

# Apple iCloud inside out

iCloud backups, FindMyPhone, document storage, iCloud keychain

*DeepSec 2013, Vienna, Austria  
Vladimir Katalov, ElcomSoft Co. Ltd.*

# Global smartphone market

**Top Smartphone Operating Systems, Shipments, and Market Share, 2013 Q3 (Units in Millions)**

| Operating System | 2Q13 Unit Shipments | 2Q13 Market Share | 2Q12 Unit Shipments | 2Q12 Market Share | Year-over-Year Change |
|------------------|---------------------|-------------------|---------------------|-------------------|-----------------------|
| Android          | 187.4               | 79.3%             | 108                 | 69.1%             | 73.5%                 |
| iOS              | 31.2                | 13.2%             | 26                  | 16.6%             | 20.0%                 |
| Windows Phone    | 8.7                 | 3.7%              | 4.9                 | 3.1%              | 77.6%                 |
| BlackBerry OS    | 6.8                 | 2.9%              | 7.7                 | 4.9%              | -11.7%                |
| Linux            | 1.8                 | 0.8%              | 2.8                 | 1.8%              | -35.7%                |
| Symbian          | 0.5                 | 0.2%              | 6.5                 | 4.2%              | -92.3%                |
| Others           | N/A                 | 0.0%              | 0.3                 | 0.2%              | -100.0%               |
| <b>Total</b>     | <b>236.4</b>        | <b>100.0%</b>     | <b>156.2</b>        | <b>100.0%</b>     | <b>51.3%</b>          |

- About 1.2 billion smartphones worldwide
- “Smart devices” – carry a lot of sensitive data
- Corporate deployments are increasing
- ... hard need for forensics!

# Smartphone forensics methods

|                      | Android | iOS    | Windows Phone | BlackBerry OS |
|----------------------|---------|--------|---------------|---------------|
| Logical acquisition  | Yes     | Yes    | Yes           | ?             |
| Physical acquisition | Yes/No  | Yes/No | No            | Yes*          |
| Chip-off             | Yes/No  | No     | ?             | Yes           |
| Local backup         | Yes     | Yes    | No            | Yes           |
| Cloud backup         | Yes     | Yes    | Yes           | No            |
| Documents in cloud   | Yes     | Yes    | Yes           | No            |
| Location service     | Yes     | Yes    | Yes           | No            |

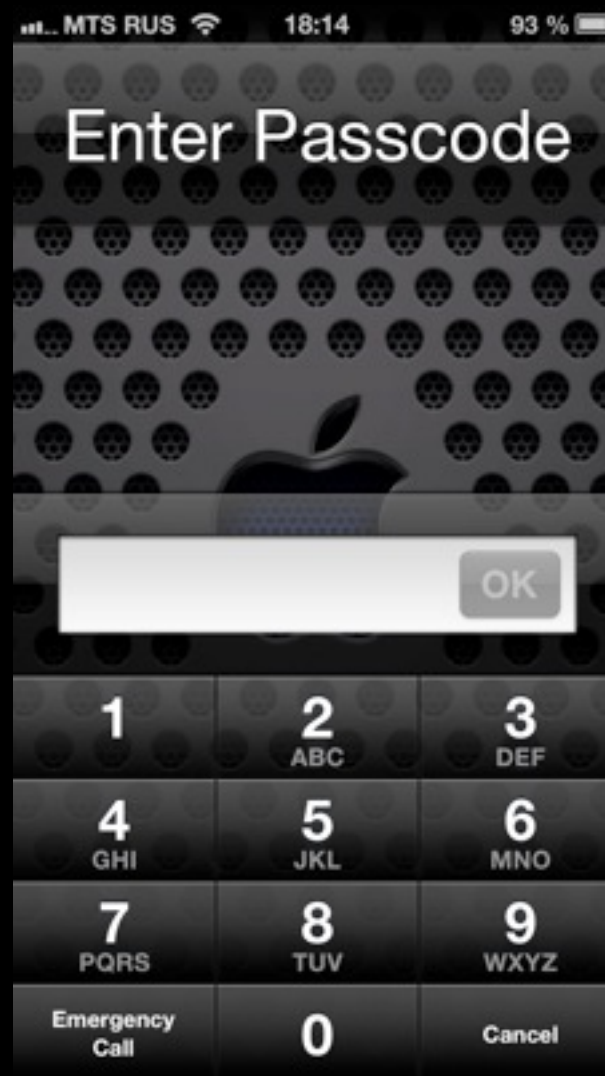
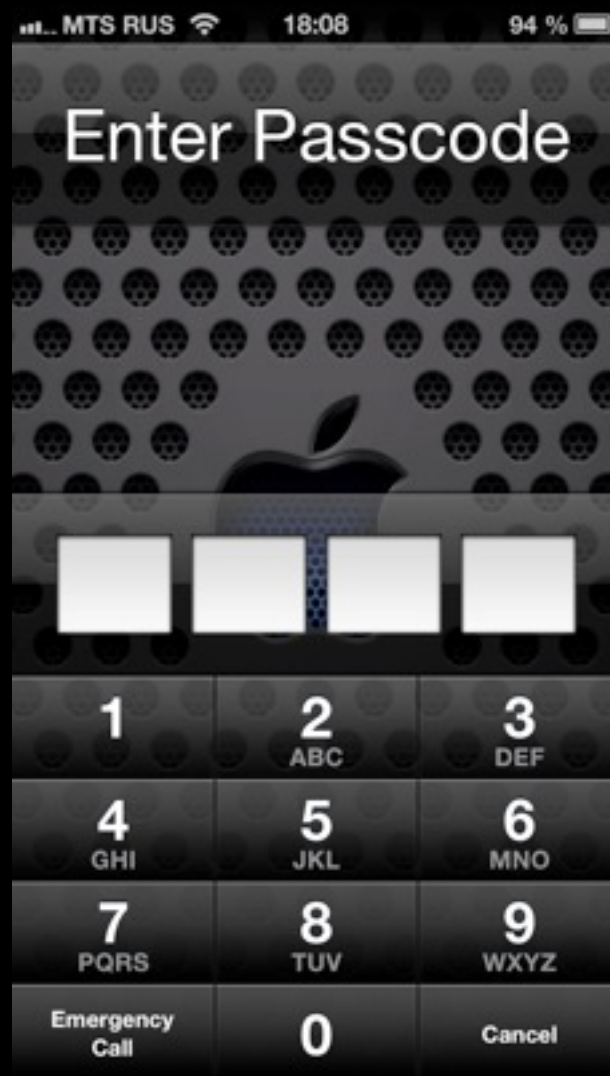
# iOS forensics

- Physical acquisition
  - Boot-time exploit to run unsigned code or jailbreak
  - Device lock state isn't relevant, can bruteforce passcode
  - Can get all information from the device (incl. deleted data)
- Logical acquisition
  - “Ask” device to produce backup
  - Device must be unlocked\*
  - Device may produce encrypted backup
  - Limited amount of information (but more than you think)
- Advanced logical acquisition
  - By direct access to some services running on the iPhone
  - Device must be unlocked\*
  - Limited amount of information (some as in local backup, but plus something extra)
  - Backup password isn't relevant
  - Can be performed over Wi-Fi
- iCloud
  - Need Apple ID and password
  - Can be performed without the device itself
  - Almost the same information as in local backup
  - Can get the documents and location data, too

*\* But there is a workaround ;)*

# iOS passcode

- Device passcode
  - Protect unauthorized access to the device
  - Bypassing is not enough (used in encryption)
- Disk encryption
- Keychain
  - System-wide storage for sensitive data (keys, passwords etc)
  - Data is encrypted



# Backups - what & when

- *Contacts and Contact Favorites*
- *Messages (including iMessages)*
- *Call history*
- *Application data*
- *Device settings*
- *Camera roll (photos and videos)*
- *Purchases (music, movies, TV, apps, books)*
- *Mail accounts*
- *Network settings (saved Wi-Fi hotspots, VPN settings etc)*
- *Paired Bluetooth devices*
- *Safari bookmarks, cookies, history, offline data*
- *... and much more*

## ★ **Local backups**

- iTunes create backups when:
  - Sync with iTunes
  - [File] | [Devices backup]

## ★ **iCloud backups**

- Backup runs daily when device is:
  - Connected to the Internet over Wi-Fi
  - Connected to a power source
  - Locked
- Can force backup
  - [Settings] | [iCloud] | [Storage & Backup] | [Back Up Now]

Backups

Vladimir's iPhone 5 (Tue Oct 22 09:59:11 2013)

System Files

CameraRollDomain

DatabaseDomain

HomeDomain

Library

Accounts

AddressBook

Application Support

BackBoard

BulletinBoard

Caches

Calendar

ConfigurationProfiles

Cookies

DataAccess

Keyboard

Mail

Maps

MobileInstallation

MusicLibrary

Notes

Passes

Preferences

SMS

Safari

SpringBoard

TCC

Voicemail

WebClips

YouTube

com.apple.itunesstored

KeychainDomain

ManagedPreferencesDomain

MediaDomain

iBackupBot

iPhone 5 Global



Vladimir's iPhone 5

iOS 7.0.2 (build 11A501)

Phone Number: +7 (985) 998-68-20

Serial Number: C39JT465F39D

Unique Identifier: b026b06988940617008c9f81dd9e6ab13e07bbcc

IMEI: 013420001267660

What's In Backup

(NOTE: Before making any changes please select Duplicate from the File menu to make a copy of the backup)

Backup Date: Tue Oct 22 09:59:11 2013

Backup Location:  
/Users/vkatalov/Downloads/b026b06988940617008c9f81dd9e6ab13e07bbcc

Total: 8677 Files, 13.4 GB

System Files: [4698 Files, 12.8 GB](#)

User Information:  
[Contacts](#)  
[Messages](#)  
[Call History](#)  
[Calendars](#)  
[Notes](#)  
[Recent Email Address](#)  
[Safari Bookmarks](#)  
[Safari History](#)

Multimedia Files:

[Camera Roll](#)  
[Voice Mails](#)  
[Voice Memos](#)  
[Other Multimedia Files](#)

User App: [134 Apps, 3979 Data Files, 578.5 MB](#)

Devices

Welcome to iBackupBot

Total: 1 Selected: 0 Selected Size: 0



# But wait, there is more...

Google Apps data: Search, Maps, YouTube, Gmail, Drive, Translate, Orkut etc.)

