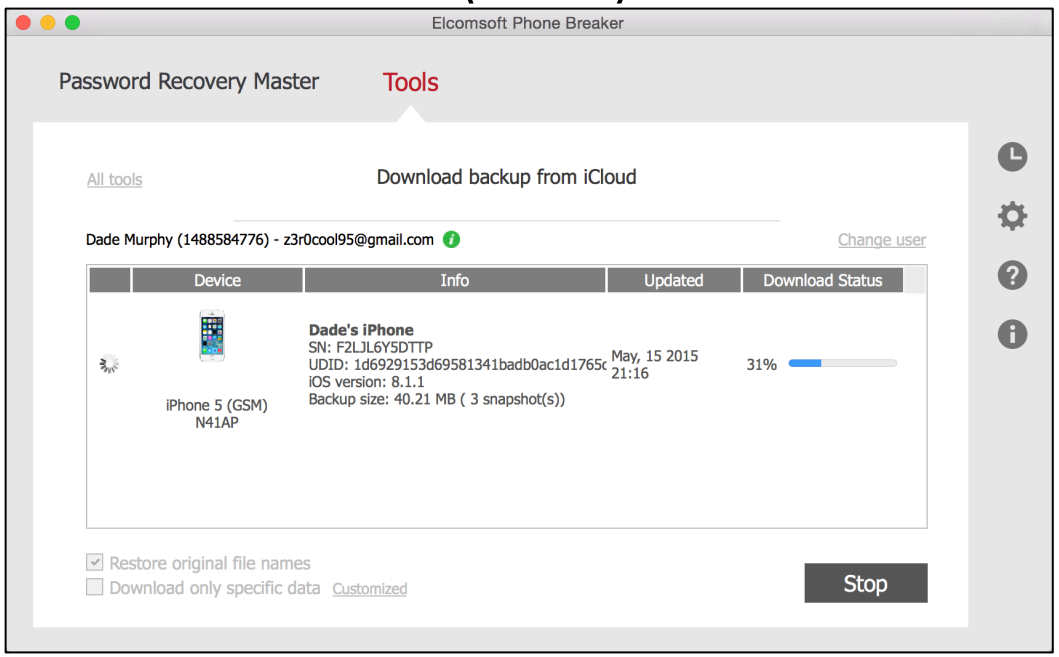
Getting to the iCloud Data
iCloud Backup Download Tools

- 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.apple.Maps-com.apple.MapsSupport.bookmarks.plist
com.apple.Maps-com.apple.MapsSupport.history.plist
com.apple.Safari-com.apple.Safari.UserRequests.plist
com.apple.Safari-com.apple.Safari.WebFeedSubscriptions.plist
com.apple.Safari.plist
com.apple.cmfsyncagent.plist
com.apple.finder.plist
com.apple.mail-com.apple.mail.vipsenders.plist
com.apple.ncplugin.stocks.plist
com.apple.ncplugin.weather.plist
com.apple.sbd.plist
com.apple.security.cloudkeychainproxy3.plist
com.apple.syncedpreferences.plist
com.apple.wifi.WiFiAgent.plist
icbaccountsd.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 3f79b21a 00000
timestamp	Number	447,904,063

Applications - Synced Preferences
Email – VIP Senders

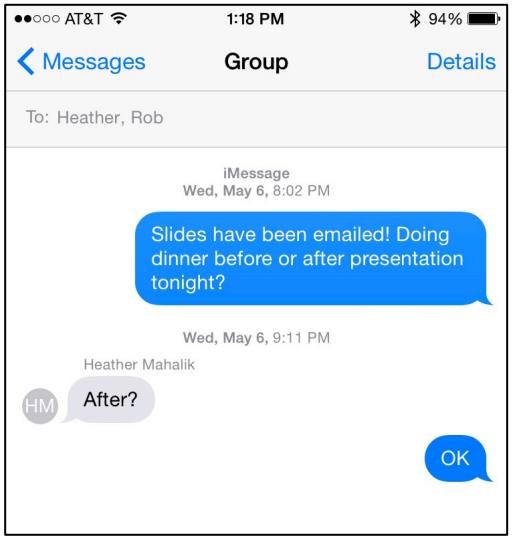
- **OS X:**
  - ~/Library/SyncedPreferences/com.apple.mail-com.apple.mail.vipsenders.plist
  - ~/Library/Containers/com.apple.mail/Data/Library/SyncedPreferences/com.apple.mail-com.apple.mail.vipsenders.plist
- **iOS:**
  - /private/var/mobile/Applications/<GUID>/Library/SyncedPreferences/com.apple.mobilemail-com.apple.mail.vipsenders.plist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

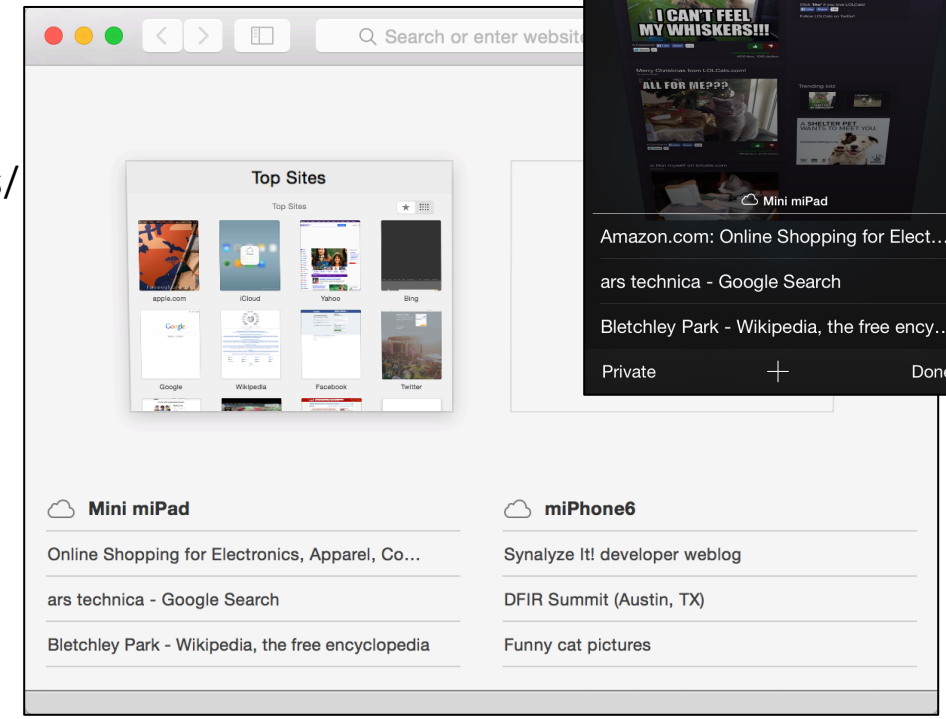
- MR = Single Recipient, GR = Group

▼ 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

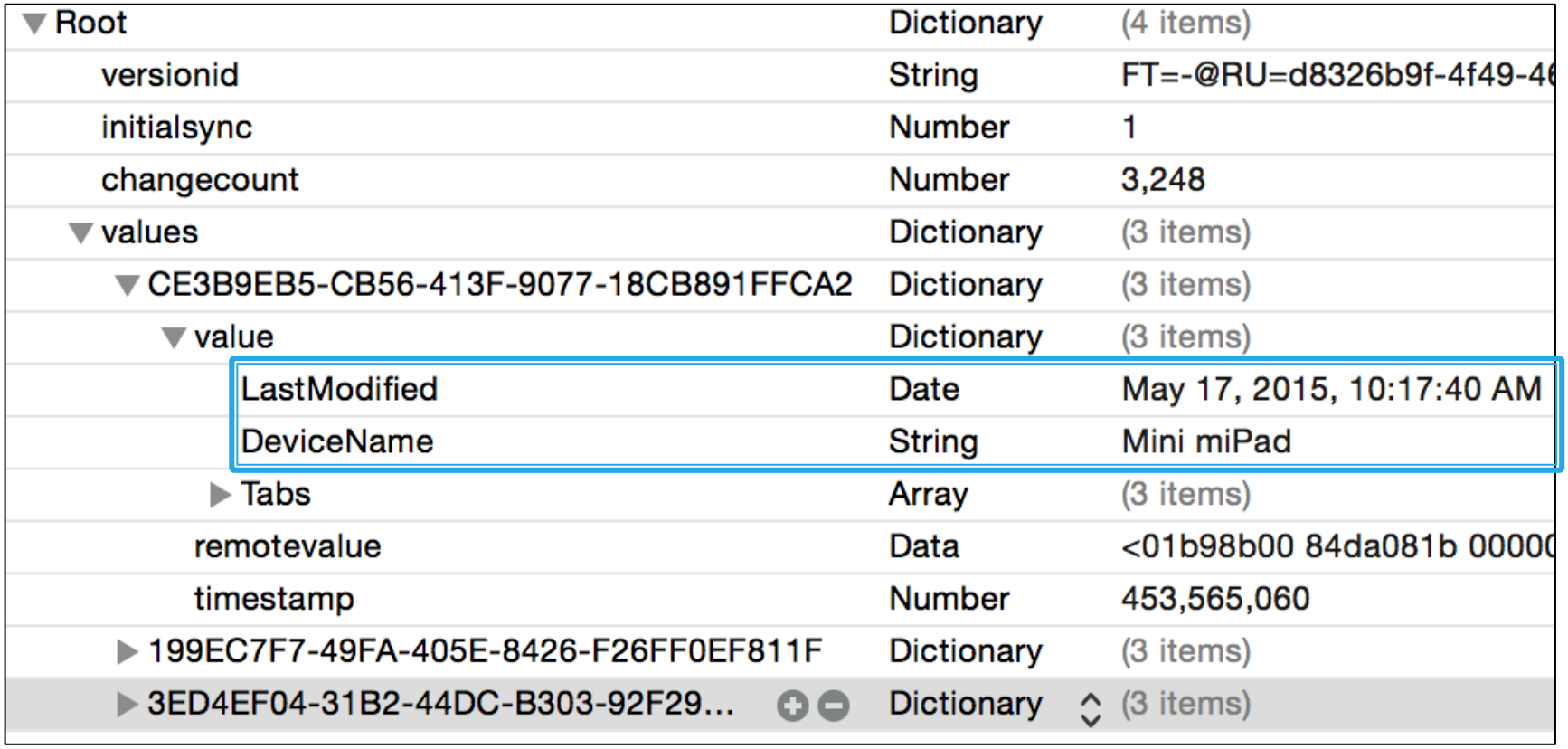
▼ GP_5F06D656864AB82329C27640B6781513	Dictionary	(3 items)
▼ value	Dictionary	(6 items)
k	String	gr
gK	Number	0
▼ t	Array	(1 item)
Item 0	Date	May 6, 2015, 8:02:16 PM
▼ mrs	Array	(2 items)
▼ Item 0	Dictionary	(3 items)
n	String	Rob Lee
a	String	+1[redacted]
k	String	phone
▼ Item 1	Dictionary	(3 items)
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

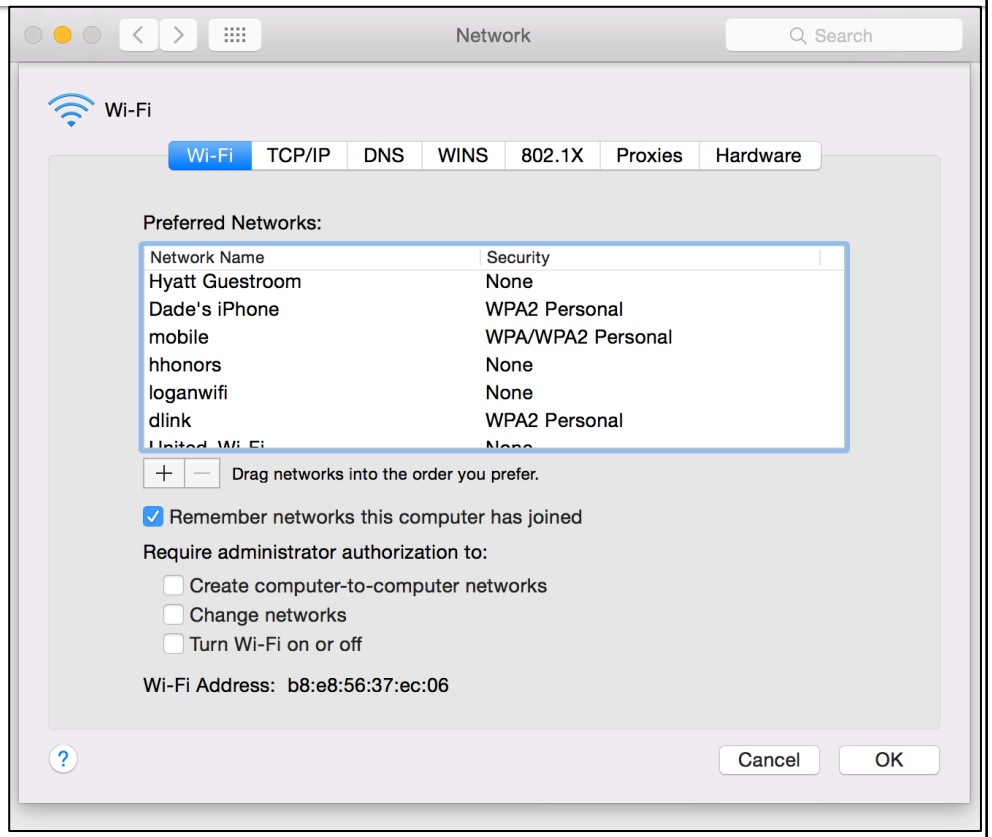


Applications - Synced Preferences
Safari – Synced Tabs

▼ 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 d5010
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

