Ubiquity Forensics: Your iCloud and You
By Day – Test Engineer at Parsons Corporation (Government Contractor)

By Night – SANS Author & Instructor
• FOR518 – Mac Forensic Analysis (sans.org/course/mac-forensic-analysis)
• Upcoming classes:
  • August/September – Virginia Beach
  • September – Las Vegas
  • October – Singapore
  • October – Prague
  • 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

Sarah Edwards
oompa@csh.rit.edu
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
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 iPhone 4S 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/

**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

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

```python
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

- 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
Synced Preferences
Applications
Synced Preferences

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

```bash
word:SyncedPreferences oompa$ pwd
/Users/oompa/Library/SyncedPreferences
word:SyncedPreferences oompa$ ls -1
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
icbacountsd.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-

<table>
<thead>
<tr>
<th>Key</th>
<th>Type</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Root</td>
<td></td>
<td></td>
</tr>
<tr>
<td>versionid</td>
<td>String</td>
<td>FT=-@RU=d8326b9f-4f49-46cb-8e6f-99bb3e963f9b@S=78594</td>
</tr>
<tr>
<td>initialsnc</td>
<td>Number</td>
<td>2</td>
</tr>
<tr>
<td>changecount</td>
<td>Number</td>
<td>491</td>
</tr>
<tr>
<td>values</td>
<td></td>
<td></td>
</tr>
<tr>
<td>GP_D42A57A67E5DF4FDB4BDC67B9FF2D9C7</td>
<td>Dictionary</td>
<td>(3 items)</td>
</tr>
<tr>
<td>MR_5DA23DA86B5574E5C862872558D6E2C8</td>
<td>Dictionary</td>
<td>(3 items)</td>
</tr>
<tr>
<td>MR_1ABCFC8ACFDD90B8EA7A46833DEFAA2F4</td>
<td>Dictionary</td>
<td>(3 items)</td>
</tr>
<tr>
<td>MR_9CFDBE0E4FC5C5D4731E49AF12C323</td>
<td>Dictionary</td>
<td>(3 items)</td>
</tr>
<tr>
<td>GP_B643BD5EA084BE04C1ADF43A7F30311</td>
<td>Dictionary</td>
<td>(3 items)</td>
</tr>
<tr>
<td>MR_C9DAFF659EDC27A0FA6E8094787A33A7</td>
<td>Dictionary</td>
<td>(3 items)</td>
</tr>
</tbody>
</table>
Applications - Synced Preferences
Email – Recent Emails