AppDomain-com.google.\*

## **Social networking & communications**

AppDomain-net.whatsapp.WhatsApp\\*

AppDomain-com.burbn.instagram\\*

AppDomain-com.facebook.Facebook\\*

AppDomain-com.facebook.Messenger\\*

AppDomain-com.skype.skype\\*

AppDomain-com.atebits.Tweetie2\\*

AppDomain-com.linkedin.Linkedin\\*

AppDomain-com.naveenium.foursquare\\*

AppDomain-com.viber\\*

## **Other**

HomeDomain\Library\Keyboard\\*

HomeDomain\Library\Passes\\*

HomeDomain\Library\Voicemail\\*

HomeDomain\Library\Maps\\*

RootDomain\Library\Caches\locationd\\*

- Message attachments (even from deleted conversations!)
- Pictures from twitter posts
- Last backup date & time
- Info on Wi-Fi access points you ever connected to (SSID, security, signal etc)
- ... a lot of other interesting stuff :)



## Timeline record info

Type: MMS  
Direction: Outgoing  
Time stamp: Device time: 9/6/2012 7:39:49 PM  
UTC: 9/6/2012 3:39:49 PM  
Remote party: +79688685325  
Description: Watch out! We have guests!

## Details

Data source: Messages  
Folder: MMS - Sent  
Phone Number: +79688685325  
Remote party: +79688685325  
Time stamp: Device time: 9/6/2012 7:39:49 PM  
UTC: 9/6/2012 3:39:49 PM

## Evidence note

## Relevant Contact



Mr Crow John Peter  
Nickname: Good Guy  
Birthday: 5 July 1970  
Company: SPS LTD  
Job title: CEO  
Mobile: +79688685325  
Work: vpetrov1234@gmail.com  
Other: john@yahoo.com  
HomePage: www.bestservices.com  
Home: www.johncrow.com  
Work: www.sps.org  
Note: Do not call him on weekends  
Father: Bob  
Mother: Sara  
Country: United States  
Country: United Kingdom  
Country: Germany

| List                                                    | Date                                      | Remote party                              | Contact                | Geo data |
|---------------------------------------------------------|-------------------------------------------|-------------------------------------------|------------------------|----------|
| Type                                                    | Remote party                              | Description                               | Time stamp (UTC)       |          |
| <input checked="" type="checkbox"/> Email               | Twitter <n-Cngevpxcnlrbzr=tznvy.pb...     | We've missed you on Twitter, Patric...    | 8/1/2012 4:36:31 PM    |          |
| <input checked="" type="checkbox"/> Email               | Twitter <twitter-bulkr-Patrickpaygehom... | We've missed you on Twitter, Patric...    | 11/5/2011 4:29:44 PM   |          |
| <input checked="" type="checkbox"/> SMS                 | +7 968 868-53-25 ( +7 968 868-53-25 )     | We won the tender!!                       | 9/4/2012 1:27:25 PM    |          |
| <input checked="" type="checkbox"/> Email               | patrickpaygehome@gmail.com ( Patric...    | We think that the price is too high. L... | 4/26/2011 7:22:05 AM   |          |
| <input checked="" type="checkbox"/> Kik Message         | John Crow                                 | We have a cat now                         | 9/6/2012 10:12:11 AM   |          |
| <input checked="" type="checkbox"/> Kik Message         | Nina Lahie                                | We are friends and should help each...    | 9/6/2012 10:45:37 AM   |          |
| <input checked="" type="checkbox"/> Note                |                                           | Water flowers -ask Clara                  | 10/12/2012 11:20:00 AM |          |
| <input checked="" type="checkbox"/> MMS                 | +79688685325 ( Mr Crow John Peter )       | Watch out! We have guests!                | 9/6/2012 3:39:49 PM    |          |
| <input checked="" type="checkbox"/> WhatsApp message    | Mr John Peter Crow                        | Watch "Hell Yeah! Covers                  | 12/18/2012 1:35:01 PM  |          |
| <input checked="" type="checkbox"/> Textie messages     | patrickpaygehome@gmail.com                | Wanted to send a photo                    | 12/14/2011 10:31:31 AM |          |
| <input checked="" type="checkbox"/> Email               | patrickpaygehome@gmail.com ( Patric ...   | Wanna see this email.                     | 12/17/2010 8:27:10 AM  |          |
| <input checked="" type="checkbox"/> Kakao Talk messages | Mr John Peter Crow                        | voice note                                | 10/10/2012 2:01:35 PM  |          |
| <input checked="" type="checkbox"/> Kakao Talk messages | Patrick                                   | voice note                                | 11/8/2012 10:02:00 AM  |          |
| <input checked="" type="checkbox"/> Kakao Talk messages | Lena Soloveva                             | voice note                                | 11/8/2012 10:04:45 AM  |          |
| <input checked="" type="checkbox"/> Kakao Talk messages | Patrick                                   | voice note                                | 11/8/2012 10:05:43 AM  |          |
| <input checked="" type="checkbox"/> Opera Mini history  |                                           | Vk.com                                    | 11/21/2012 3:02:59 PM  |          |
| <input checked="" type="checkbox"/> Opera Mini history  |                                           | VK   Share Link                           | 11/21/2012 3:02:47 PM  |          |
| <input checked="" type="checkbox"/> Line messages       | John Crow                                 | visiting my friends                       | 12/29/2012 10:44:26 AM |          |
| <input checked="" type="checkbox"/> Appointment         |                                           | Visit private club with Mary Ades         | 2/23/2013 5:00:00 PM   |          |

## Filters:

## Date filter

☐ After date:

9/ 5/1948

☐ Before date:

9/ 1/2035

## Remote party filter

Clear

- ☐ Bobson Anna
- ☐ Collingwood Andrew
- ☐ Cook John
- ☐ Davidson Ivan
- ☐ Dixon Mary
- ☐ Echo / Sound Test Ser...
- ☐ Espozito Dan
- ☐ Fring Contact
- ☐ Granny
- ☐ Henri Horowitz (jasonp...

## Additional:

☐ Show Calendar occurrences

## Diagram

## Item data

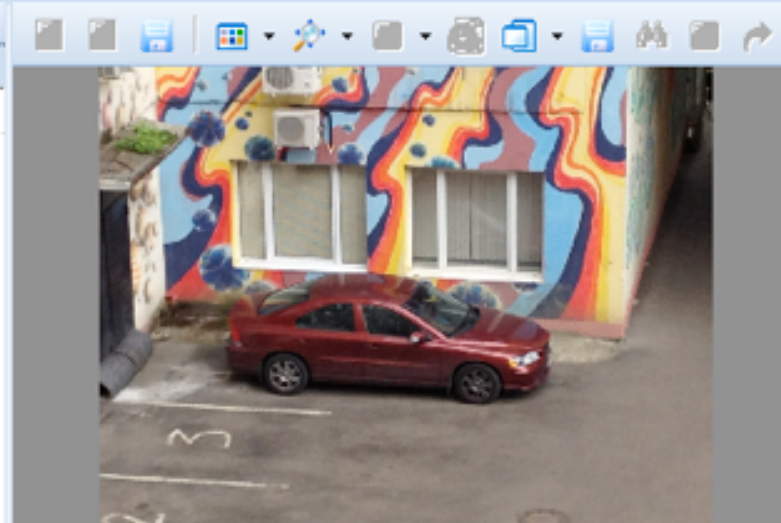
+79688685325 ( Mr Crow John Peter )

Data source: Messages  
Folder: MMS - Sent  
Phone Number: +79688685325  
Remote party: +79688685325  
Time stamp: Device time: 9/6/2012 7:39:49 PM  
UTC: 9/6/2012 3:39:49 PM