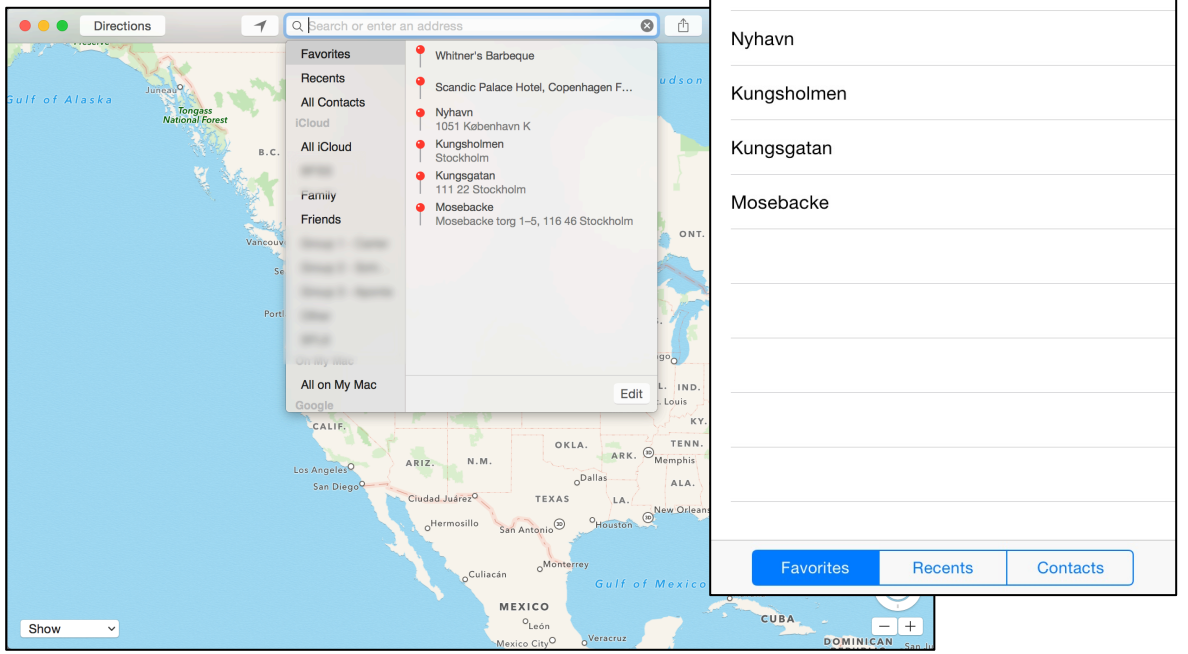
Key	Type	Value
▼ Root	Dictionary	(4 items)
versionid	String	FT=-@RU=c
initialsync	Number	5
changecount	Number	30
▼ values	Dictionary	(37 items)
▶ FOR518	Dictionary	(3 items)
▶ Reagan National WiFi	Dictionary	(3 items)
▶ Parsons_Visitor	Dictionary	(3 items)
▶ ASUS	Dictionary	(3 items)
▶ SJ	Dictionary	(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 0(
timestamp	Number	450,457,431

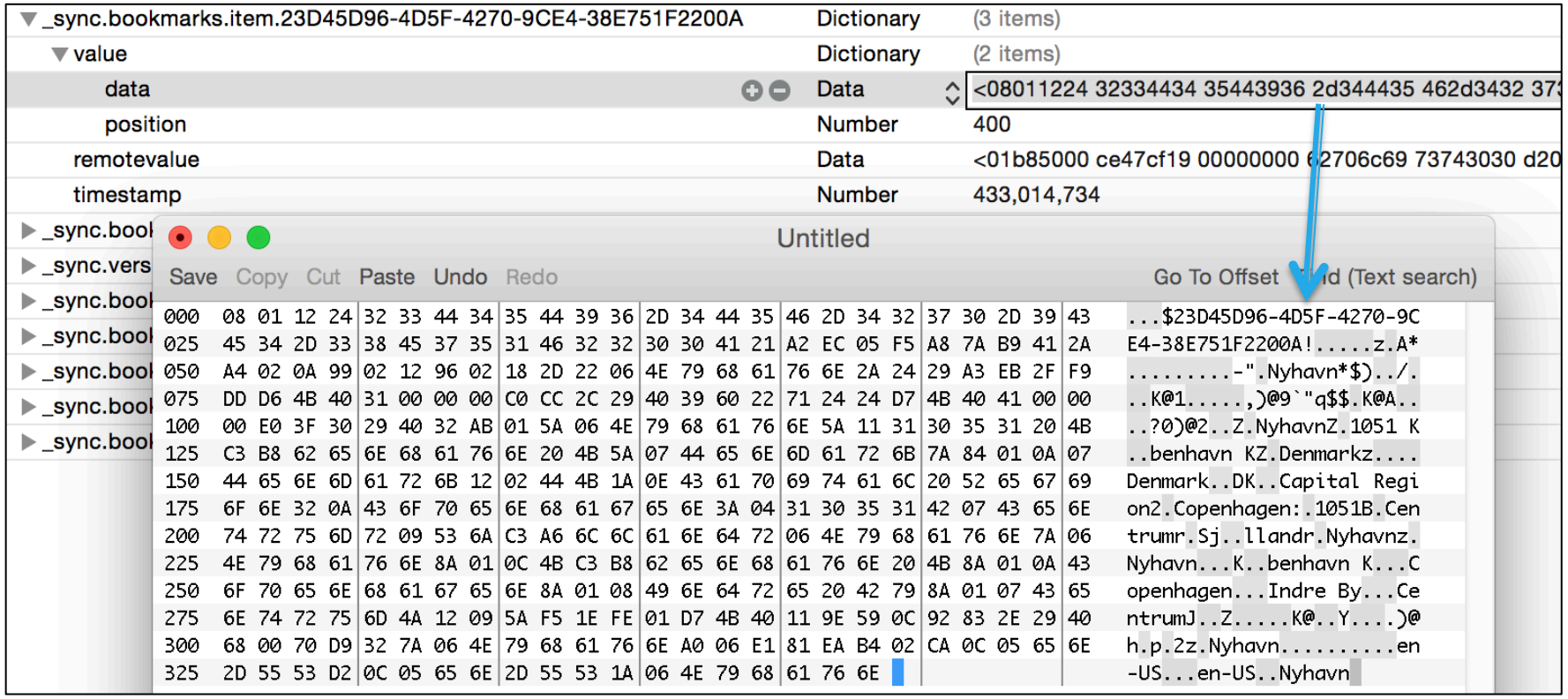
Applications - Synced Preferences
Maps – Synced Bookmarks (Favorites)

OS X:
~/Library/SyncedPreferences/
com.apple.Maps-
com.apple.MapsSupport.bookmarks.plist
~/Library/Containers/com.apple.Maps/
Data/Library/SyncedPreferences/
com.apple.Maps-
com.apple.MapsSupport.bookmarks.plist

iOS:
/private/var/mobile/Library/
SyncedPreferences/com.apple.Maps.plist
/private/var/mobile/Containers/Data/
Application/<GUID>/Library/
SyncedPreferences/com.apple.Maps-
com.apple.MapsSupport.bookmarks.plist

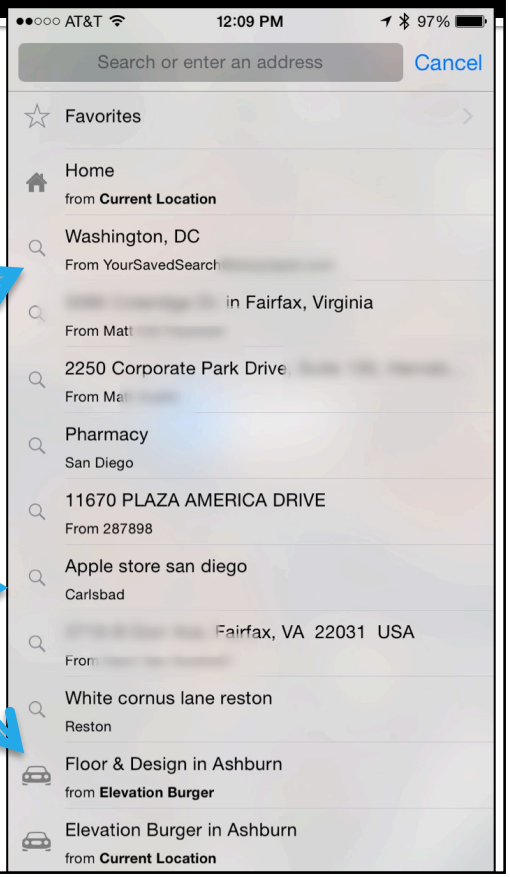


Applications - Synced Preferences
Maps – Bookmarks (Favorites)



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.apple.Maps-com.apple.MapsSupport.history.plist
  - /Users/oompa/Library/Containers/com.apple.Maps/Data/Library/SyncedPreferences/com.apple.Maps-com.apple.MapsSupport.history.plist
- **iOS:**
  - /private/var/mobile/Library/SyncedPreferences/com.apple.Maps-com.apple.Maps.recents.plist
  - /private/var/mobile/Containers/Data/Application/<GUID>/Library/SyncedPreferences/com.apple.Maps-com.apple.Maps.recents.plist
  - /private/var/mobile/Containers/Data/Application/<GUID>/Library/SyncedPreferences/com.apple.Maps-com.apple.MapsSupport.history.plist

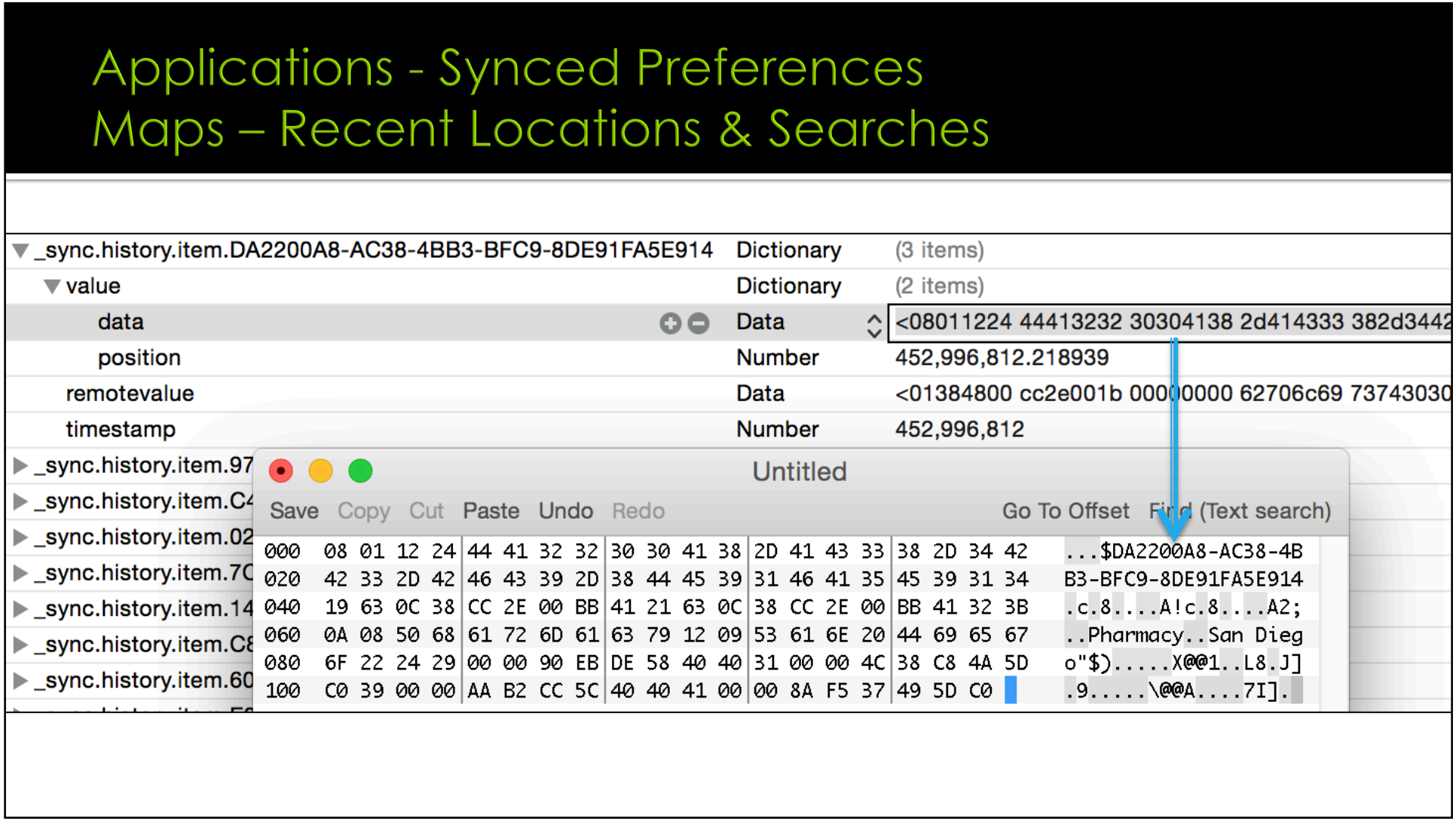


Applications - Synced Preferences
Maps – Recent Addresses

- Extracted from Mail emails – "From…"