- **MR – Single Contact**
- **GP – Group Email**

<table>
<thead>
<tr>
<th>Field</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>value</td>
<td>Dictionary (3 items)</td>
</tr>
<tr>
<td>k</td>
<td>String gr</td>
</tr>
<tr>
<td>t</td>
<td>Array (3 items)</td>
</tr>
<tr>
<td>Item 0</td>
<td>Date Mar 12, 2015, 9:47:43 PM</td>
</tr>
<tr>
<td>Item 1</td>
<td>Date Jul 28, 2014, 5:44:23 PM</td>
</tr>
<tr>
<td>Item 2</td>
<td>Date Jul 27, 2014, 10:26:47 AM</td>
</tr>
<tr>
<td>gK</td>
<td>Number 0</td>
</tr>
<tr>
<td>S</td>
<td>String com.apple.mail</td>
</tr>
<tr>
<td>v</td>
<td>Number 1</td>
</tr>
<tr>
<td>n</td>
<td>String Rob Lee</td>
</tr>
<tr>
<td>s</td>
<td>String <a href="mailto:ooompa@csh.rit.edu">ooompa@csh.rit.edu</a></td>
</tr>
<tr>
<td>a</td>
<td>String <a href="mailto:hmahalik@gmail.com">hmahalik@gmail.com</a></td>
</tr>
<tr>
<td>mrs</td>
<td>Array (2 items)</td>
</tr>
<tr>
<td>Item 0</td>
<td>Dictionary (3 items)</td>
</tr>
<tr>
<td>n</td>
<td>String Henri van Goethem</td>
</tr>
<tr>
<td>a</td>
<td>String <a href="mailto:hvangoethem@sans.org">hvangoethem@sans.org</a></td>
</tr>
<tr>
<td>k</td>
<td>String email</td>
</tr>
<tr>
<td>Item 1</td>
<td>Dictionary (3 items)</td>
</tr>
<tr>
<td>n</td>
<td>String Rob Lee</td>
</tr>
<tr>
<td>a</td>
<td>String <a href="mailto:ilee@sans.org">ilee@sans.org</a></td>
</tr>
<tr>
<td>k</td>
<td>String email</td>
</tr>
<tr>
<td>remotevalue</td>
<td>Data &lt;01196a02 379b21a 000000</td>
</tr>
<tr>
<td>timestamp</td>
<td>Number 447,904,063</td>
</tr>
<tr>
<td>MR_9CFDBEF0E4FC5C54D4731E49AF12C323</td>
<td>Dictionary (3 items)</td>
</tr>
<tr>
<td>value</td>
<td>Dictionary (6 items)</td>
</tr>
<tr>
<td>S</td>
<td>String com.apple.mail</td>
</tr>
<tr>
<td>v</td>
<td>Number 1</td>
</tr>
<tr>
<td>n</td>
<td>String Heather Mahalik</td>
</tr>
<tr>
<td>s</td>
<td>String <a href="mailto:ooompa@csh.rit.edu">ooompa@csh.rit.edu</a></td>
</tr>
<tr>
<td>a</td>
<td>String <a href="mailto:hmahalik@gmail.com">hmahalik@gmail.com</a></td>
</tr>
<tr>
<td>t</td>
<td>Array (5 items)</td>
</tr>
<tr>
<td>Item 0</td>
<td>Date May 12, 2015, 9:30:38 PM</td>
</tr>
<tr>
<td>Item 1</td>
<td>Date May 10, 2015, 2:40:35 PM</td>
</tr>
<tr>
<td>Item 2</td>
<td>Date May 10, 2015, 2:23:48 PM</td>
</tr>
<tr>
<td>Item 3</td>
<td>Date May 10, 2015, 12:21:41 PM</td>
</tr>
<tr>
<td>Item 4</td>
<td>Date May 6, 2015, 7:52:22 PM</td>
</tr>
<tr>
<td>remotevalue</td>
<td>Data &lt;0179770f bee0021b 000000</td>
</tr>
<tr>
<td>timestamp</td>
<td>Number 453,173,438</td>
</tr>
</tbody>
</table>
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

<table>
<thead>
<tr>
<th>Key</th>
<th>Type</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>▼ Root</td>
<td></td>
<td></td>
</tr>
<tr>
<td>▼ versionid</td>
<td>String</td>
<td>FT=+BRE=8RU=d8326b9f-4f49-46cb-8e6f-99bb3e963f9b@S=78647</td>
</tr>
<tr>
<td>▼ initials</td>
<td>Number</td>
<td>4</td>
</tr>
<tr>
<td>▼ changecount</td>
<td>Number</td>
<td>7</td>
</tr>
<tr>
<td>▼ values</td>
<td></td>
<td></td>
</tr>
<tr>
<td>▼ VIP_C23ECE34-264F-4134-9F23-4EA4B80FD2AE ▼ value</td>
<td>Dictionary</td>
<td>(3 items)</td>
</tr>
<tr>
<td>▼ n</td>
<td>String</td>
<td>Rob Lee</td>
</tr>
<tr>
<td>▼ a</td>
<td>Array (1 item)</td>
<td></td>
</tr>
<tr>
<td>▼ item 0</td>
<td>String</td>
<td><a href="mailto:riee@sans.org">riee@sans.org</a></td>
</tr>
<tr>
<td>▼ value</td>
<td>Dictionary</td>
<td>(3 items)</td>
</tr>
<tr>
<td>▼ remotevalue</td>
<td>Data</td>
<td>&lt;01090809 fc0f081b 00000000 62706c69 73743030 d3010203</td>
</tr>
<tr>
<td>▼ timestamp</td>
<td>Number</td>
<td>453,513,212</td>
</tr>
</tbody>
</table>
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-