## Description

## Attachments

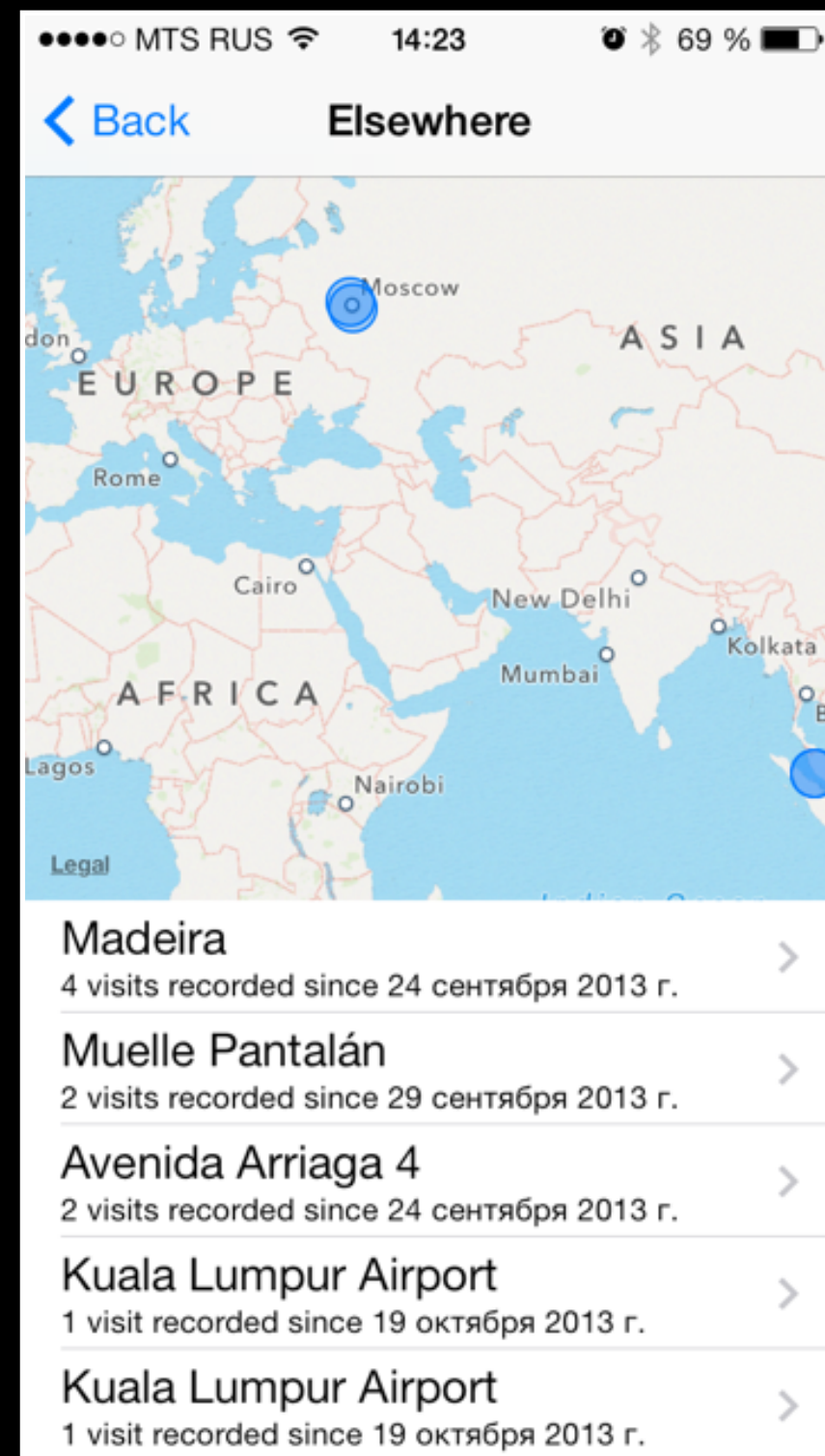
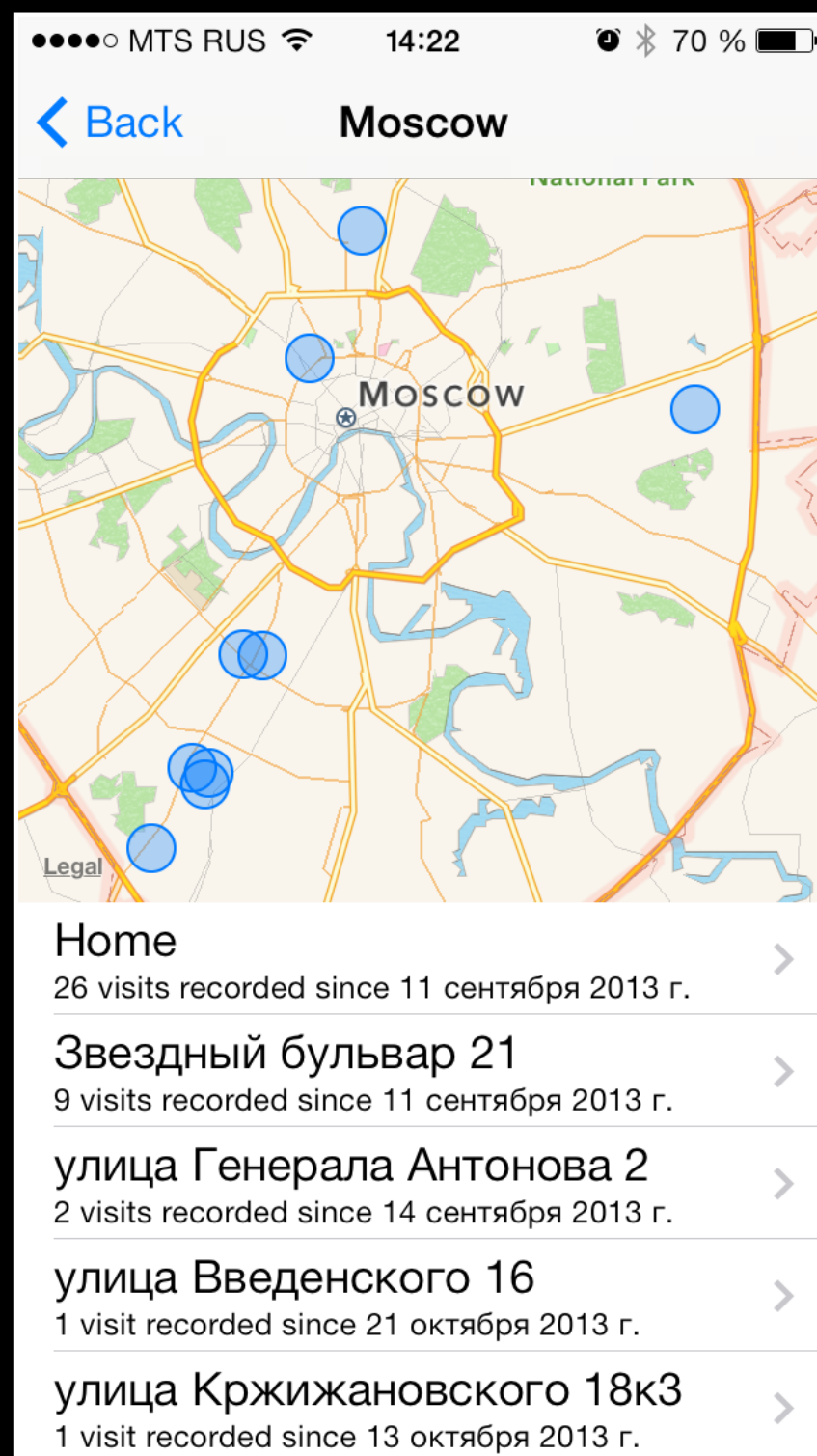
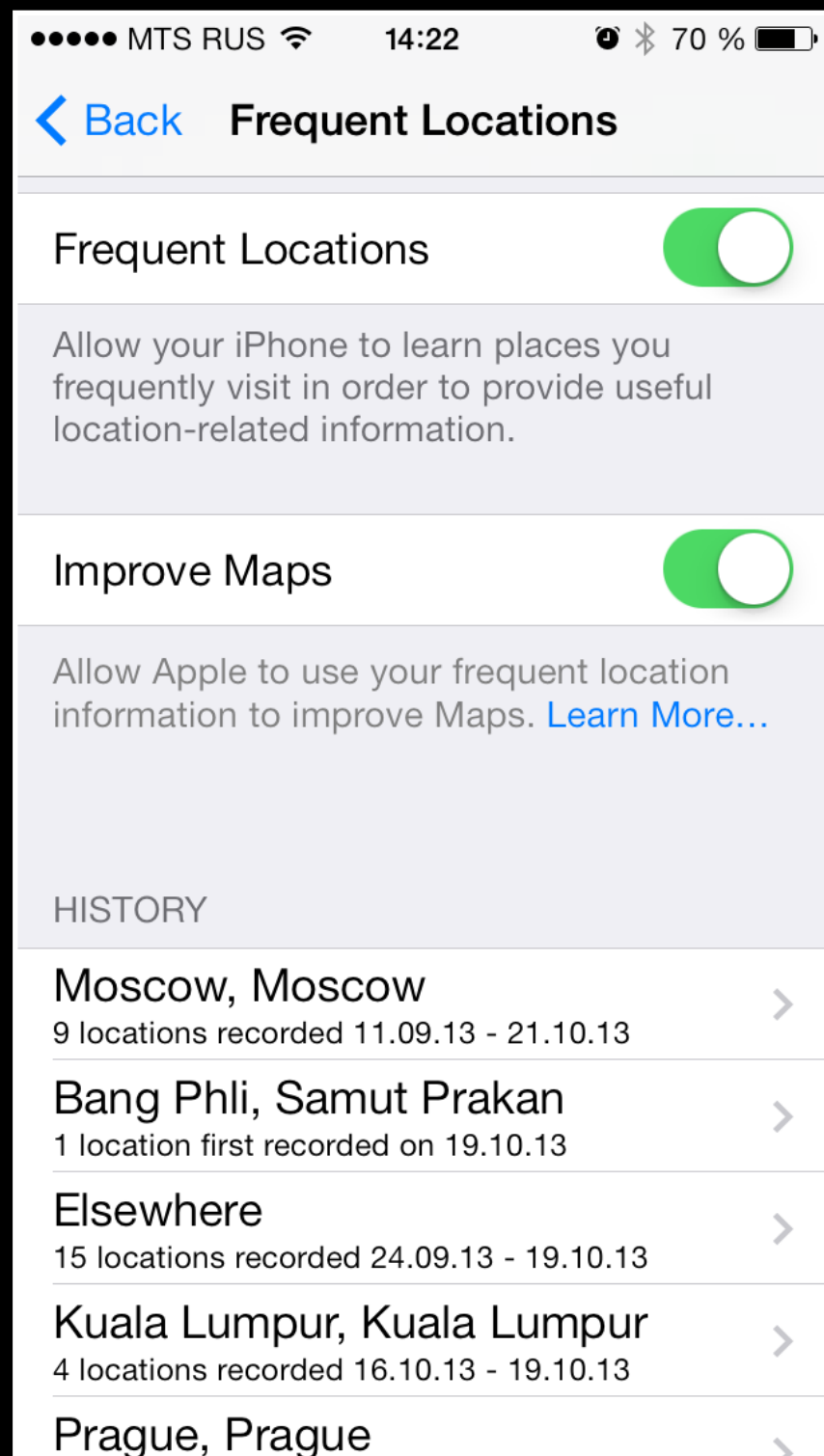
| Name          | Description   | MIME Type  |
|---------------|---------------|------------|
| IMG_2714.jpg  | JPG File      | image/jpeg |
| text_0002.txt | Text Document | text/plain |