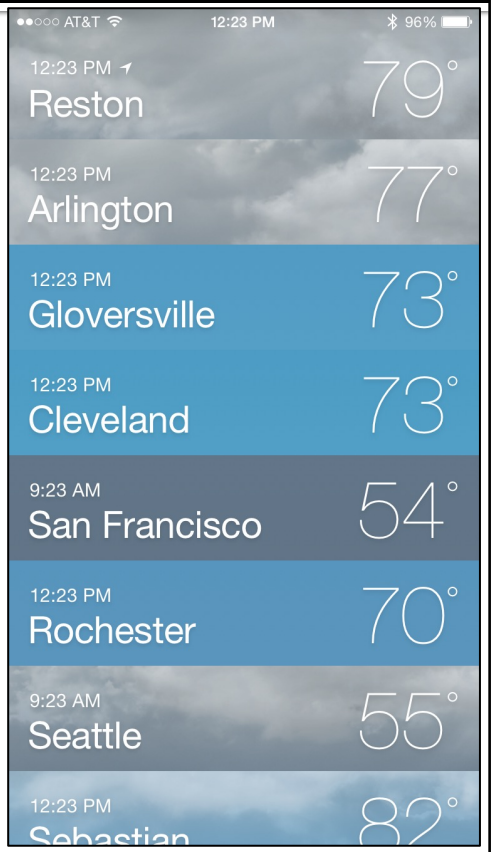
▼ MR_F8EA2DAFA7D6877F5B232D00534B0797558A5D6C	Dictionary	(3 items)
▼ value	Dictionary	(7 items)
k	String	m
▼ t	Array	(4 items)
Item 0	Date	Apr 26, 2015, 9:58:31 AM
Item 1	Date	Apr 26, 2015, 7:25:33 AM
Item 2	Date	Apr 15, 2015, 8:26:02 PM
Item 3	Date	Apr 15, 2015, 7:35:59 PM
▼ m	Dictionary	(4 items)
▼ 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



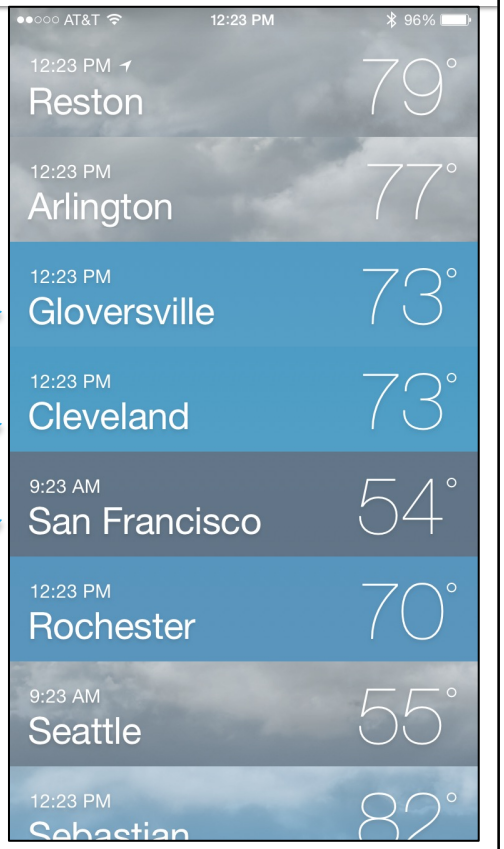
Applications - Synced Preferences Weather

- **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



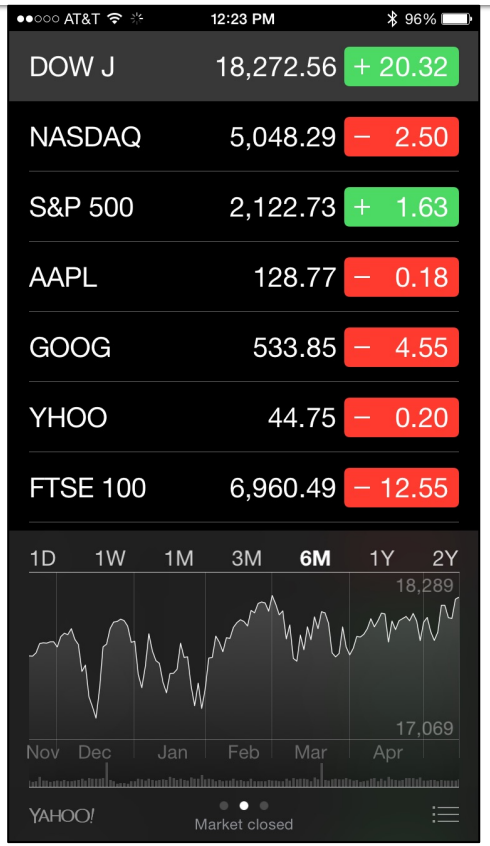
Applications - Synced Preferences
Weather – Synced Cities

▼ 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



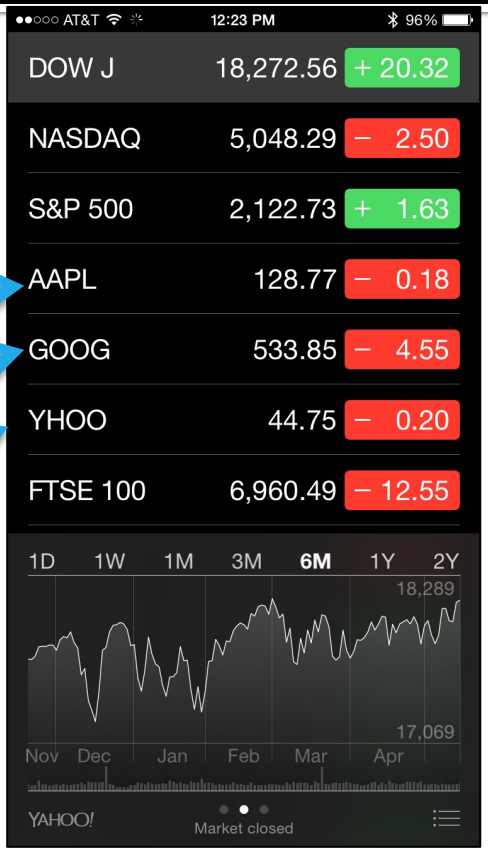
Applications - Synced Preferences Stocks

- **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



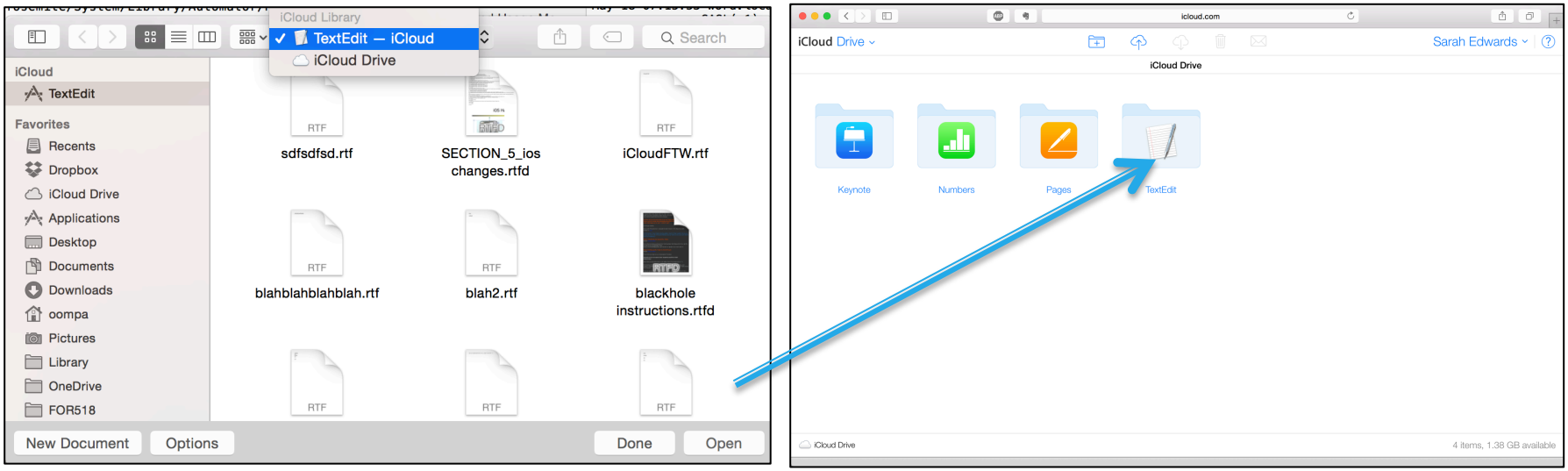
Applications - Synced Preferences
Stocks – Synced Stock Symbols

▼ 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

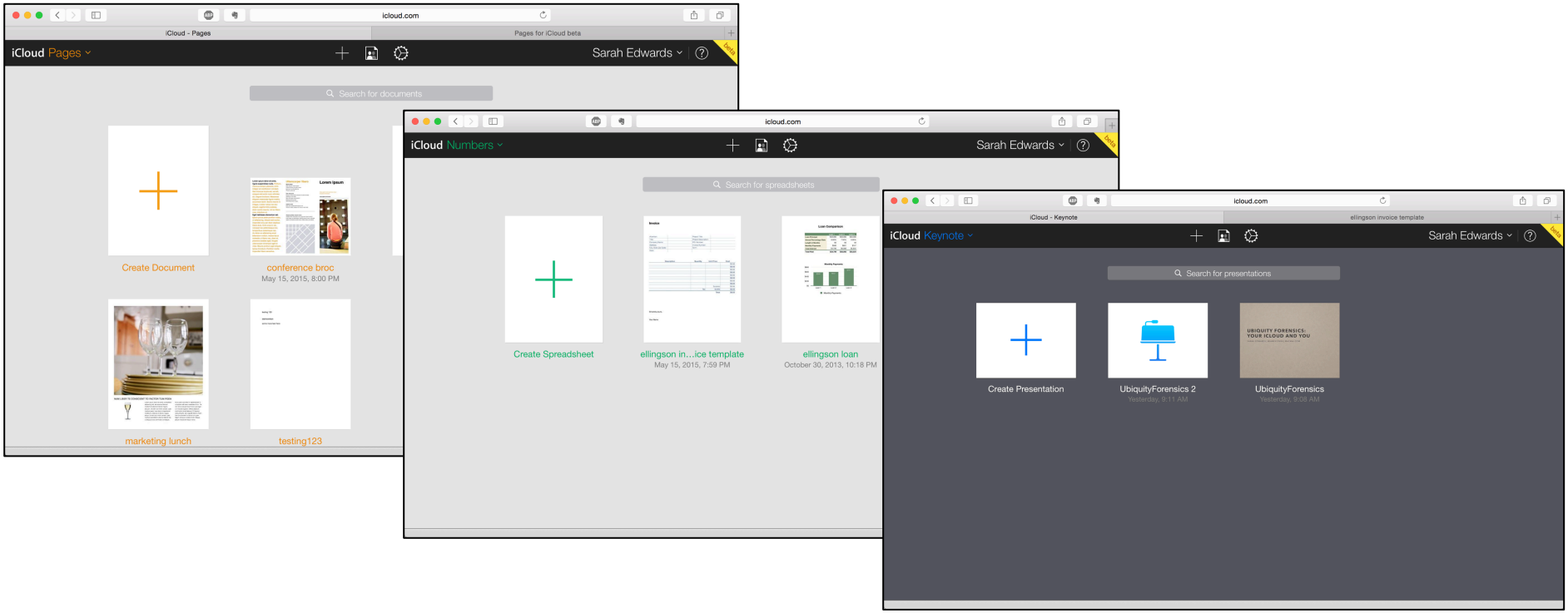


Application Data

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

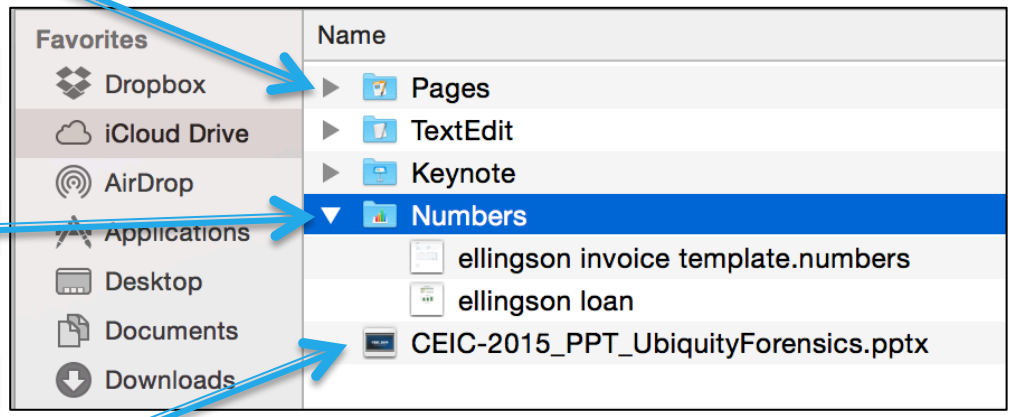
- ~/Library/Mobile Documents/ com~apple~Numbers/