<table>
<thead>
<tr>
<th>▼ Root</th>
<th>Dictionary</th>
<th>(4 items)</th>
</tr>
</thead>
<tbody>
<tr>
<td>versionid</td>
<td>String</td>
<td>FT=-@RU=d83</td>
</tr>
<tr>
<td>initialscount</td>
<td>Number</td>
<td>2</td>
</tr>
<tr>
<td>changecount</td>
<td>Number</td>
<td>1,227</td>
</tr>
<tr>
<td>▼ values</td>
<td>Dictionary</td>
<td>(198 items)</td>
</tr>
<tr>
<td>GP_BB031C1D39B13CB975BD2B5D1B704D65</td>
<td>Dictionary</td>
<td>(3 items)</td>
</tr>
<tr>
<td>MR_C93D9B19B6118D5D9BF1622CABBE5FE1</td>
<td>Dictionary</td>
<td>(3 items)</td>
</tr>
<tr>
<td>MR_434D0C13A43BD98872E495089BFE5CF5</td>
<td>Dictionary</td>
<td>(3 items)</td>
</tr>
<tr>
<td>MR_74589F9321BA59AE3DB18194339BD134</td>
<td>Dictionary</td>
<td>(3 items)</td>
</tr>
</tbody>
</table>
Applications - Synced Preferences

Messages – “Recent” Messages

- MR = Single Recipient, GR = Group
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

<table>
<thead>
<tr>
<th>Key</th>
<th>Type</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>▼ Root</td>
<td>Dictionary</td>
<td>(4 items)</td>
</tr>
<tr>
<td>versionid</td>
<td>String</td>
<td>FT=-@RU=d8326b9f-4f49-46b7-b687-c4a0f2f454b0</td>
</tr>
<tr>
<td>initialsSync</td>
<td>Number</td>
<td>1</td>
</tr>
<tr>
<td>changeCount</td>
<td>Number</td>
<td>3,248</td>
</tr>
<tr>
<td>▼ values</td>
<td>Dictionary</td>
<td>(3 items)</td>
</tr>
<tr>
<td>▼ CE3B9EB5-CB56-413F-9077-18CB891FFCA2</td>
<td>Dictionary</td>
<td>(3 items)</td>
</tr>
<tr>
<td>▼ value</td>
<td>Dictionary</td>
<td>(3 items)</td>
</tr>
<tr>
<td>LastModified</td>
<td>Date</td>
<td>May 17, 2015, 10:17:40 AM</td>
</tr>
<tr>
<td>DeviceName</td>
<td>String</td>
<td>Mini miPad</td>
</tr>
<tr>
<td>▼ Tabs</td>
<td>Array</td>
<td>(3 items)</td>
</tr>
<tr>
<td>remoteValue</td>
<td>Data</td>
<td>&lt;01b98b00 84da081b 00000000</td>
</tr>
<tr>
<td>timestamp</td>
<td>Number</td>
<td>453,565,060</td>
</tr>
<tr>
<td>▼ 199EC7F7-49FA-405E-8426-F26FF0EF811F</td>
<td>Dictionary</td>
<td>(3 items)</td>
</tr>
<tr>
<td>▼ 3ED4EF04-31B2-44DC-B303-92F29...</td>
<td>Dictionary</td>
<td>(3 items)</td>
</tr>
</tbody>
</table>
### Applications - Synced Preferences

#### Safari – Synced Tabs

<table>
<thead>
<tr>
<th>Title</th>
<th>URL</th>
</tr>
</thead>
<tbody>
<tr>
<td>Synalyze It! developer weblog</td>
<td><a href="https://www.synalysis.net/developer-weblog/">https://www.synalysis.net/developer-weblog/</a></td>
</tr>
<tr>
<td>DFIR Summit (Austin, TX)</td>
<td><a href="https://www.sans.org/event/digital-forensics-summit-2015">https://www.sans.org/event/digital-forensics-summit-2015</a></td>
</tr>
<tr>
<td>LOLCats - Funny cat pictures</td>
<td><a href="http://www.lolcats.com/">http://www.lolcats.com/</a></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Title</th>
<th>UUID</th>
</tr>
</thead>
<tbody>
<tr>
<td>Synalyze It! developer weblog</td>
<td>199EC7F7-49FA-405E-8426-F26FF0EF811F</td>
</tr>
<tr>
<td>DFIR Summit (Austin, TX)</td>
<td>81D25DBE-9817-43D9-AB68-A47490EA5D64</td>
</tr>
<tr>
<td>LOLCats - Funny cat pictures</td>
<td>F7F167CB-BC5B-4CF2-8B10-9A5F82F1F31E</td>
</tr>
</tbody>
</table>