Mode: Image

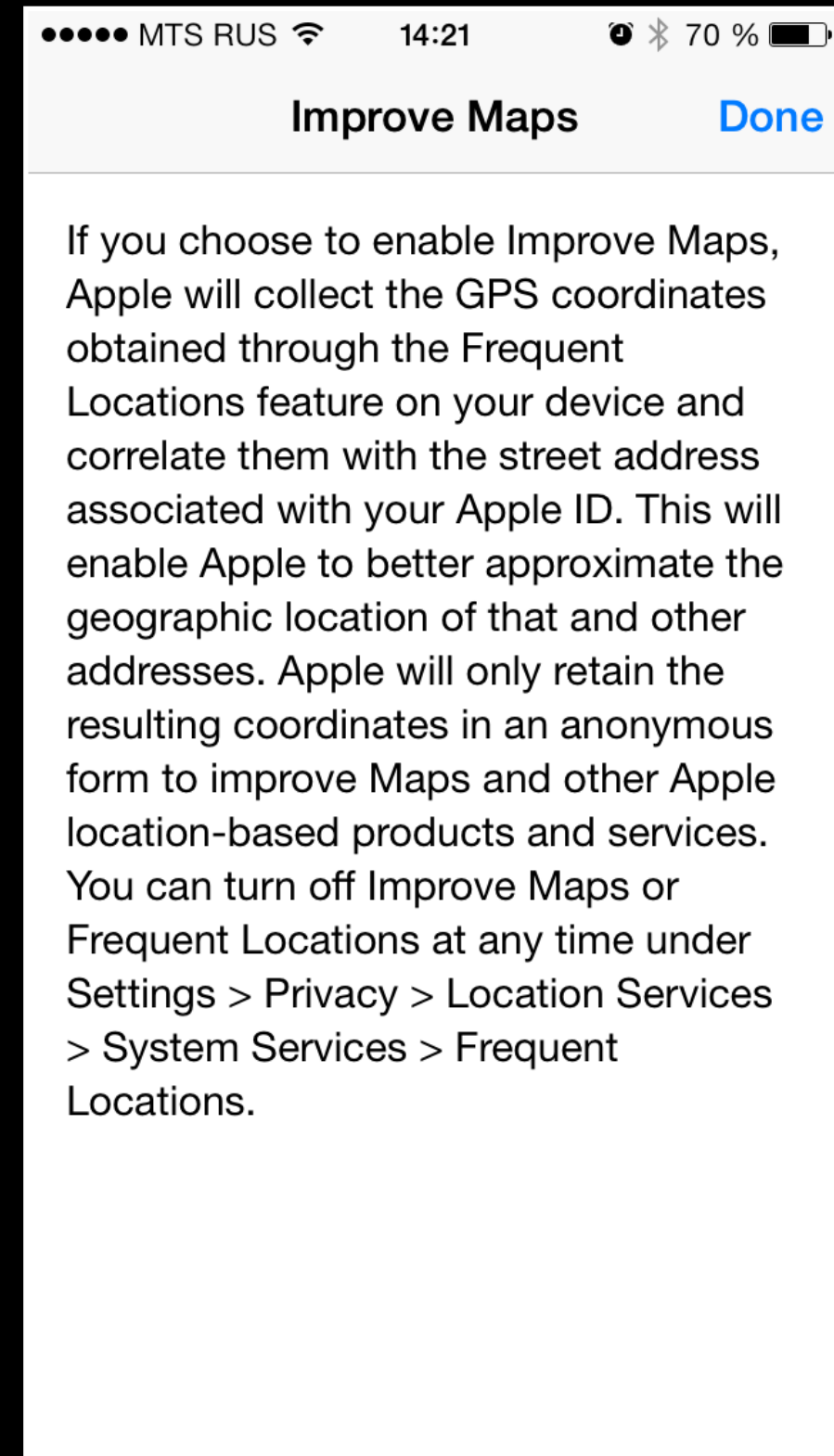
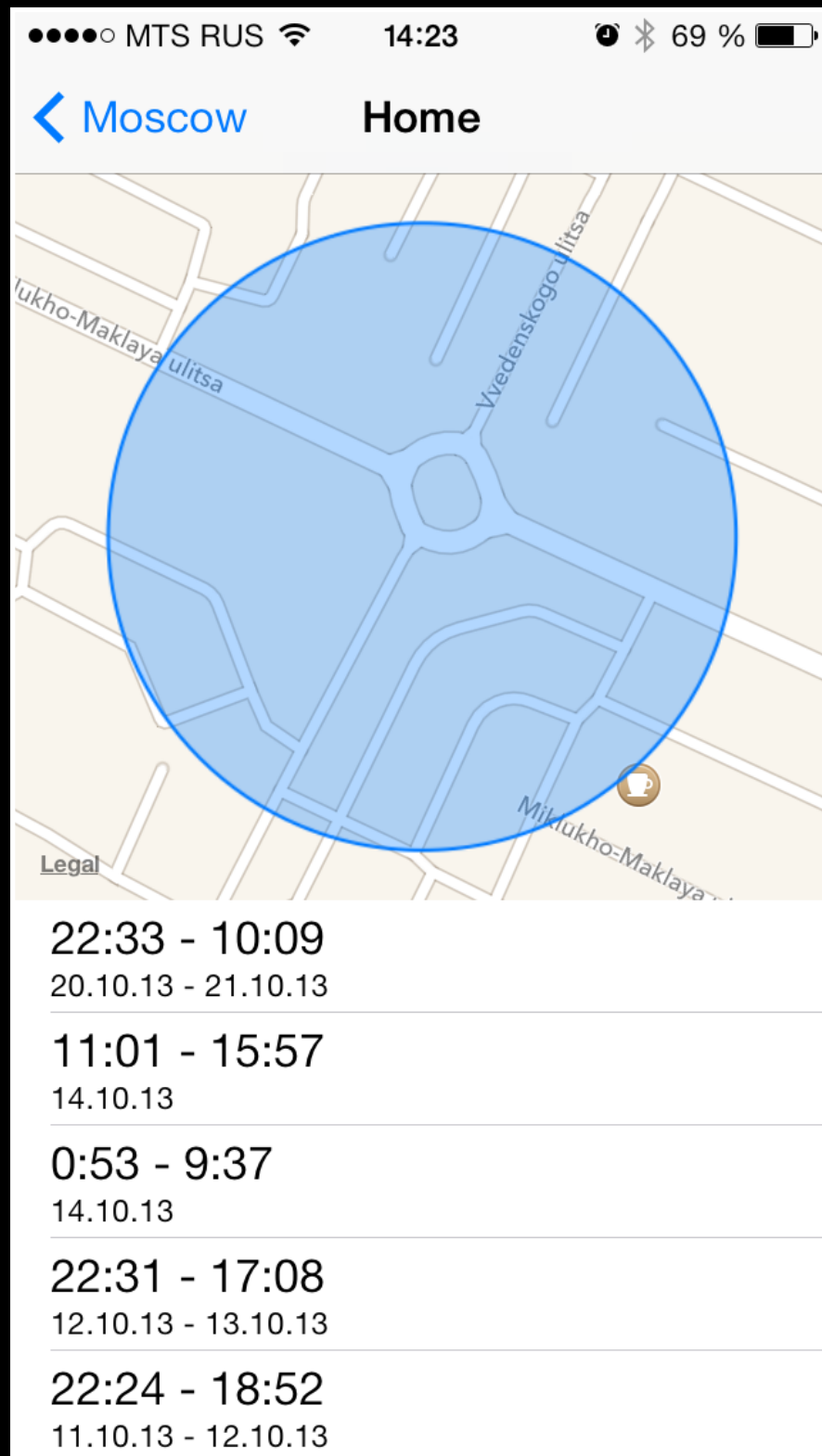
Zoom: Fit