TextEdit

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

Other

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



Applications – Documents
iWork & TextEdit – Mobile Documents

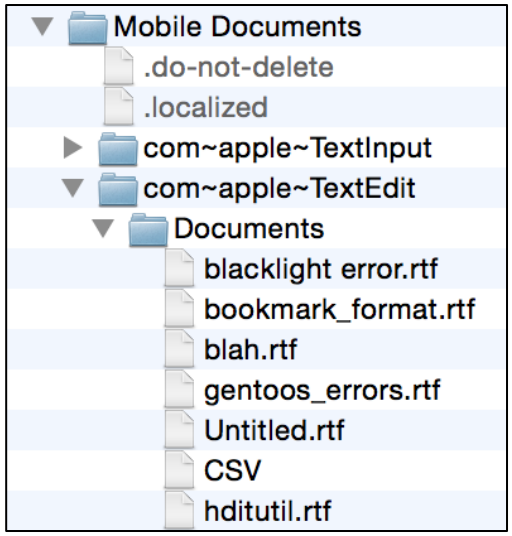
```
word:com~apple~Numbers oompa$ pwd
/Users/oompa/Library/Mobile Documents/com~apple~Numbers
word:com~apple~Numbers oompa$ tree .
.
├── Documents
│   ├── ellingson invoice template.numbers
│   │   ├── Data
│   │   ├── Index.zip
│   │   ├── Metadata
│   │   │   ├── BuildVersionHistory.plist
│   │   │   ├── 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

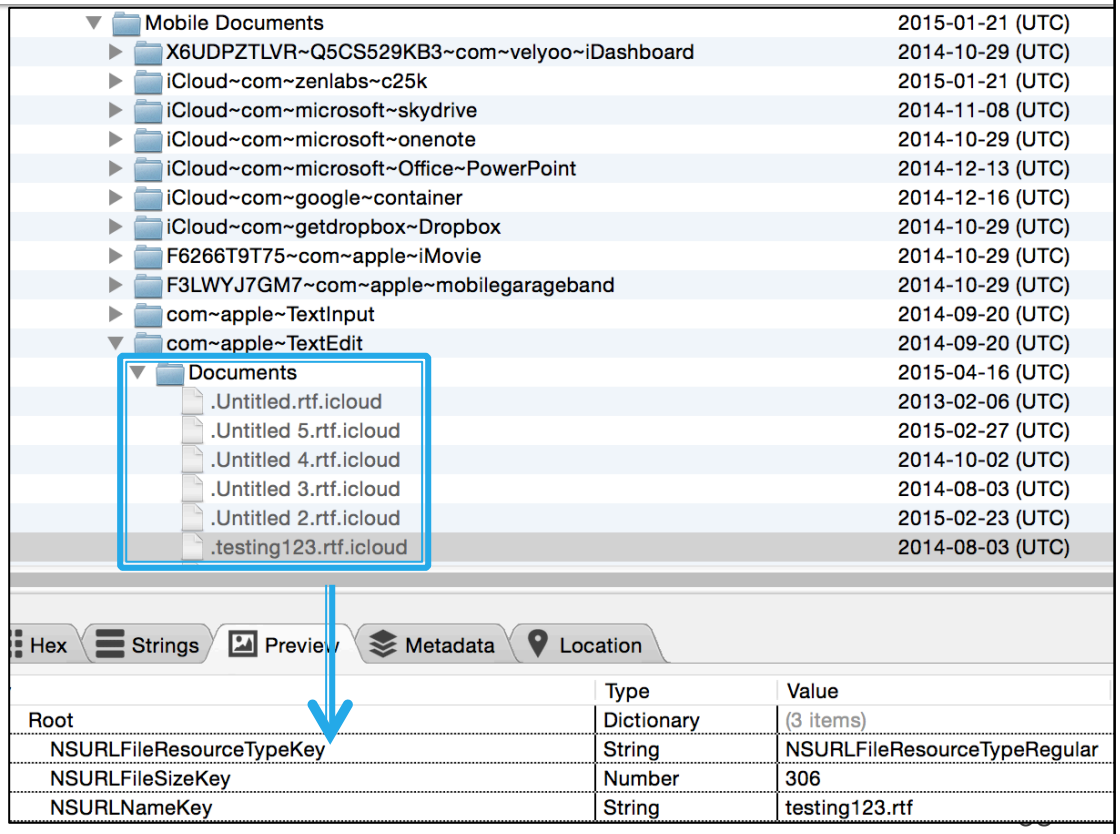
- iOS: /private/var/mobile/Library/Mobile Documents/




```
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

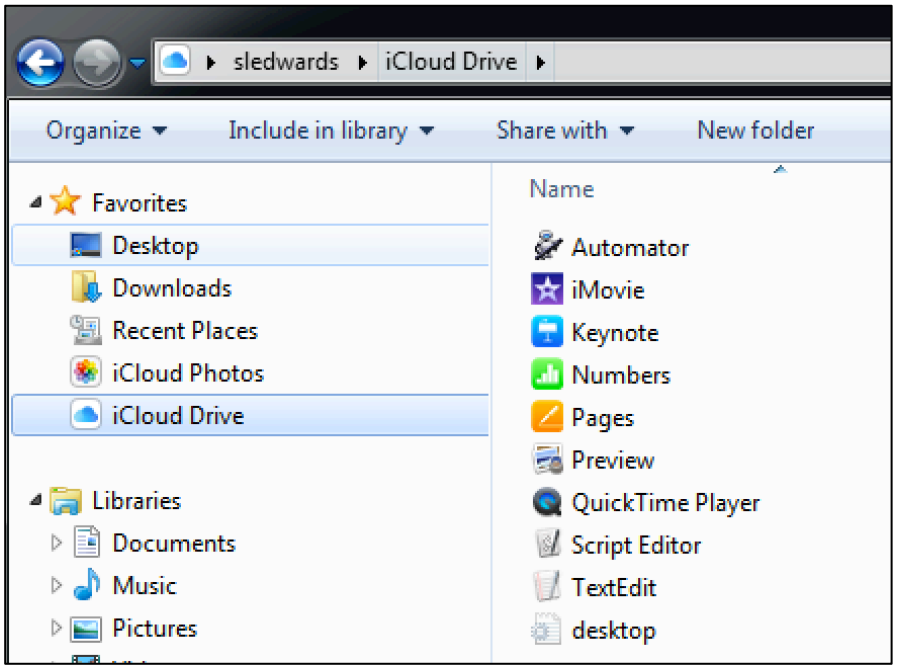
- Follows same structure
- However…
- Hidden plist files
- <document_name>.icloud
- Theories
  - Files had yet to be downloaded to device?
  - Pointer Records?
  - Image acquired in strange state?



Applications – Documents
iWork & TextEdit – Mobile Documents on Windows

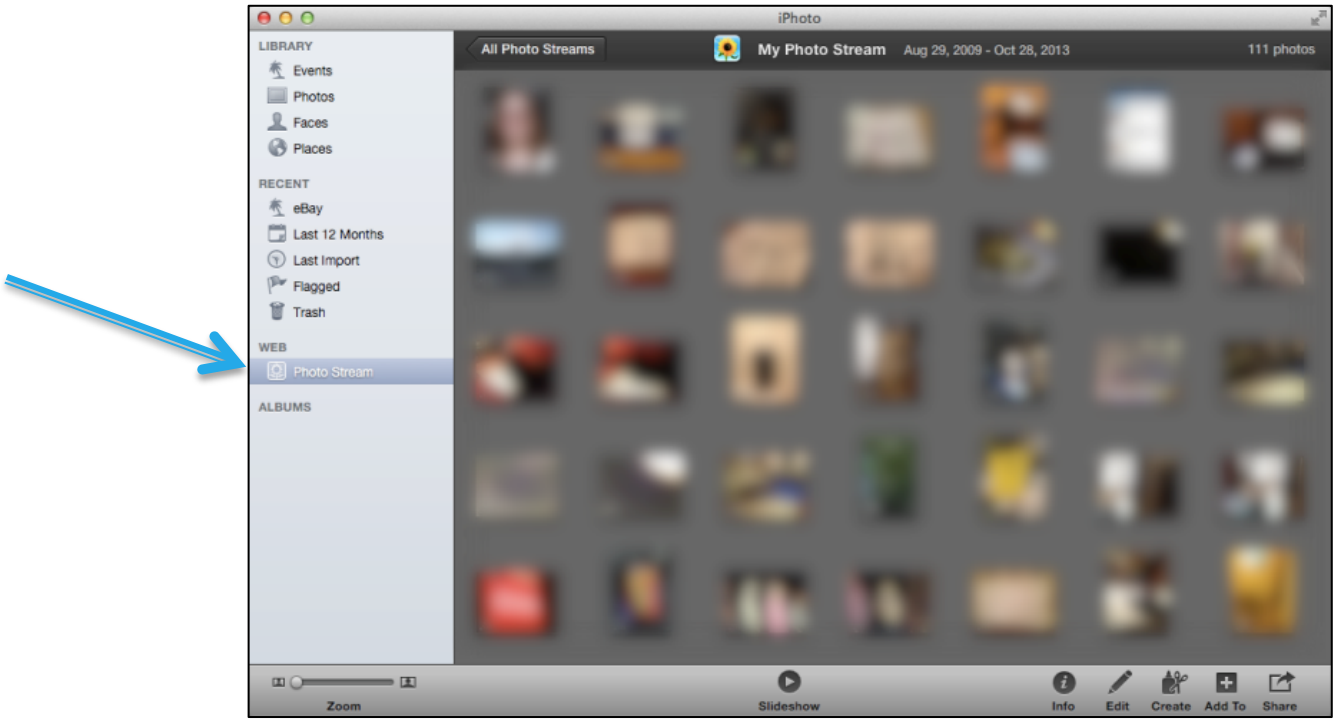
- Similar directory structure:
  - com~apple~KeyNote (Pages, Numbers, TextEdit)

```
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/



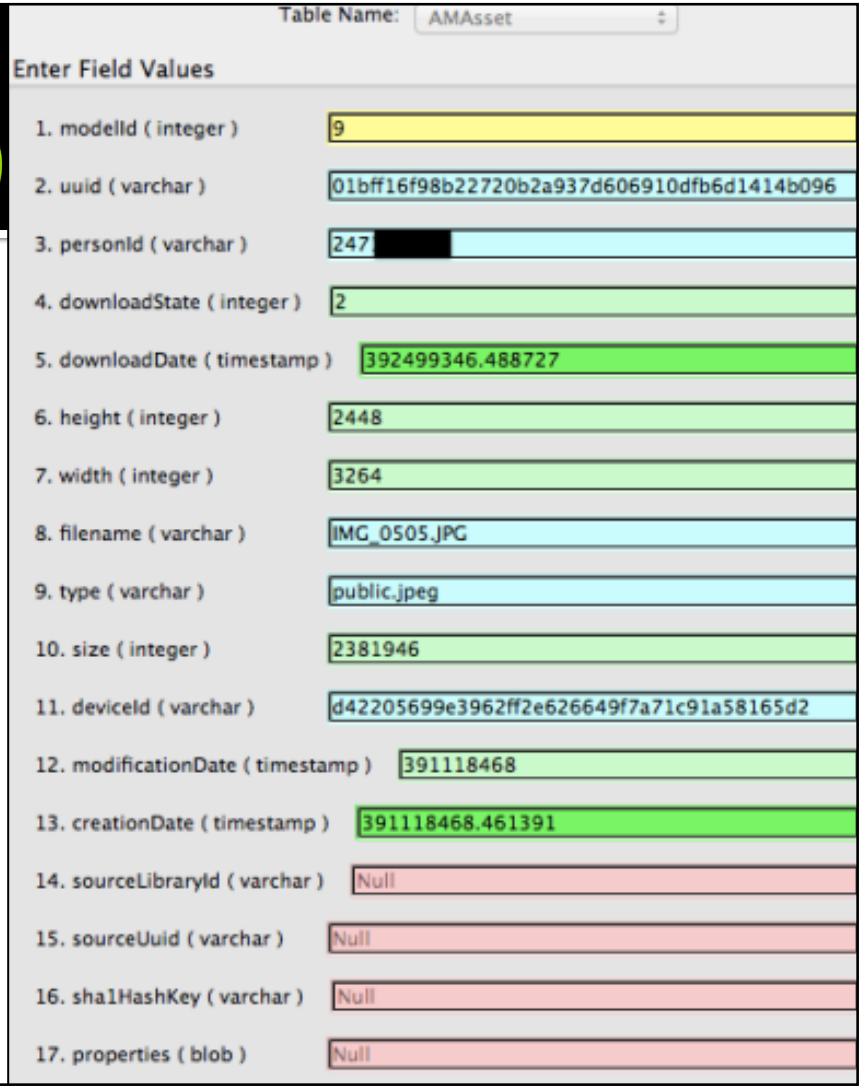
Applications
Photos – iPhoto (Legacy Application)

- 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)

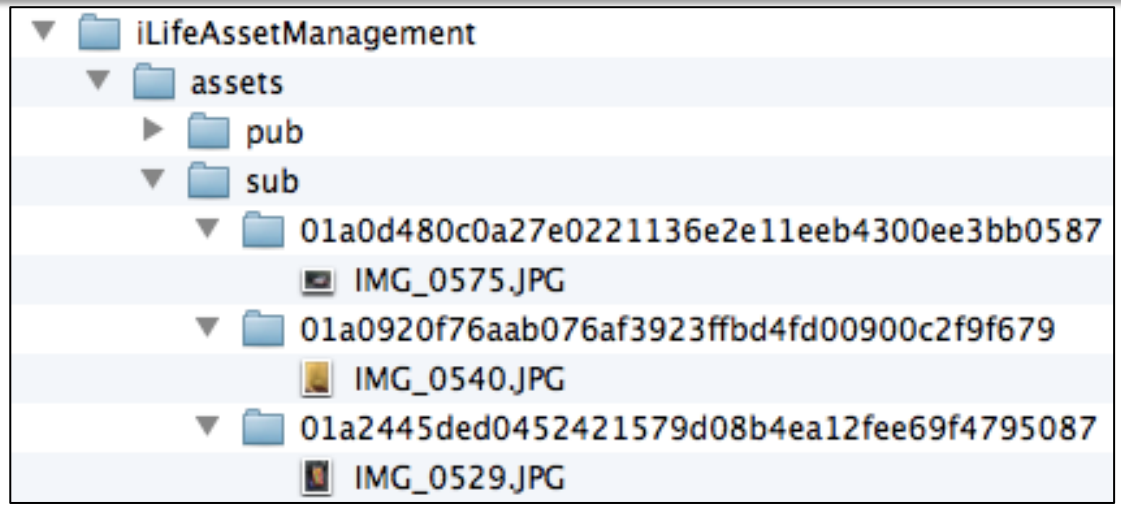
- OS X – iLifeAssetManagement.db
- SQLite Database
- Contains iCloud photo metadata in AMAsset table:
  - Photo UUID
  - iCloud Person ID
  - Timestamps (Downloaded, Modified, Created)
  - Height/Width
  - Filename
  - File Size
  - Device UDID



Applications
Photos – iPhoto (Legacy Application)

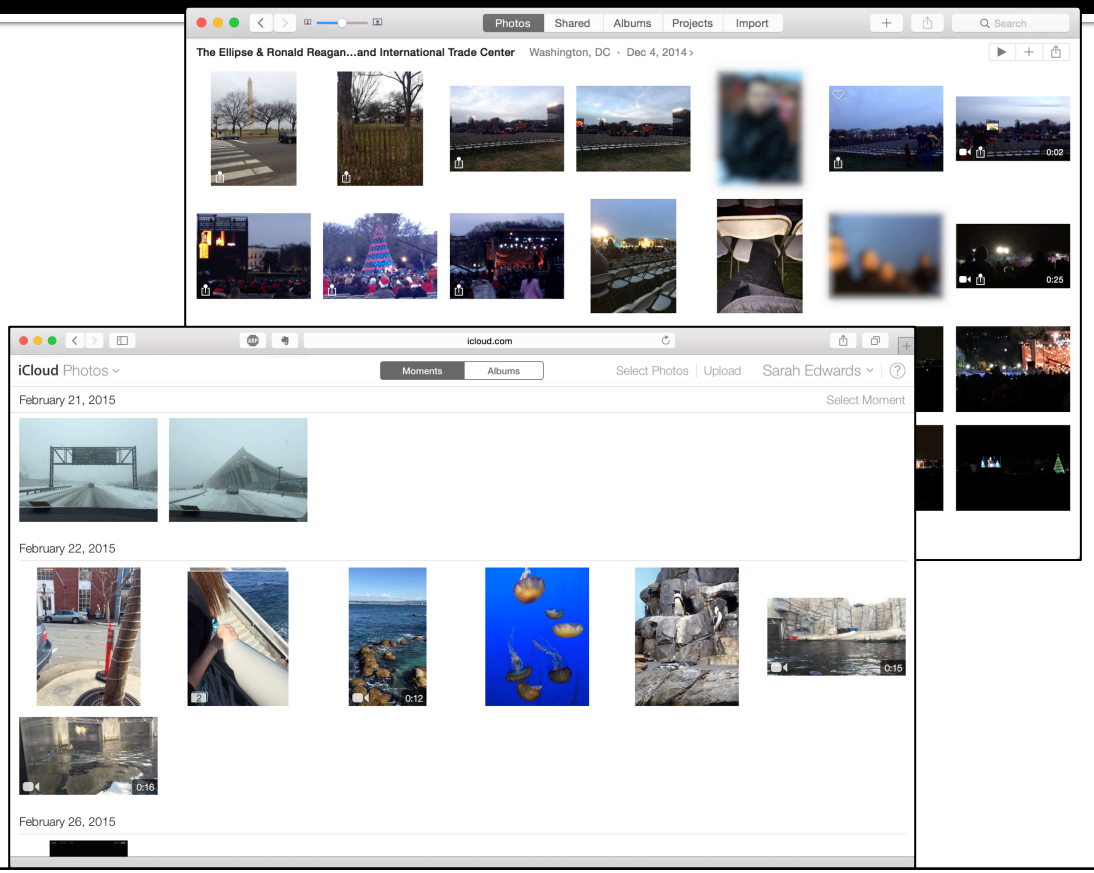
Your Photo Stream Photos - sub/

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 = cloudphotosd, iCloud