| LastModified     | May 17, 2015, 10:15:50 AM |
| DeviceName       | iPhone6                    |
| DictionaryType   | Device                     |
| remotevalue      | 01f81b00 16da081b 000000000 62706c69 73743030 d50103 |
| timestamp        | 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.wifi.plist
### Applications - Synced Preferences

**WiFi – Synced Access Points**

<table>
<thead>
<tr>
<th>Key</th>
<th>Type</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>▼ Root</td>
<td>Dictionary</td>
<td>(4 items)</td>
</tr>
<tr>
<td>versionid</td>
<td>String</td>
<td>FT=-@RU=0</td>
</tr>
<tr>
<td>initials</td>
<td>Number</td>
<td>5</td>
</tr>
<tr>
<td>changecount</td>
<td>Number</td>
<td>30</td>
</tr>
<tr>
<td>▼ values</td>
<td>Dictionary</td>
<td>(37 items)</td>
</tr>
<tr>
<td>▲ FOR518</td>
<td>Dictionary</td>
<td>(3 items)</td>
</tr>
<tr>
<td>Reagan National WiFi</td>
<td>Dictionary</td>
<td>(3 items)</td>
</tr>
<tr>
<td>Parsons_Visitor</td>
<td>Dictionary</td>
<td>(3 items)</td>
</tr>
<tr>
<td>ASUS</td>
<td>Dictionary</td>
<td>(3 items)</td>
</tr>
<tr>
<td>SJ</td>
<td>Dictionary</td>
<td>(3 items)</td>
</tr>
<tr>
<td>RitzCarlton_Guest</td>
<td>Dictionary</td>
<td>(3 items)</td>
</tr>
<tr>
<td>Marriott_GUEST</td>
<td>Dictionary</td>
<td>(3 items)</td>
</tr>
<tr>
<td>Hyatt Lobby</td>
<td>Dictionary</td>
<td>(3 items)</td>
</tr>
<tr>
<td>scandic_easy</td>
<td>Dictionary</td>
<td>(3 items)</td>
</tr>
</tbody>
</table>

#### Reagan National WiFi

```
<table>
<thead>
<tr>
<th>Key</th>
<th>Type</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>value</td>
<td>Dictionary</td>
<td>(11 items)</td>
</tr>
<tr>
<td>WEP</td>
<td>Boolean</td>
<td>NO</td>
</tr>
<tr>
<td>enabled</td>
<td>Boolean</td>
<td>YES</td>
</tr>
<tr>
<td>UserDirected</td>
<td>Boolean</td>
<td>NO</td>
</tr>
<tr>
<td>added_by</td>
<td>String</td>
<td>miPhone5s</td>
</tr>
<tr>
<td>SSID_STR</td>
<td>String</td>
<td>Reagan National WiFi</td>
</tr>
<tr>
<td>IS_NETWORK_CUSTOMIZED</td>
<td>Boolean</td>
<td>NO</td>
</tr>
<tr>
<td>BSSID</td>
<td>String</td>
<td>0:1c:f6:60:45:30</td>
</tr>
<tr>
<td>added_at</td>
<td>String</td>
<td>Feb 9 2014 20:25:23</td>
</tr>
<tr>
<td>IS_NETWORK_CONFIGURED</td>
<td>Boolean</td>
<td>NO</td>
</tr>
<tr>
<td>IS_NETWORK_EAP</td>
<td>Boolean</td>
<td>NO</td>
</tr>
<tr>
<td>AP_MODE</td>
<td>Number</td>
<td>2</td>
</tr>
<tr>
<td>remotevalue</td>
<td>Data</td>
<td>&lt;01b94900 576fd91a 00</td>
</tr>
<tr>
<td>timestamp</td>
<td>Number</td>
<td>450,457,431</td>
</tr>
</tbody>
</table>
```
Applications - Synced Preferences
Maps – Synced Bookmarks (Favorites)