# Frequent locations (iOS 7)

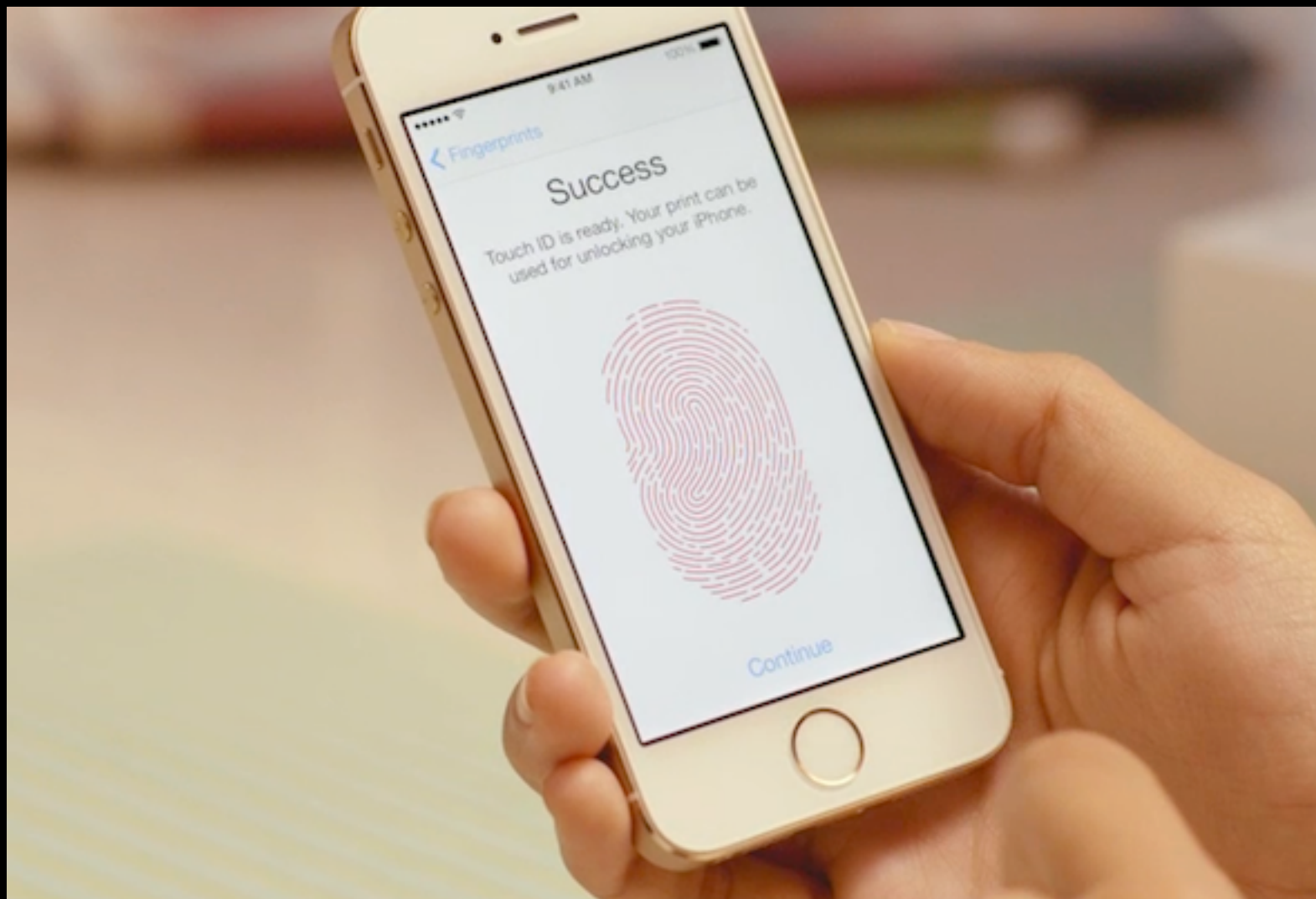




# Home, sweet home...



# Touch ID

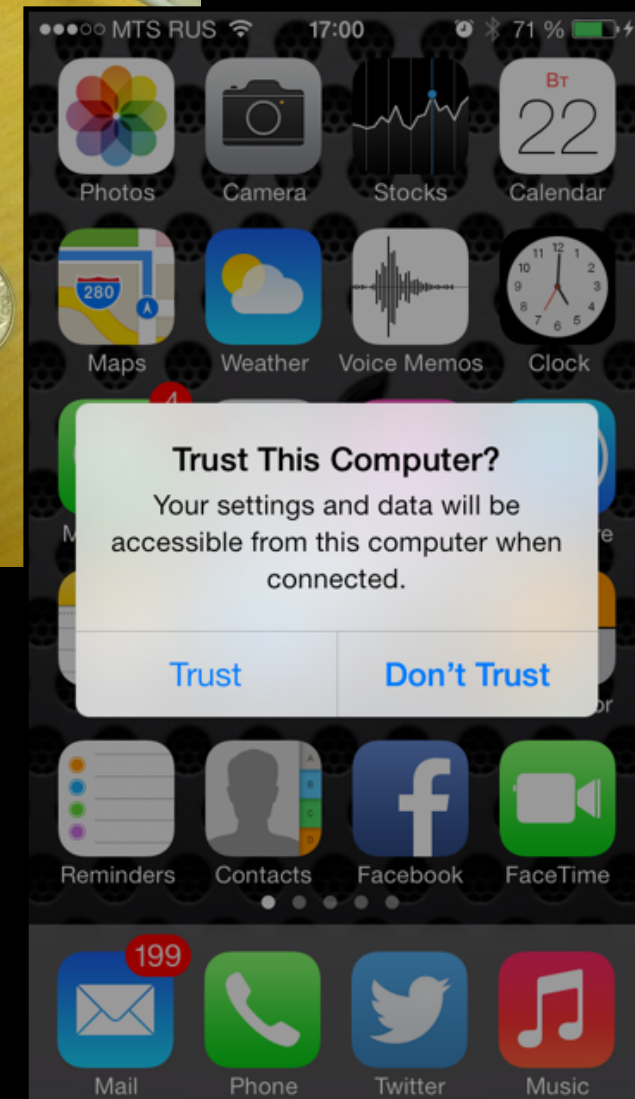
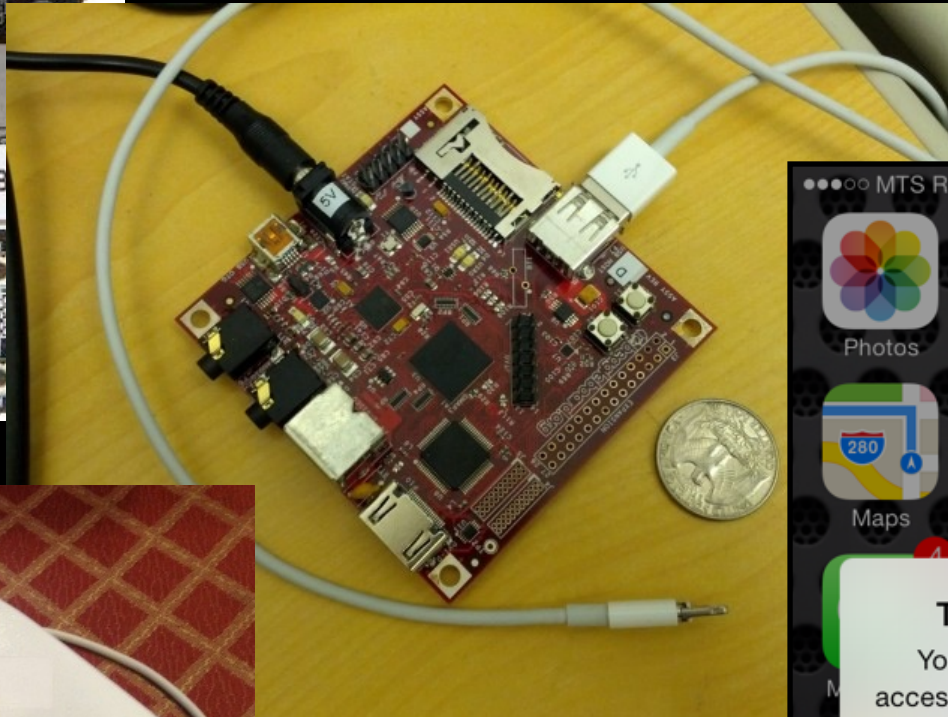
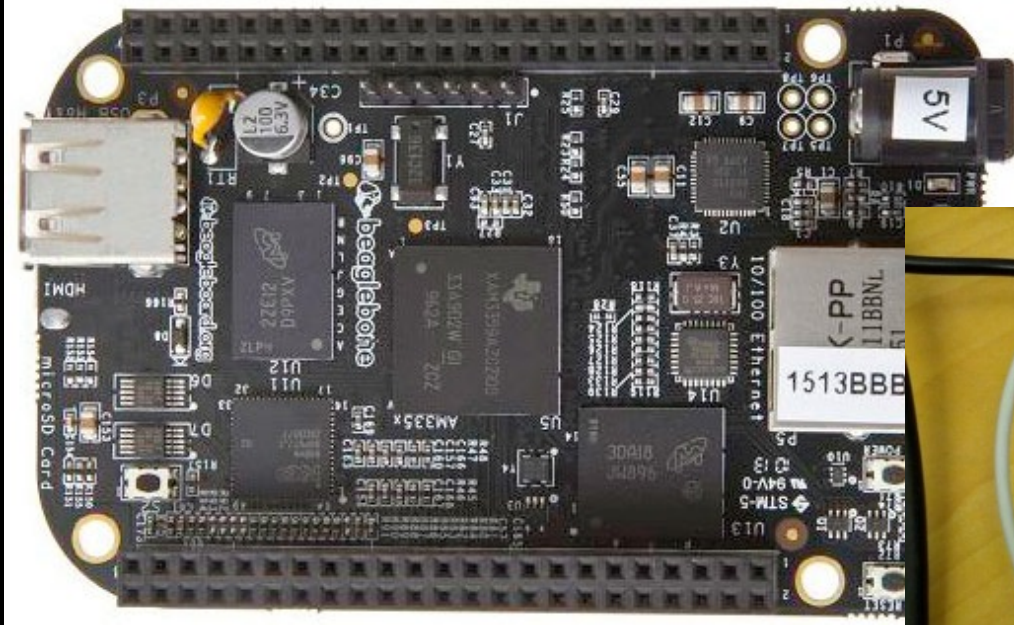


“All fingerprint information is encrypted and stored securely in the Secure Enclave inside the A7 chip on the iPhone 5s; it’s never stored on Apple servers or backed up to iCloud.”