```
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;cl|
00000010  6F 75 64 70 68 6F 74 6F 73 64 3B                 |oudphotosd;|
0000001b
```

```
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
```

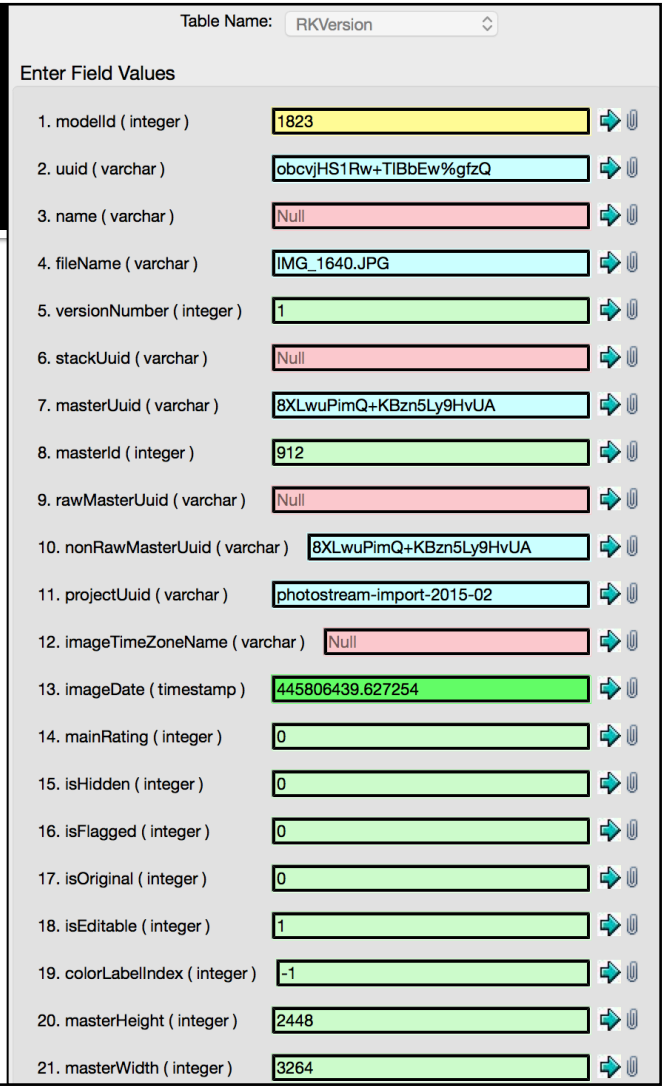
Applications
Photos – New Photos Application

- 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
lrwxr-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
lrwxr-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
lrwxr-xr-x@  1 oompa  staff        17 May 15 18:21 History.apdb -> apdb/History.apdb
lrwxr-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
lrwxr-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
lrwxr-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. ☹



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/*

```
miPhone5s:/private/var/mobile/Media/PhotoStreamsData/[redacted]/.MISC root# pwd
/private/var/mobile/Media/PhotoStreamsData/24713276/.MISC
miPhone5s:/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";
    kPLLocalMSMetadataAssetPLUUIDKey = "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;
}
```

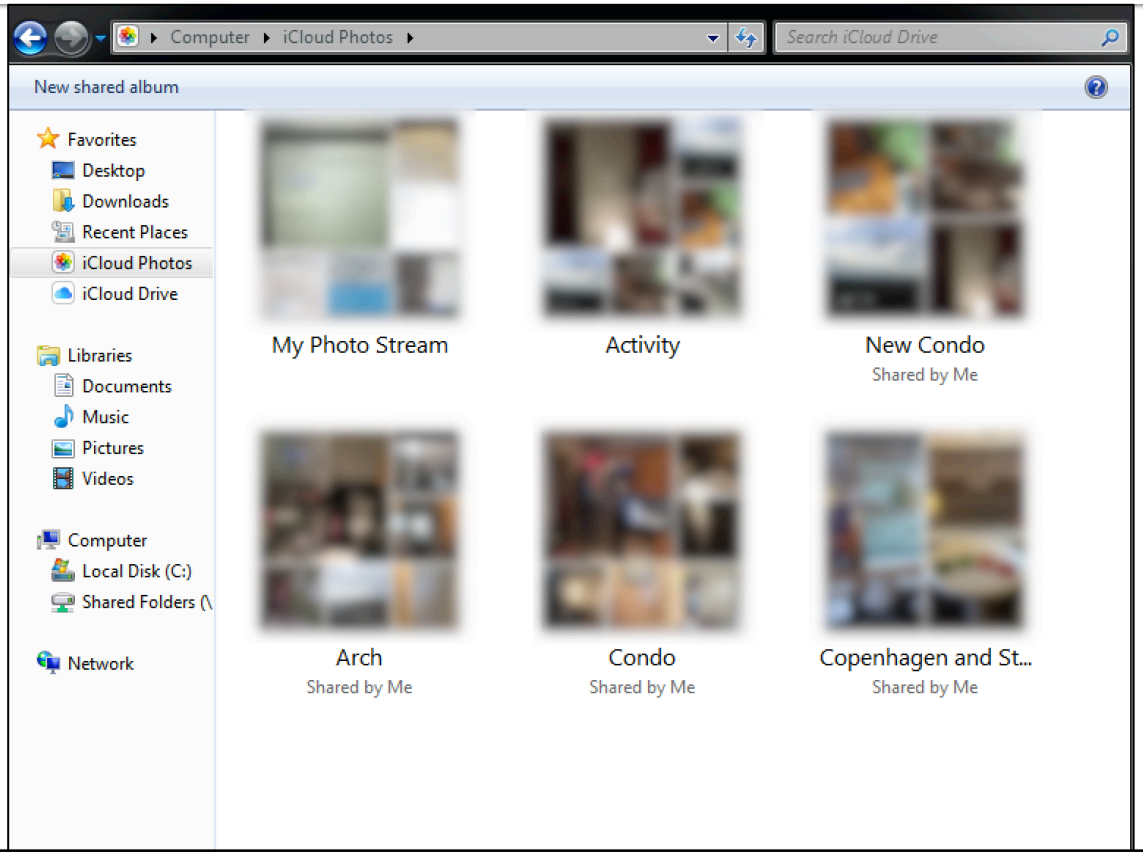
Applications
Photos – New Photos Application – Shared Albums

- 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