- **OS X:**

- **iOS:**
  - /private/var/mobile/Library/SyncedPreferences/com.apple.Maps.plist
### Applications - Synced Preferences

#### Maps – Bookmarks (Favorites)

<table>
<thead>
<tr>
<th>_sync.bookmarks.item.23D45D96-4D5F-4270-9CE4-38E751F2200A</th>
<th>Dictionary (3 items)</th>
</tr>
</thead>
<tbody>
<tr>
<td>_value</td>
<td>data</td>
</tr>
<tr>
<td>position</td>
<td>Dictionary (2 items)</td>
</tr>
<tr>
<td>remotevalue</td>
<td>Data</td>
</tr>
<tr>
<td>timestamp</td>
<td>Number</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>_sync.bool</th>
<th>Go To Offset (Text search)</th>
</tr>
</thead>
<tbody>
<tr>
<td>_sync.bool</td>
<td>Untitled</td>
</tr>
<tr>
<td>_sync.bool</td>
<td>Save Copy Cut Paste Undo Redo</td>
</tr>
</tbody>
</table>

| 000 | 08 | 01 | 12 | 24 | 32 | 33 | 44 | 34 |
| 025 | 45 | 34 | 2D | 33 | 38 | 35 | 37 | 35 |
| 050 | 4A | 02 | 00 | 19 | 02 | 12 | 96 | 02 |
| 075 | 6D | D6 | 48 | 30 | 31 | 00 | 00 | 00 |
| 100 | E0 | 03 | 3F | 30 | 29 | 40 | 32 | AB |
| 125 | C3 | B8 | 02 | 65 | 6E | 68 | 61 | 76 |
| 150 | 44 | 65 | 6E | 60 | 61 | 72 | 68 | 12 |
| 175 | 6E | 6F | 02 | 0A | 43 | 6F | 70 | 65 |
| 200 | 74 | 72 | 75 | 6D | 72 | 09 | 53 | 6A |
| 225 | 4E | 79 | 6E | 61 | 76 | 6E | 0A | 01 |
| 250 | 6F | 07 | 0E | 6E | 68 | 61 | 67 | 65 |
| 275 | 6E | 74 | 72 | 75 | 6D | 04 | 12 | 09 |
| 300 | 6B | 00 | 70 | D9 | 32 | 7A | 06 | 0E |
| 325 | 2D | 55 | 53 | D2 | 0C | 05 | 65 | 6E |
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:

Recent Locations & Searches
  - OS X:
  - iOS:
# Applications - Synced Preferences

Maps – Recent Addresses

- Extracted from Mail emails – “From…”