*(From “Apple Announces iPhone 5s—The Most Forward-Thinking Smartphone in the World” at [apple.com](http://apple.com))*



# Backups when charging??



# Pair-locking

- iOS device: /var/root/Library/Lockdown
- Mac: /var/db/lockdown

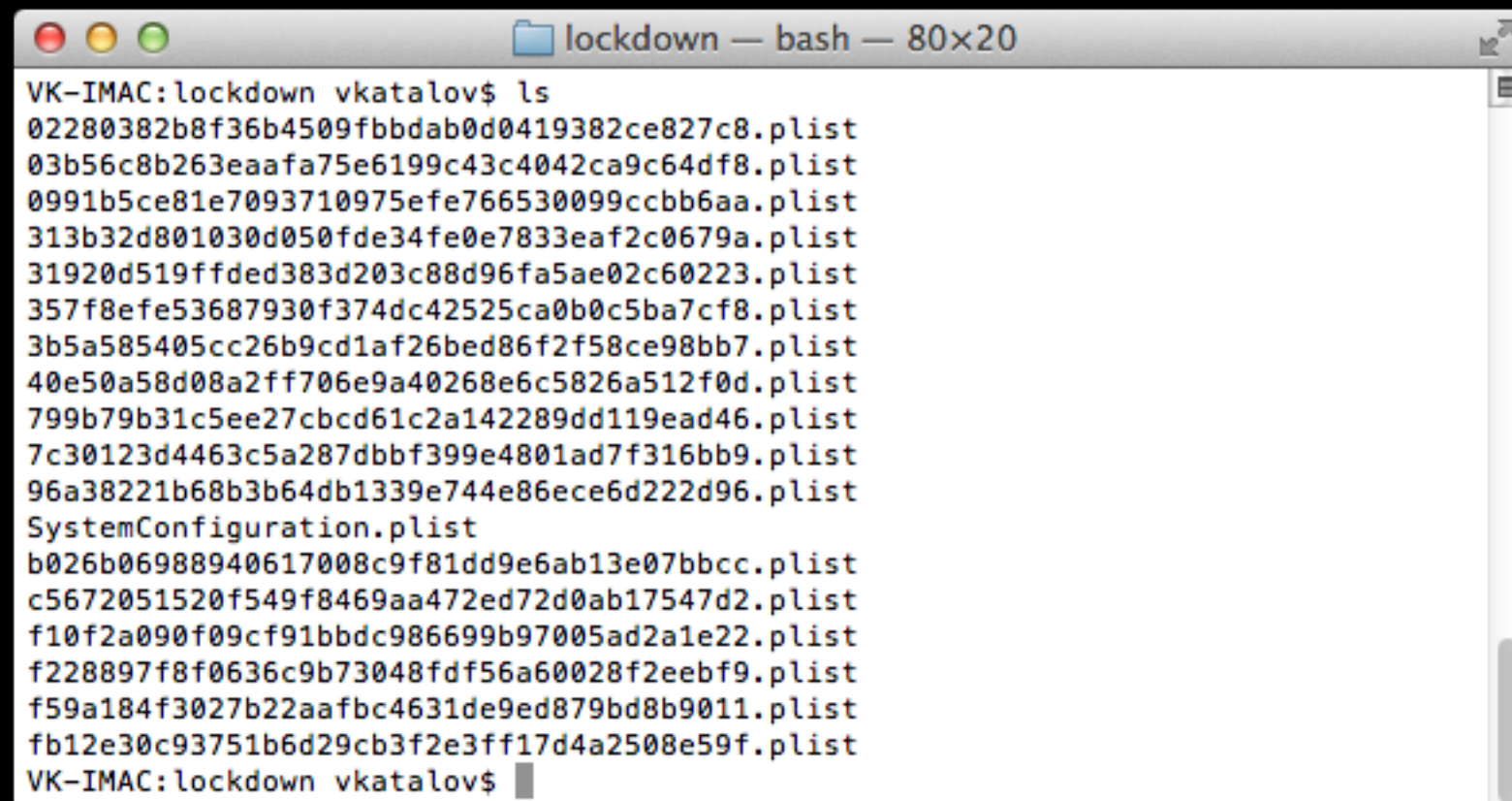
*lockdownd* service

- **backup service**
- software installation service
- get device name & UDID
- sync data
- retrieve a screenshot
- request iOS diagnostic information
- put device into recovery mode
- manage provisioning profiles

More information:

- How to Pair-Lock Your iOS Device  
<http://www.zdziarski.com/blog/?p=2307>
- How Juice Jacking Works  
<http://www.zdziarski.com/blog/?p=2345>
- libmobiledevice  
<http://www.libmobiledevice.org>

*Thanks to Jonathan Zdziarski (@JZdziarski)*



```
lockdown — bash — 80x20
VK-IMAC:lockdown vkatalov$ ls
02280382b8f36b4509fbbdab0d0419382ce827c8.plist
03b56c8b263eaafa75e6199c43c4042ca9c64df8.plist
0991b5ce81e7093710975efe766530099ccbb6aa.plist
313b32d801030d050fde34fe0e7833eaf2c0679a.plist
31920d519ffded383d203c88d96fa5ae02c60223.plist
357f8efe53687930f374dc42525ca0b0c5ba7cf8.plist
3b5a585405cc26b9cd1af26bed86f2f58ce98bb7.plist
40e50a58d08a2ff706e9a40268e6c5826a512f0d.plist
799b79b31c5ee27cbcd61c2a142289dd119ead46.plist
7c30123d4463c5a287dbbf399e4801ad7f316bb9.plist
96a38221b68b3b64db1339e744e86ece6d222d96.plist
SystemConfiguration.plist
b026b06988940617008c9f81dd9e6ab13e07bbcc.plist
c5672051520f549f8469aa472ed72d0ab17547d2.plist
f10f2a090f09cf91bbdc986699b97005ad2a1e22.plist
f228897f8f0636c9b73048fdf56a60028f2eebf9.plist
f59a184f3027b22aafbc4631de9ed879bd8b9011.plist
fb12e30c93751b6d29cb3f2e3ff17d4a2508e59f.plist
VK-IMAC:lockdown vkatalov$
```



# Advanced logical acquisition

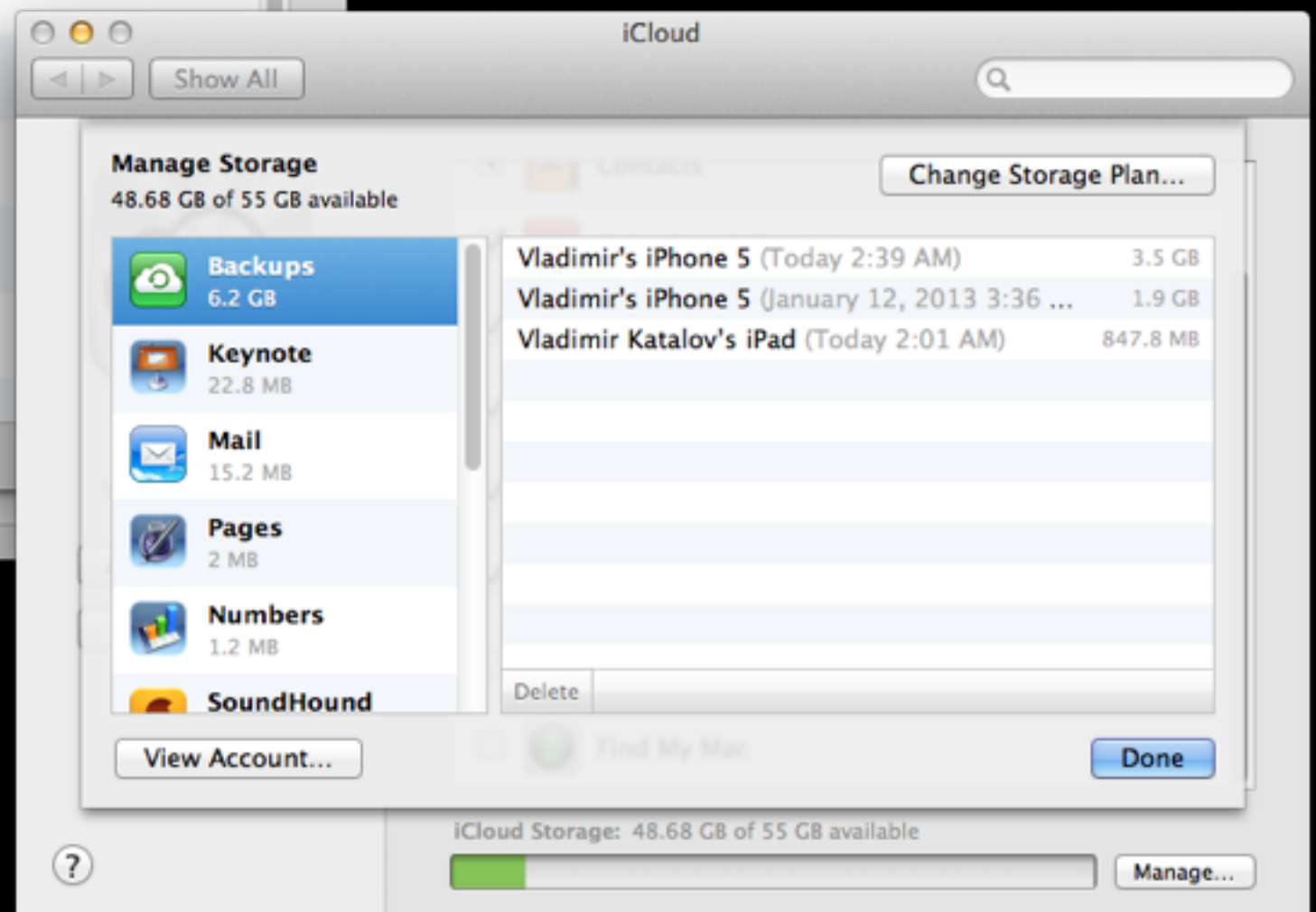
- *for jailbroken devices - the entire file system*
- device information: name, model, IMEI, UUID, serial number etc
- all the media (photos, videos, iTunes library, iBooks)
- application data (including temporary files and *caches* folder)
- various device settings
- log files and diagnostic information
- cached web data (e.g. pictures from social networks)
- keyboard typing caches
- SMS and iMessages (including attachments, even to deleted messages)
- address book
- calendar
- voice mail
- .WAL (Write-Ahead Logging) files for most SQLite databases
- for jailbroken devices - the entire file system
- ...and more