```
miPhone5s:/private/var/mobile/Media/PhotoData/PhotoCloudSharingData/[redacted] root# pwd
/private/var/mobile/Media/PhotoData/PhotoCloudSharingData/[redacted]
miPhone5s:/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
miPhone5s:/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";
}
```

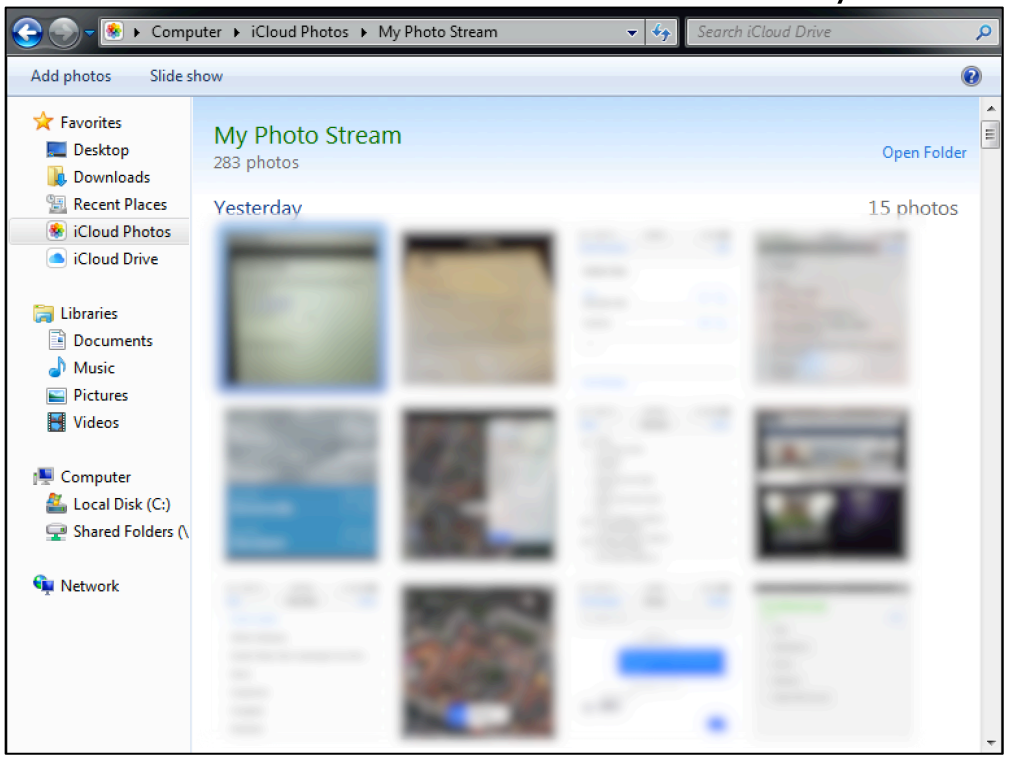
Applications
Photos – On Windows – iCloud Photos

- "My Photo Stream"
- "Shared"
  - "New Condo"
  - "Arch"
  - "Condo"
  - "Copenhagen and St…"



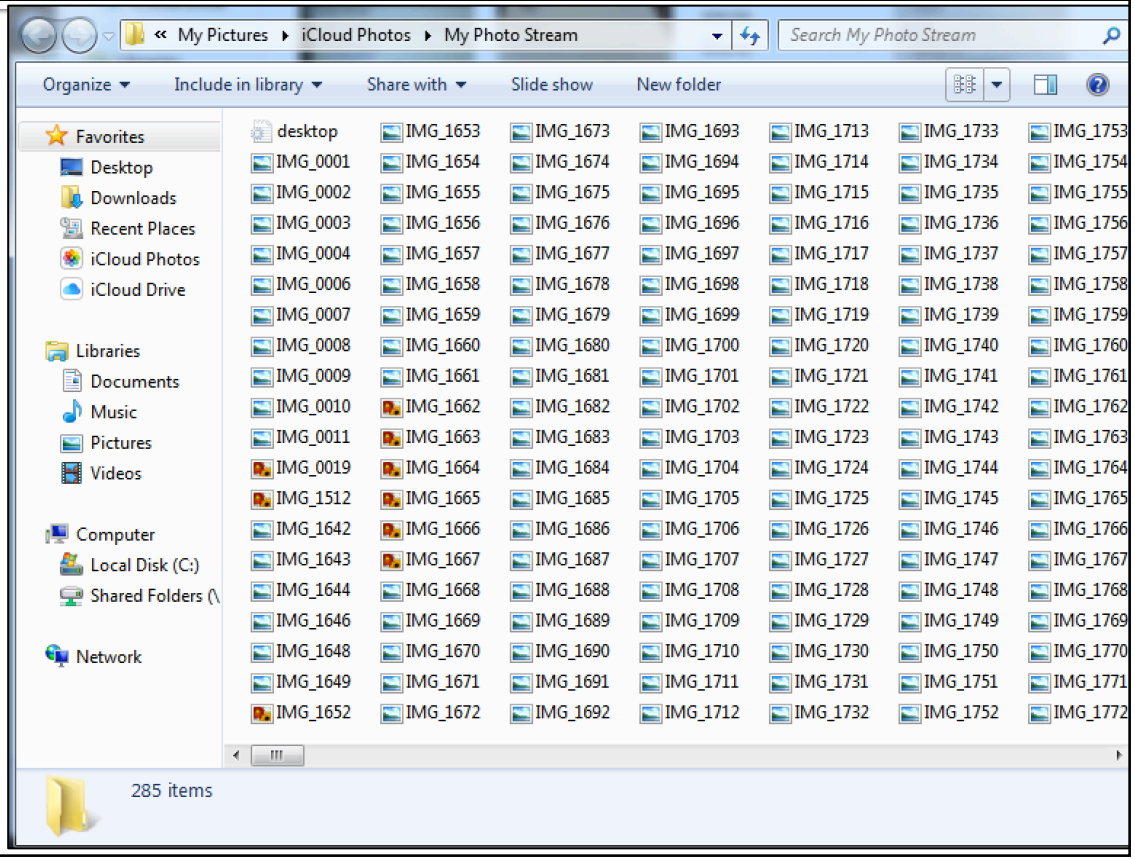
Applications
Photos – On Windows – My Photo Stream

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



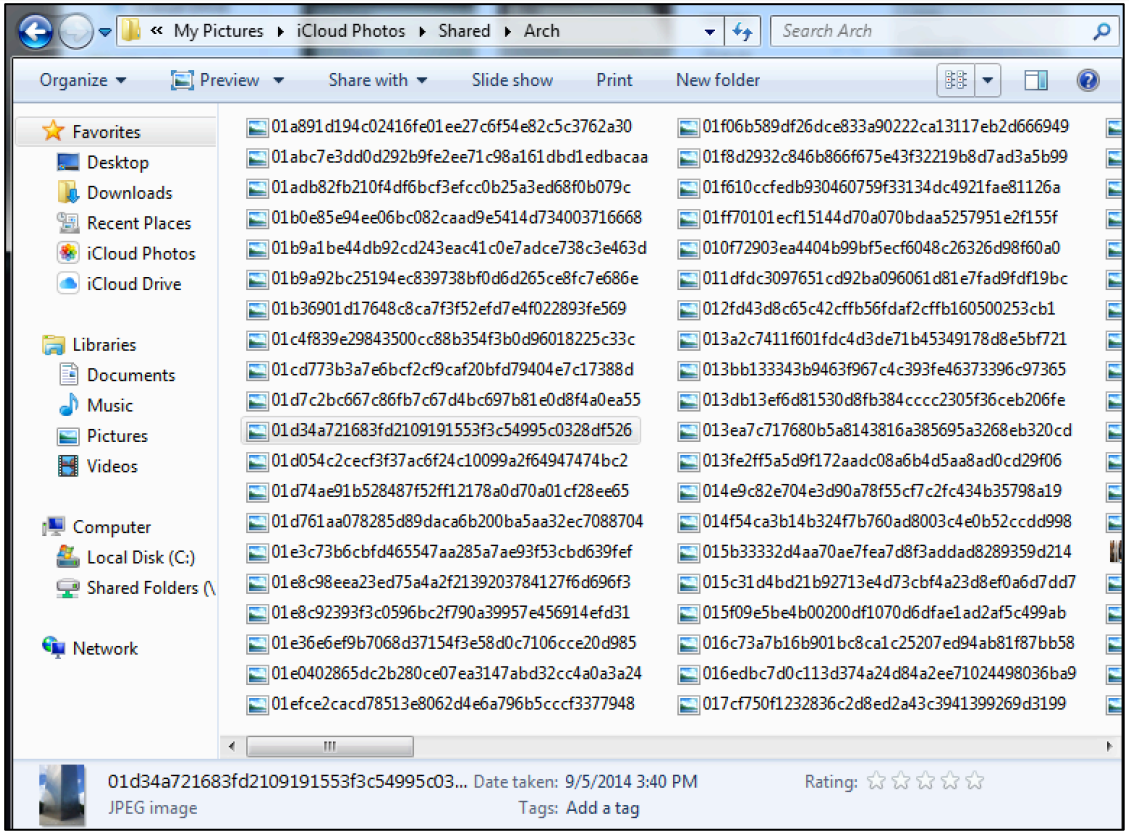
Applications
Photos – On Windows – My Photo Stream

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



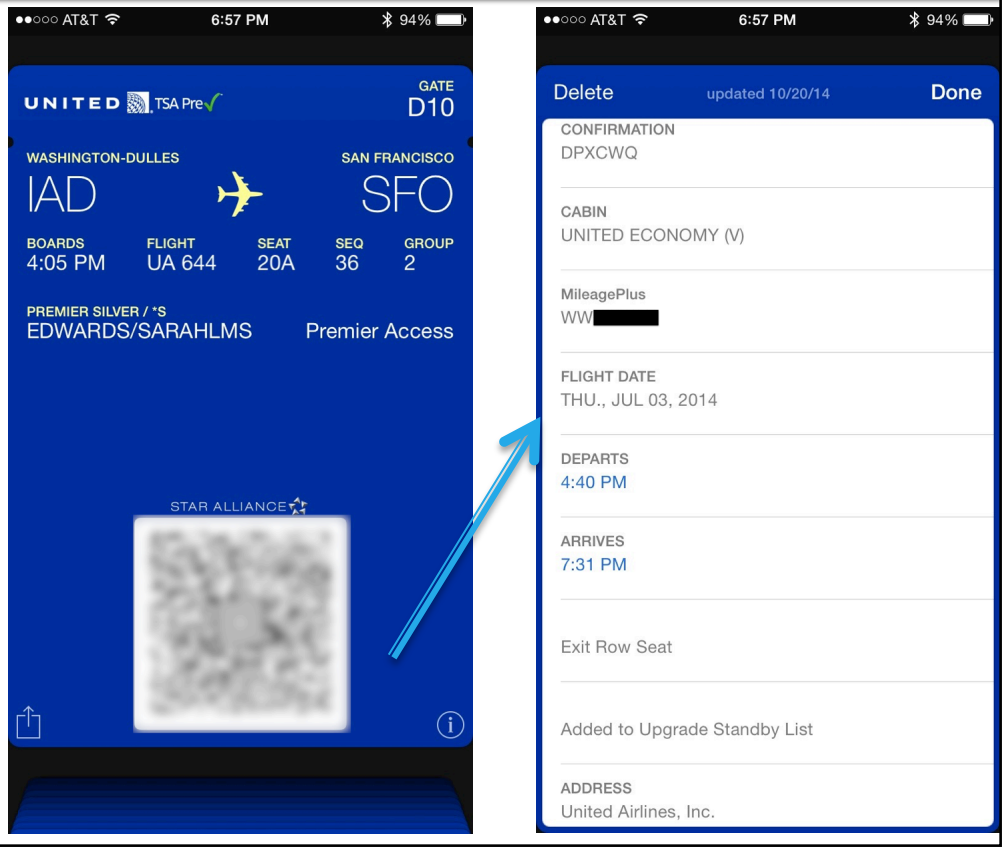
Applications
Photos – On Windows – Shared Albums

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



Applications
Passbook Passes

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



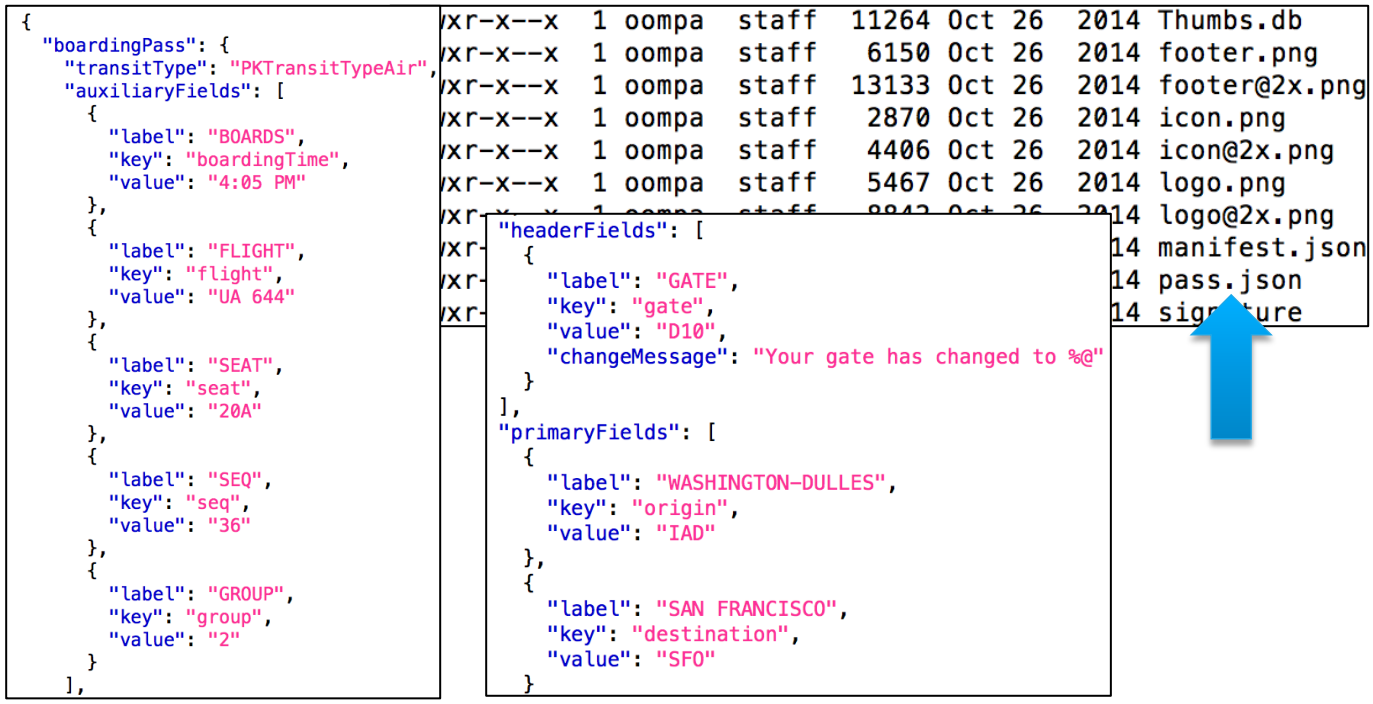
Applications
Passbook Passes - *.pkpass Files