<table>
<thead>
<tr>
<th>MR_F8EA2DAFA7D6877F5B232D00534B0797558A5D6C</th>
<th>Dictionary</th>
<th>(3 items)</th>
</tr>
</thead>
<tbody>
<tr>
<td>value</td>
<td>Dictionary</td>
<td>(7 items)</td>
</tr>
<tr>
<td>k</td>
<td>String</td>
<td>m</td>
</tr>
<tr>
<td>t</td>
<td>Array</td>
<td>(4 items)</td>
</tr>
<tr>
<td>Item 0</td>
<td>Date</td>
<td>Apr 26, 2015, 9:58:31 AM</td>
</tr>
<tr>
<td>Item 1</td>
<td>Date</td>
<td>Apr 26, 2015, 7:25:33 AM</td>
</tr>
<tr>
<td>Item 2</td>
<td>Date</td>
<td>Apr 15, 2015, 8:26:02 PM</td>
</tr>
<tr>
<td>Item 3</td>
<td>Date</td>
<td>Apr 15, 2015, 7:35:59 PM</td>
</tr>
<tr>
<td>m</td>
<td>Dictionary</td>
<td>(4 items)</td>
</tr>
<tr>
<td>corerecents:from</td>
<td>Dictionary</td>
<td>(3 items)</td>
</tr>
<tr>
<td>kind</td>
<td>String</td>
<td>email</td>
</tr>
<tr>
<td>address</td>
<td>String</td>
<td><a href="mailto:listings@redfin.com">listings@redfin.com</a></td>
</tr>
<tr>
<td>displayName</td>
<td>String</td>
<td>Redfin</td>
</tr>
<tr>
<td>corerecents:event-time</td>
<td>Date</td>
<td>Apr 26, 2015, 7:23:45 AM</td>
</tr>
<tr>
<td>corerecents:reference-url</td>
<td>String</td>
<td>message:%3Cdata-listingAlerts-20150424_1041_740ed27991d0e463fd3fc61f3dbb786c93a342ed%3E</td>
</tr>
<tr>
<td>corerecents:subject</td>
<td>String</td>
<td>Status change on 5035 25TH St SOUTH; New Hot Home on 3103 19TH St</td>
</tr>
<tr>
<td>S</td>
<td>String</td>
<td>com.apple.mobilemail</td>
</tr>
<tr>
<td>v</td>
<td>Number</td>
<td>1</td>
</tr>
<tr>
<td>a</td>
<td>String</td>
<td>5035 25TH St SOUTH</td>
</tr>
<tr>
<td>w</td>
<td>Number</td>
<td>5</td>
</tr>
<tr>
<td>remotevalue</td>
<td>Data</td>
<td>-&gt;</td>
</tr>
<tr>
<td>timestamp</td>
<td>Number</td>
<td>451,749,511</td>
</tr>
</tbody>
</table>
Application Data
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/

- Favorites
  - Dropbox
  - iCloud Drive
  - AirDrop
  - Applications
  - Desktop
  - Documents
  - Downloads

- CEIC-2015_PPT_UbiquityForensics.pptx
Applications – Documents
iWork & TextEdit – Mobile Documents

- `com~apple~Numbers` (and Keynote, Pages, & TextEdit)
  - "Documents" Directory
  - iWorkPreviews Directory (iWork Only)
- `com~apple~CloudDocs`
  - No "Documents" Directory
Applications – Documents
iWork & TextEdit – Mobile Documents on iOS 7 & Older

- iOS: /private/var/mobile/Library/Mobile Documents/
• Follows same structure
• Kinda Funky – Need to research
  • Waiting on 8.2/8.3 Jailbreak 😊
• 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)
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.)
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/

![Folder structure for photo streams](image-url)
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/
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
Applications
Photos – New Photos Application

- **OS X – Photos App Metadata**
  - ~/Pictures/Photos Library.photoslibrary/Databases/Library.apdb
  - Link to /apdb/Library.apdb
  - SQLite Database
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/*
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/)root# pwd
/private/var/mobile/Media/PhotoData/PhotoCloudSharingData/...
miPhone5s:/private/var/mobile/Media/PhotoData/PhotoCloudSharingData/)root# ls -l
total 0
drwxr-xr-x 2 mobile mobile 102 Apr 11 08:03 13836496-E555-4241-8FB8-F99700ADA7A9
drwxr-xr-x 2 mobile mobile 102 Apr 11 08:03 C7482CD5-D258-4E12-8280-587F7B4EF734
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-A9034CA2F91
miPhone5s:/private/var/mobile/Media/PhotoData/PhotoCloudSharingData/)root# plutil -show 13836496-E555-4241-8FB8-F99700ADA7A9/Info.plist
{
    cloudOwnerEmail = "oompa@csh.rit.edu";
    cloudOwnerFirstName = Sarah;
    cloudOwnerHashedPersonID = fbc09
    cloudOwnerLastName = Edwards;
    cloudPublicURLEnabled = 1;
    cloudRelationshipState = 0;
    publicURL = "https://www.icloud.com/photos/stream/#A25"
    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\n  - IMG_#####.JPG or PNG
Applications
Photos – On Windows – Shared Albums

- C:\Users\<user>\Pictures\iCloud Photos\Shared\n- 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-cM9ac3eFNA9iCZ0mbkGqaN10E=.pkpass
drwxr-xr-x 9 oompa staff 306 Jul 26 2014 07DvKQIpN4QMgtfti5miHNJW6mQ=.pkpass
drwxr-xr-x 12 oompa staff 408 Aug 10 2014 0cxFFcwnrkg7WiwhgBX07v4qr7i=.pkpass
```