*Works even if device is passcode-locked and backup encryption is set*

*Can be done over Wi-Fi*

*Only need the pairing record*

# iCloud Control Panel





# iCloud backups reverse-engineering

- no backup to iCloud from iTunes :(

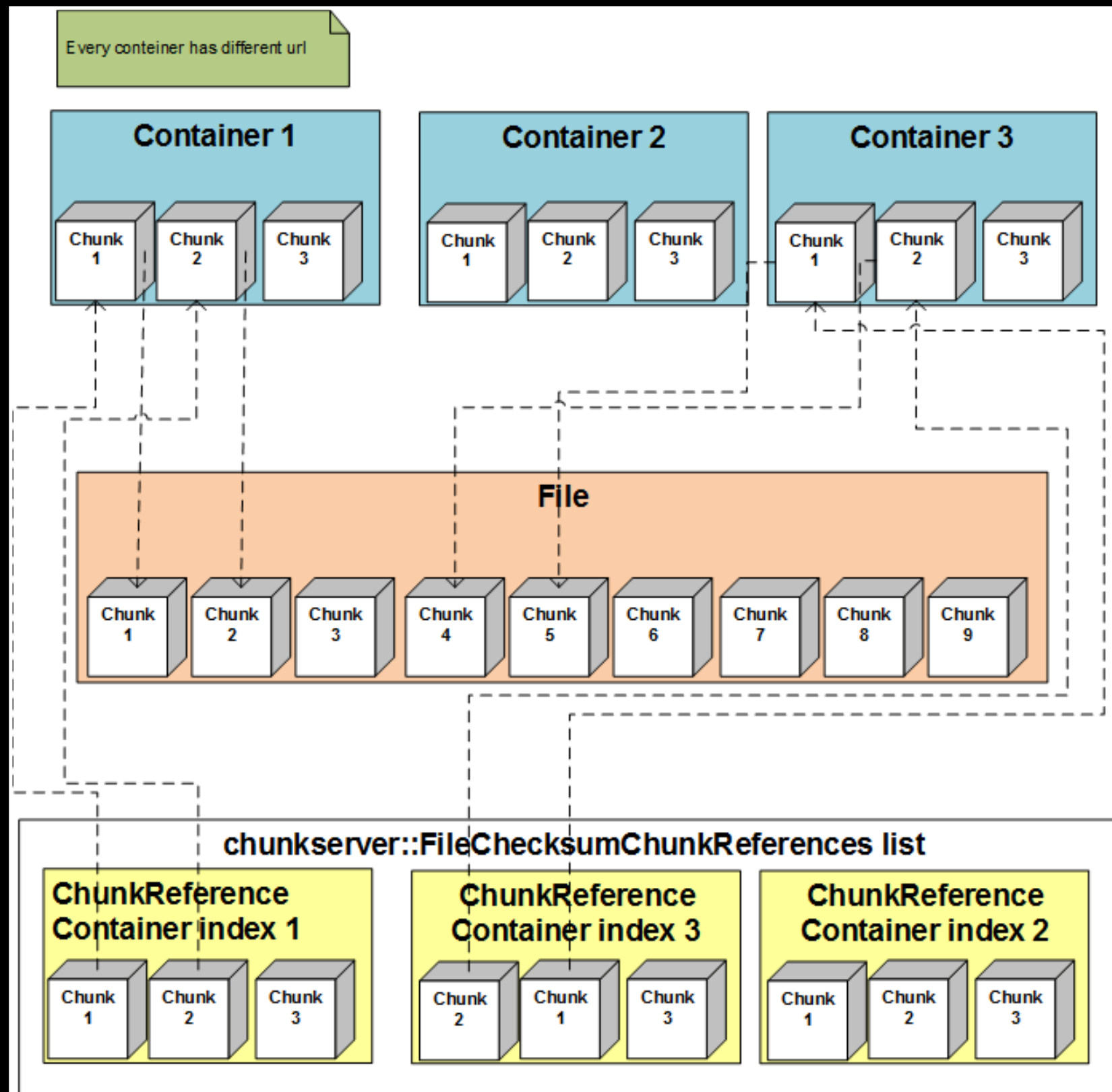
so...

- jailbreak iPhone
- Install Open SSH, get keychain (keychain-2.db)
- [Settings] | [iCloud] | [Delete Account] | [Delete from My iPhone]
- [Settings] | [General] | [Reset] | [Reset All Settings]
- reboot
- set up Wi-Fi connection (proxy)
- replace keychain with our own trusted root certificate (need key 0x835 & keychain)
- ... read all the traffic :)

# iCloud backup protocol flow

- Dynamic: endpoints depend on Apple ID
- Built on Google Protocol Buffers (mostly)
- Files are split into chunks
- Apple provides file-to-chunks mapping, chunk encryption keys, and full request info to 3rd-party storage provider (Amazon/Microsoft)
- Encryption key depends on chunk data

# Files in iCloud



# iCloud backup: authentication

query:

[https://setup.icloud.com/setup/authenticate/\\$APPLE\\_ID\\$](https://setup.icloud.com/setup/authenticate/$APPLE_ID$),

Authorization:Basic <authentication data>

authentication data = mime64 (AppleID:password)

returns: mmeAuthToken, dsPrsID

*example:*

GET /setup/authenticate/\$APPLE\_ID\$ HTTP/1.1

Host: setup.icloud.com

Accept: \*/\*

User-Agent: iCloud.exe (unknown version) CFNetwork/520.2.6

X-Mme-Client-Info: <PC> <Windows; 6.1.7601/SP1.0; W> <com.apple.AOSKit/88>

Accept-Language: en-US

Authorization: Basic cXR0LnRld3RAaWNtb3VkJmNvbTqRd2VydHkxMjM0NQ==



# iCloud backup: get auth. token, backup IDs, keys

query:

[https://setup.icloud.com/setup/get\\_account\\_settings](https://setup.icloud.com/setup/get_account_settings)

Authorization: Basic <authentication data>

authentication data = mime64 (dsPrsID:mmeAuthToken)

returns: mmeAuthToken (new/other one!!)

query:

[https://p11-mobilebackup.icloud.com/mbs/\(dsPrsID\)](https://p11-mobilebackup.icloud.com/mbs/(dsPrsID))

Authorization: <authentication data>

authentication data = mime64 (dsPrsID:mmeAuthToken)

returns: list of backup IDs (backupudid)

query:

[https://p11-mobilebackup.icloud.com/mbs/2005111682/\(backupudid\)/getKeys](https://p11-mobilebackup.icloud.com/mbs/2005111682/(backupudid)/getKeys)

# iCloud backup: download files (1)

*Enumerate snapshots*

HTTPS GET

[https://p11-mobilebackup.icloud.com/mbs/\(dsPrsID\)/\(backupudid\)/\(snapshotid\)/listFiles?offset=\(offset\)&limit=\(limit\)](https://p11-mobilebackup.icloud.com/mbs/(dsPrsID)/(backupudid)/(snapshotid)/listFiles?offset=(offset)&limit=(limit))

*Get file authentication tokens*

HTTPS POST

[https://p11-mobilebackup.icloud.com/mbs/\(dsPrsID\)/\(backupudid\)/\(snapshotid\)/getFiles](https://p11-mobilebackup.icloud.com/mbs/(dsPrsID)/(backupudid)/(snapshotid)/getFiles)

*Get URLs for file chunks*

HTTPS POST

[https://p11-content.icloud.com/\(dsPrsID\)/authorizeGet](https://p11-content.icloud.com/(dsPrsID)/authorizeGet)

# iCloud backup: download files (2)

## *Download chunks*

Windows Azure:

[http://msbnx000004.blob.core.windows.net:80/cnt/g6YMJKQBPxQruxQAr30C?  
sp=r&sr=b&byte-  
range=154-31457433&se=2013-06-07T10:14Z&st=2013-06-07T09:19Z&sig=0EdHy7  
5gGHCee%2BjKePZBqz8xbWxpTxaYyASwFXVx2%2Fg%3D](http://msbnx000004.blob.core.windows.net:80/cnt/g6YMJKQBPxQruxQAr30C?sp=r&sr=b&byte-range=154-31457433&se=2013-06-07T10:14Z&st=2013-06-07T09:19Z&sig=0EdHy75gGHCee%2BjKePZBqz8xbWxpTxaYyASwFXVx2%2Fg%3D)

*'se' contains iCloud authorization time (expires in one hour)*

Amazon AWS:

[http://us-std-00001.s3-external-1.amazonaws.com/I9rh20QBPX4jizMAr3vY?x-client-  
request-id=739A222D-0FF5-44DD-  
A8FF-2A0EB6F49816&Expires=1371208272&byte-  
range=25556011-25556262&AWSAccessKeyId=AKIAIWWR33ECHKPC2LUA&Signa  
ture=PxAdegw0PLyBn7GWZCnu0bhi3Xo%3D](http://us-std-00001.s3-external-1.amazonaws.com/I9rh20QBPX4jizMAr3vY?x-client-request-id=739A222D-0FF5-44DD-A8FF-2A0EB6F49816&Expires=1371208272&byte-range=25556011-25556262&AWSAccessKeyId=AKIAIWWR33ECHKPC2LUA&Signature=PxAdegw0PLyBn7GWZCnu0bhi3Xo%3D)