```
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-cM9ac3eFNA9iCZ0mbkGqaN1OE=.pkpass
drwxr-xr-x   9 oompa  staff  306 Jul 26  2014 07DvKQIpN4QMgdtfi5miHNJWHmQ=.pkpass
drwxr-xr-x  12 oompa  staff  408 Aug 10  2014 0cxFFcwnrkgt7WihgBXO7v4qr7I=.pkpass
drwxr-xr-x  11 oompa  staff  374 Oct 11  2014 1Ky0sMM7V4TVHm8wtU5LSb7GL9k=.pkpass
drwxr-xr-x  12 oompa  staff  408 Jan 14 15:30 3FM0j7C76ZUQaJmO1GSeG8dAsfQ=.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 8xONuOBO4WA0FfSGlV4cC21bvC8=.pkpass
```

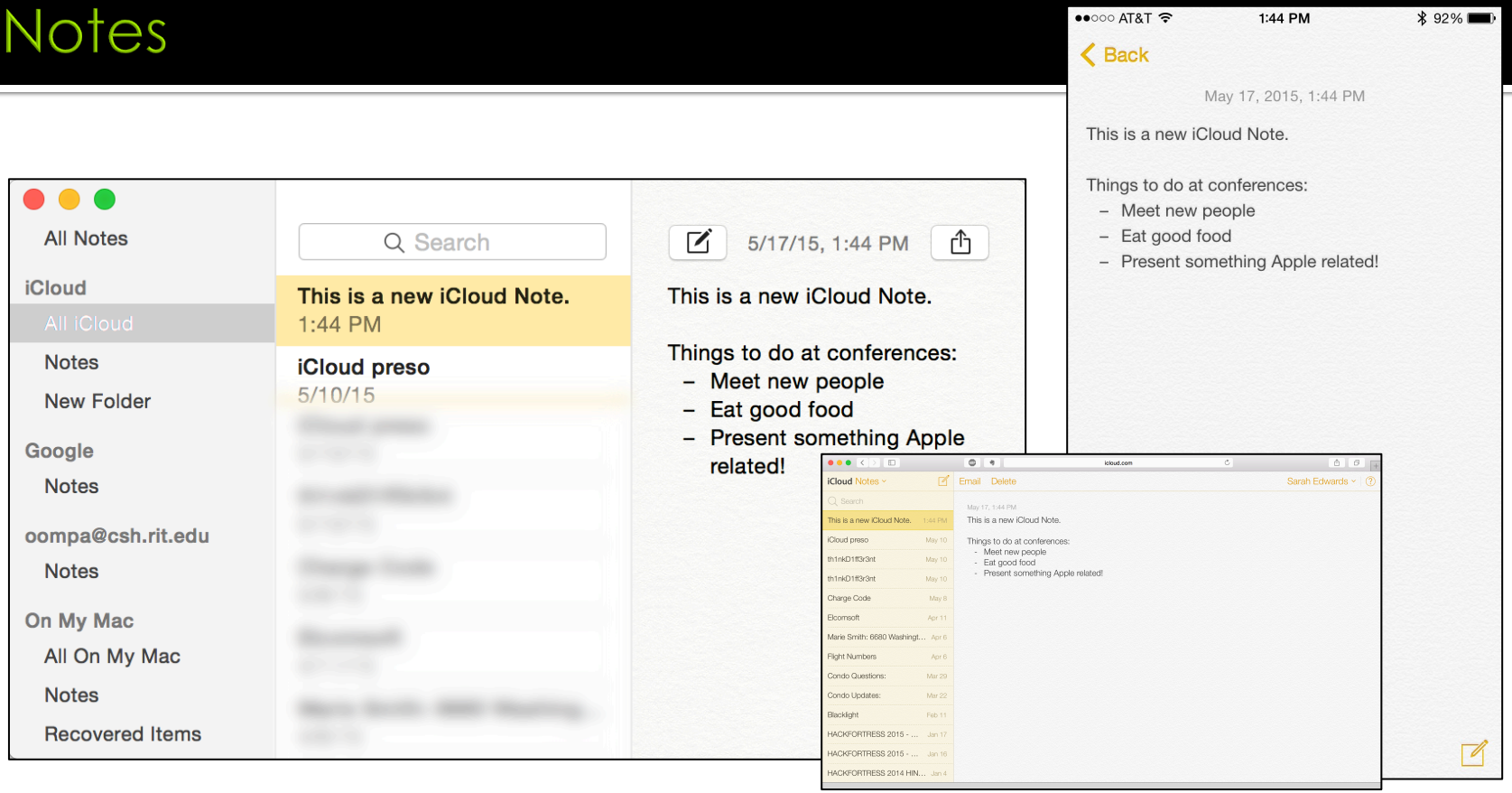
```
miPhone5s:/private/var/mobile/Library/Passes/Cards root# pwd
/private/var/mobile/Library/Passes/Cards
miPhone5s:/private/var/mobile/Library/Passes/Cards root# ls -l
total 0
drwxr-xr-x 2 mobile mobile 204 Jul 16  2014 0-cM9ac3eFNA9iCZ0mbkGqaN1OE=.cache
drwxr-xr-x 2 mobile mobile 306 Jul 16  2014 0-cM9ac3eFNA9iCZ0mbkGqaN1OE=.pkpass
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 0cxFFcwnrkgt7WihgBXO7v4qr7I=.cache
drwxr-xr-x 2 mobile mobile 408 Aug 10  2014 0cxFFcwnrkgt7WihgBXO7v4qr7I=.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



Applications
Notes



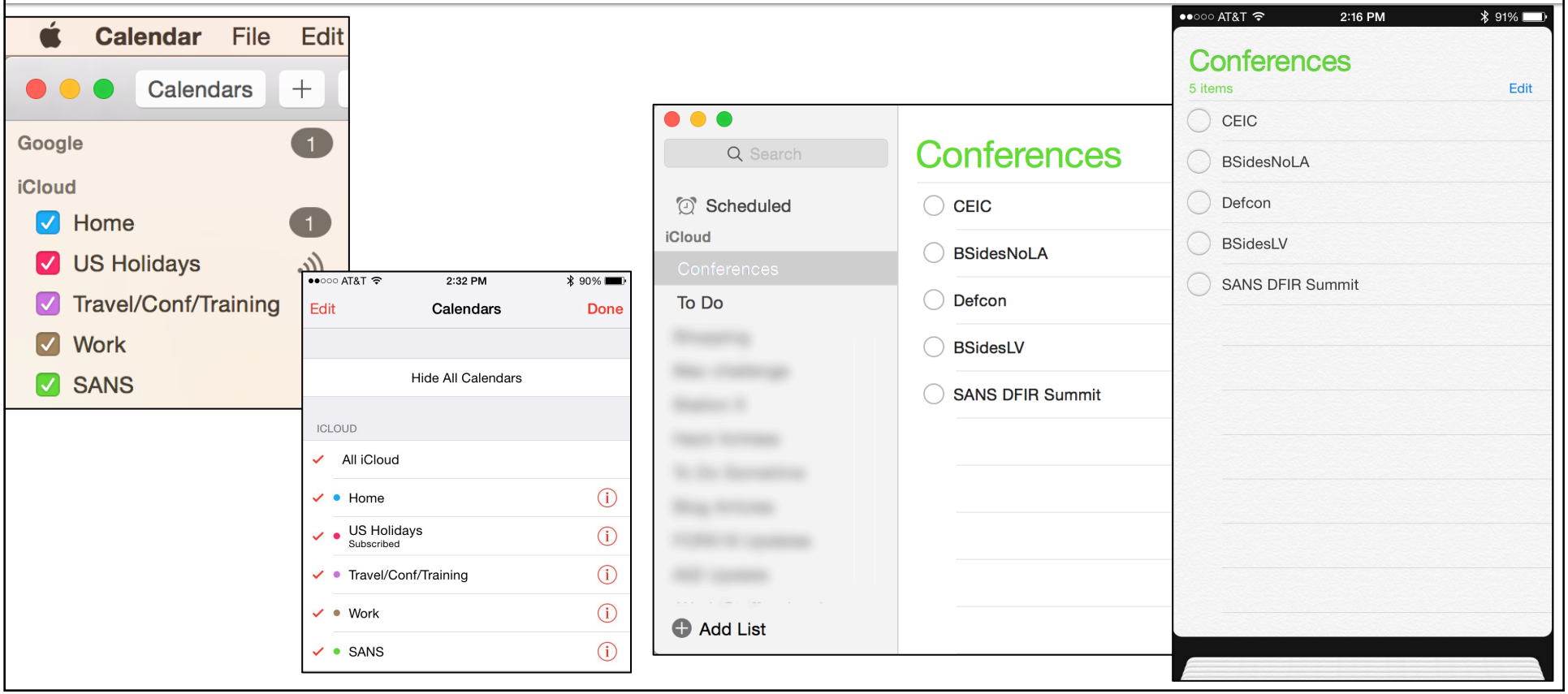
Applications
Notes

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

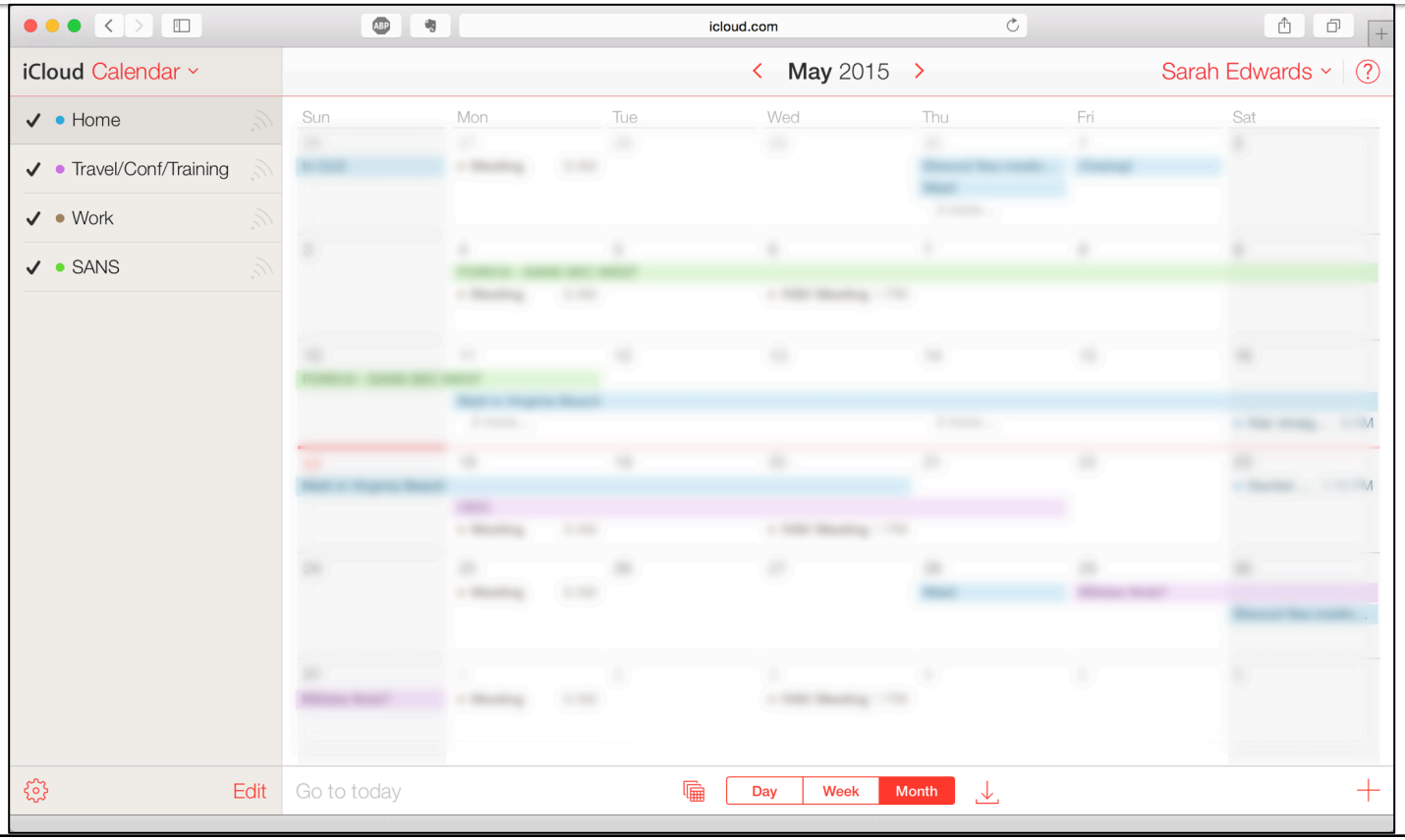
```
1 select ZNOTE.Z_PK,ZDATECREATED,ZDATEEDITED,ZTITLE,ZHTMLSTRING from ZNOTE INNER JOIN ZNOTEBODY
  ON ZNOTE.Z_PK = ZNOTEBODY.Z_PK WHERE ZNOTE.Z_PK=86;
2
```

	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. Things to do at conferences: <ul clas…