```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
Applications
Passbook Passes – Pass Info - pass.json Files

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

```json
{
  "boardingPass": {
    "transitType": "PKTransitTypeAir",
    "auxiliaryFields": [
      {
        "label": "BOARDS",
        "key": "boardingTime",
        "value": "4:85 PM"
      },
      {
        "label": "FLIGHT",
        "key": "flight",
        "value": "UA 644"
      },
      {
        "label": "SEAT",
        "key": "seat",
        "value": "28A"
      },
      {
        "label": "SEQ",
        "key": "seq",
        "value": "36"
      },
      {
        "label": "GROUP",
        "key": "group",
        "value": "2"
      }
    ],
    "primaryFields": [
      {
        "label": "WASHINGTON-DULLES",
        "key": "origin",
        "value": "IAD"
      },
      {
        "label": "SAN FRANCISCO",
        "key": "destination",
        "value": "SFO"
      }
    ],
    "headerFields": [
      {
        "label": "GATE",
        "key": "gate",
        "value": "D10"
      }
    ],
    "changeMessage": "Your gate has changed to @@
  }
}
```
Applications
Notes

This is a new iCloud Note.

Things to do at conferences:
- Meet new people
- Eat good food
- Present something Apple related!
Applications
Notes

- **OS X**: 
  ~/Library/Containers/com.apple.Notes/Data/Library/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;
```

<table>
<thead>
<tr>
<th>Z_PK</th>
<th>ZDATECREATED</th>
<th>ZDATEEDITED</th>
<th>ZTITLE</th>
<th>ZHTMLSTRING</th>
</tr>
</thead>
<tbody>
<tr>
<td>86</td>
<td>453577382.679417</td>
<td>453577442.702202</td>
<td>This is a new iCloud Note.</td>
<td>&lt;html&gt;&lt;head&gt;&lt;/head&gt;&lt;body&gt;This is a new iCloud Note.&lt;div&gt;&lt;br&gt;&lt;/div&gt;&lt;div&gt;Things to do at conferences:&lt;/div&gt;&lt;div&gt;&lt;ul class...</td>
</tr>
</tbody>
</table>
Applications
Calendar & Reminders

- Google
- iCloud
  - Home
  - US Holidays
  - Travel/Conf/Training
- Work
- SANS
Applications
Calendar & Reminders
Applications
Calendar & Reminders

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

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

<table>
<thead>
<tr>
<th>Z_PK</th>
<th>ZCREATIONDATE</th>
<th>ZTITLE</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>2178</td>
<td>453579293</td>
</tr>
<tr>
<td>2</td>
<td>2179</td>
<td>453579295</td>
</tr>
<tr>
<td>3</td>
<td>2180</td>
<td>453579304</td>
</tr>
<tr>
<td>4</td>
<td>2181</td>
<td>453579309</td>
</tr>
<tr>
<td>5</td>
<td>2182</td>
<td>453579318</td>
</tr>
</tbody>
</table>
Applications
Contacts

Andrew Case

mobile [redacted]

FaceTime

notes

Send Message

Contact List

All Contacts

All iCloud

On My Mac

All on My Mac

Google
Applications
Contacts

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

```sql
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;
```

<table>
<thead>
<tr>
<th>Z_PK</th>
<th>ZCREATIONDATE</th>
<th>ZMODIFICATIONDATE</th>
<th>ZFIRSTNAME</th>
<th>ZLASTNAME</th>
<th>ZFULLNUMBER</th>
</tr>
</thead>
<tbody>
<tr>
<td>12</td>
<td>436038309.237857</td>
<td>436038310.090837</td>
<td>Andrew</td>
<td>Case</td>
<td></td>
</tr>
</tbody>
</table>
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~UNOFree F3LWYJ7GM7~com~apple~mobilegarageband F6266T9T75~com~apple~iMovie X6UDPZTLVR~Q5CS5529KB3~com~velyoo~iDashboard
com~apple~ScriptEditor2
com~apple~TextEdit
com~apple~TextInput
com~apple~mail
com~apple~shoebox
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
```
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
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.