Applications
Calendar & Reminders



Applications
Calendar & Reminders



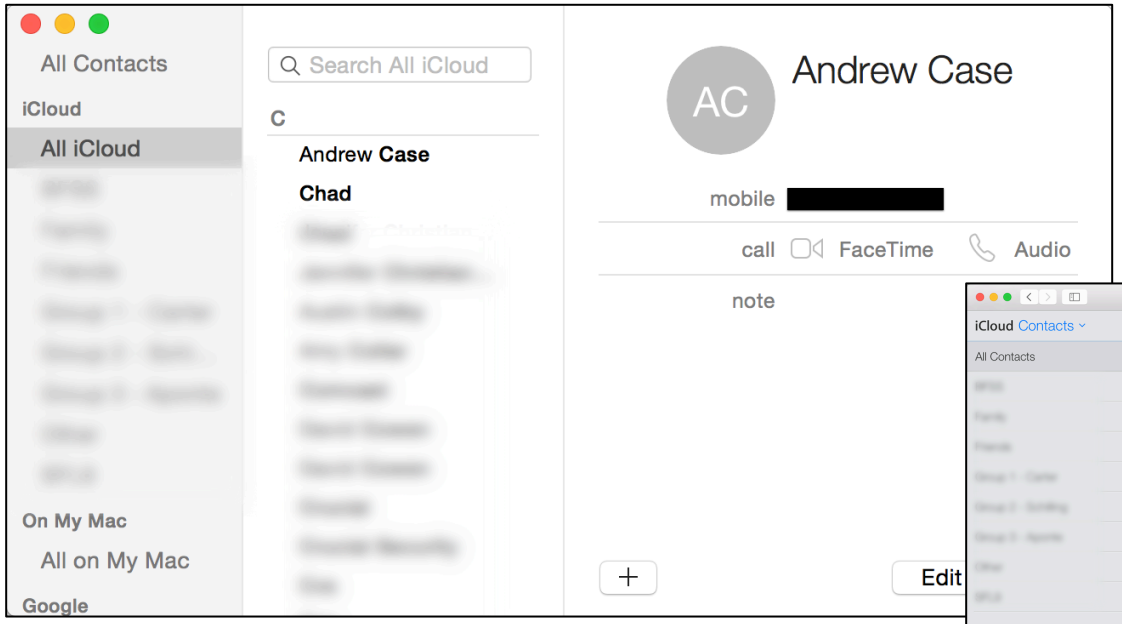
Applications
Calendar & Reminders

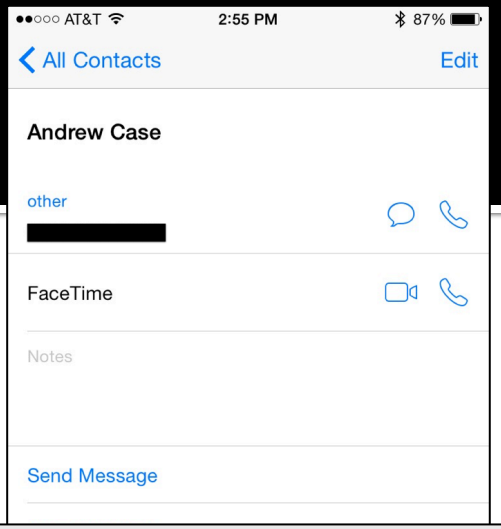
- **OS X**: ~/Library/Calendars/Calendar Cache
- **iOS**: /private/var/mobile/Library/Calendar/Calendar.sqlitedb
- SQLite Table: ZCALENDARITEM
  - Calendar item creation time and title.

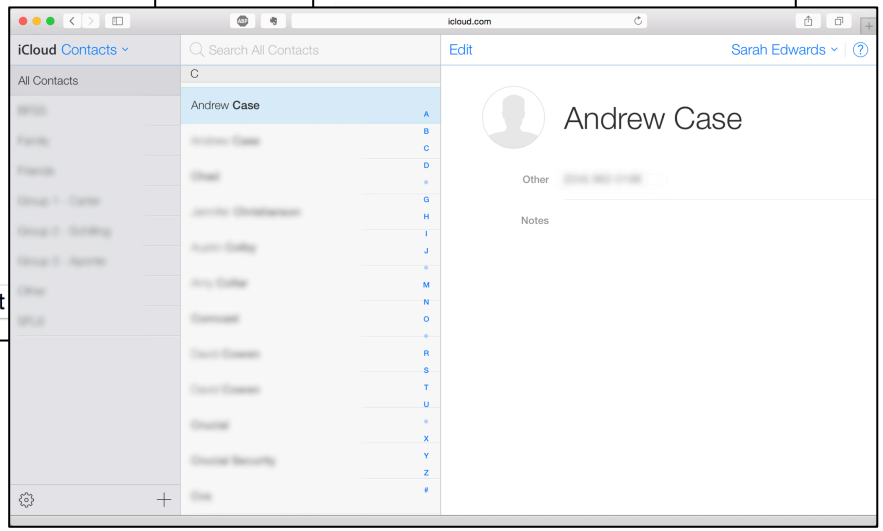
```
1 select Z_PK,ZCREATIONDATE,ZTITLE from ZCALENDARITEM where Z_PK >= 2178 and Z_PK <= 2182;
```

	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







Applications Contacts

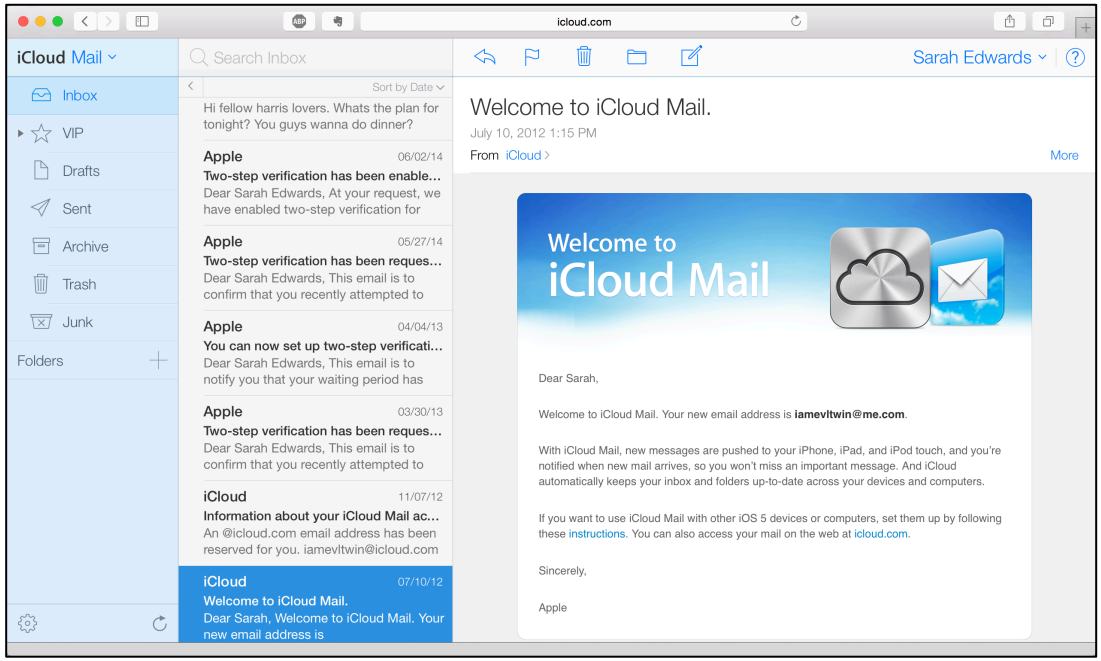
- **OS X**: ~/Library/Application Support/AddressBook/Sources/<GUID>/AddressBook-v22.abcddb
- **iOS**: /private/var/mobile/Library/AddressBook/AddressBook.sqlitdb
- SQLite Tables: ZABCDRECORD & ZABCDPHONENUMBER
  - Contact Name & Number
  - Contact Creation and Modification Dates

```
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	[redacted]

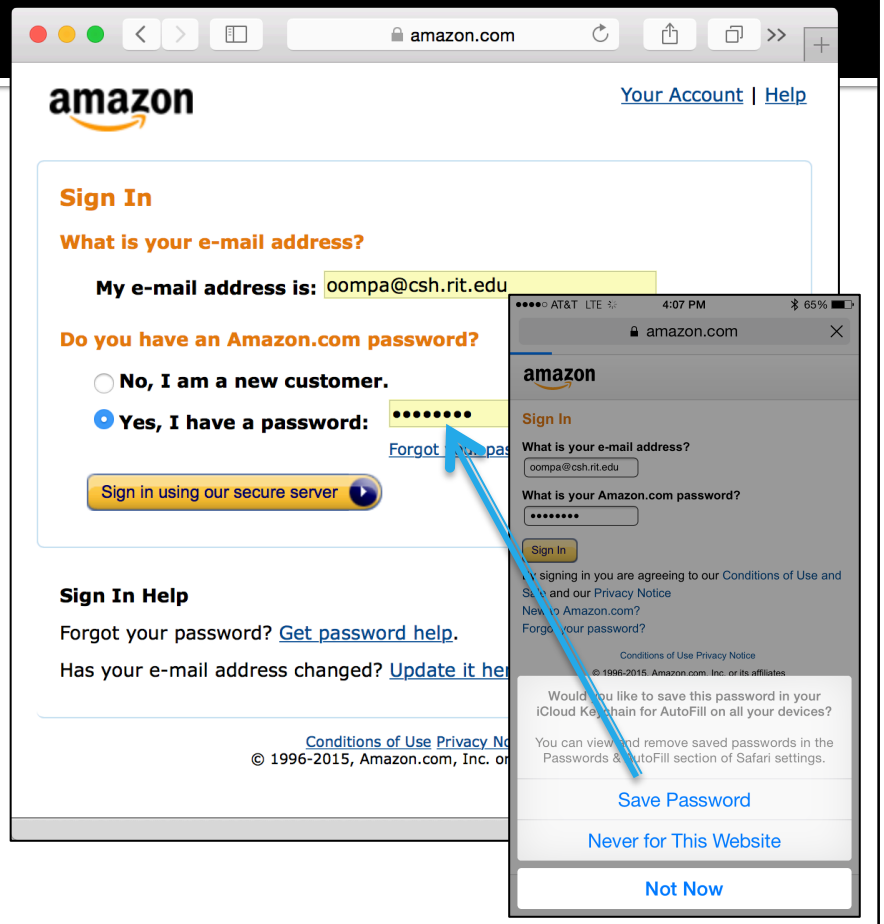
Applications
Email

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



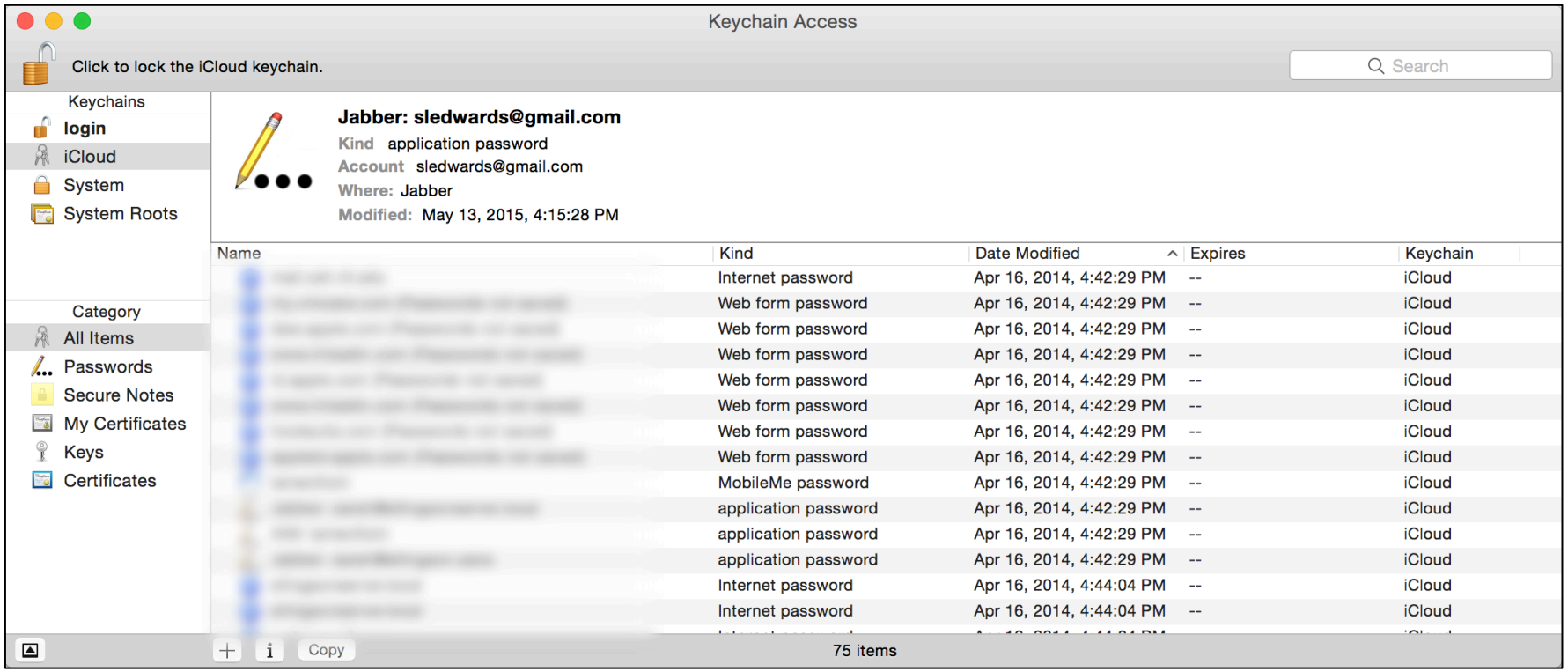
Applications
iCloud Keychain

- 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                    com~apple~ScriptEditor2
A4QBZ46HAP~com~gameloft~UNOFree                com~apple~TextEdit
F3LWYJ7GM7~com~apple~mobilegarageband          com~apple~TextInput
F6266T9T75~com~apple~iMovie                    com~apple~mail
X6UDPZTLVR~Q5CS529KB3~com~velyoo~iDashboard    com~apple~shoebox
com~apple~Automator                            com~apple~system~spotlight
com~apple~CloudDocs                            iCloud~com~getdropbox~Dropbox
com~apple~Keynote                              iCloud~com~google~container
com~apple~Notes                                iCloud~com~microsoft~Office~PowerPoint
com~apple~Numbers                              iCloud~com~microsoft~onenote
com~apple~Pages                                iCloud~com~microsoft~skydrive
com~apple~Preview                              iCloud~com~zenlabs~c25k
com~apple~QuickTimePlayerX
```

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
  - @iamevltwin
  - mac4n6.com

- All icons are owned and are the copyright of Apple, Inc.