# iCloud backups: data encryption

- get keyData from iCloud
- wrappedOffset = keyDataSize - (ECP\_LEN + WRAPPED\_KEY\_LEN)
- get wrappedKey (at wrappedOffset)
- get CLASS\_KEY
  - iOS 5/6: ((UINT32\*)(keyData + wrappedOffset))[-1]
  - iOS 7: ((UINT32\*)(keyData + wrappedOffset))[-3]
- decrypt wrappedKey using CLASS\_KEY
- get AES\_KEY from wrappedKey
- file decryption: by 0x1000 blocks (unique IV for every block)

```
#define HFS_IV_GENERATOR 0x80000061
#define IV_GEN(x) (((x) >> 1) ^ (((x) & 1) ? HFS_IV_GENERATOR : 0))
```

```
static UInt8 *genIV (UInt32 seed, void *pIV) {
    UInt32 *pdw = (UInt32*)pIV;
    pdw[0] = seed = IV_GEN(seed);
    pdw[1] = seed = IV_GEN(seed);
    pdw[2] = seed = IV_GEN(seed);
    pdw[3] = seed = IV_GEN(seed);
    return (UInt8*)pIV;
}
```

to get aesIV: sha1(AES\_KEY)

```
AES_KEY aesIV;
makeIVkey (&aesIV, abKey, SYSTEM_KEY_LEN);
(abKey is AES_KEY we have got from wrappedKey)
```

```
static AES_KEY *makeIVkey (AES_KEY *pAES, UInt8 *pb, size_t cb) {
    SHA_CTX sha;
    UInt8 abHash[SHA_DIGEST_LENGTH];
    SHA1_Init (&sha);
    SHA1_Update (&sha, pb, cb);
    SHA1_Final (abHash, &sha);
    AES_set_encrypt_key (abHash, 128, pAES);
    return pAES;
}
```

# iCloud encryption

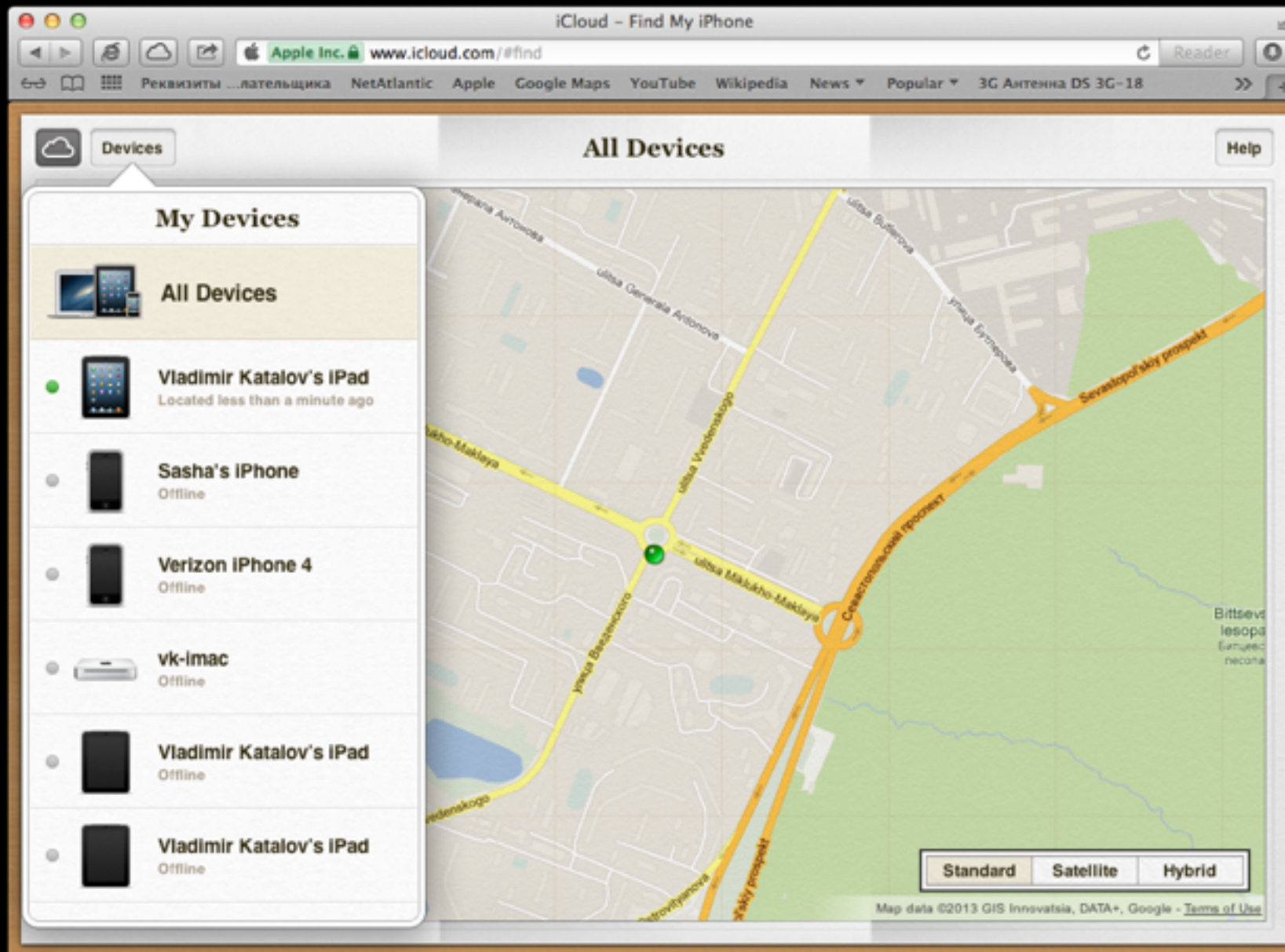
- Data stored at 3rd-party storage providers is encrypted
- Apple has encryption keys to that data
- Few files are further encrypted using keys from OTA backup keybag
- Keychain items are encrypted using keys from OTA backup keybag
- Need key 0x835 (securityd) to decrypt most keys from OTA backup keybag

## iCloud backups - summary

- There is no user-configurable encryption for iCloud backups
- iCloud backups are stored in Microsoft and Amazon clouds in encrypted form
- Apple holds encryption keys and thus have access to data in iCloud backups
- **If Apple stores 0x835 keys then it can also have access to Keychain data (i.e. passwords)**
- Apple may have legal obligations to do this (e.g. LE)
- No notification after backup downloading (as with device restore)



# Find My Phone



# FindMyPhone protocol

How: just sniffing HTTP traffic ([www.icloud.com](http://www.icloud.com), Find My Phone)

## Authentication:

validate:  
<https://setup.icloud.com/setup/ws/1/validate>

*ClientBuildNumber=1M.63768 (constant)*  
*ClientId (random GUID)*  
*<- instance*

login:  
<https://setup.icloud.com/setup/ws/1/login>

*AppleID*  
*extended\_login*  
*id=sha1(apple\_id+instance)*  
*password*  
*<- dsid*

## Get devices with location:

initClient:  
<https://p11-fmipweb.icloud.com/fmipservice/client/web/initClient>

refreshClient:  
<https://p11-fmipweb.icloud.com/fmipservice/client/web/refreshClient>

*id*  
*dsid*  
*<- content (location)*

# FindMyPhone - demo output

```
locations.txt — Edited

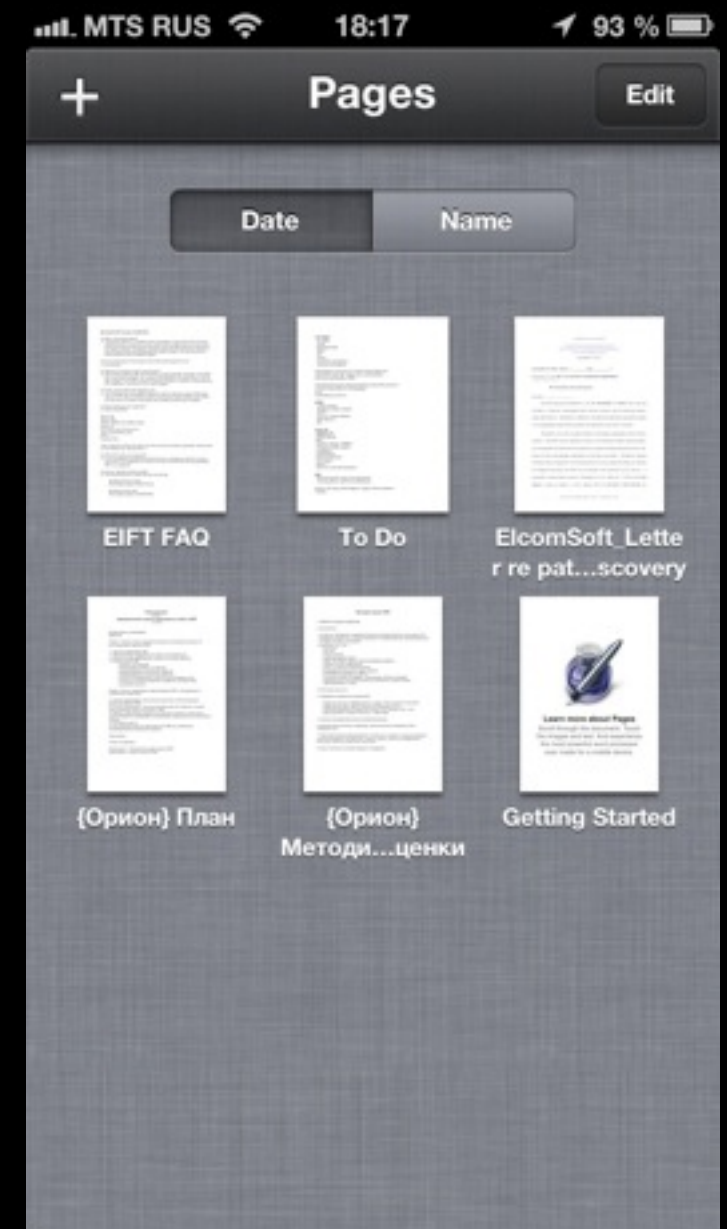
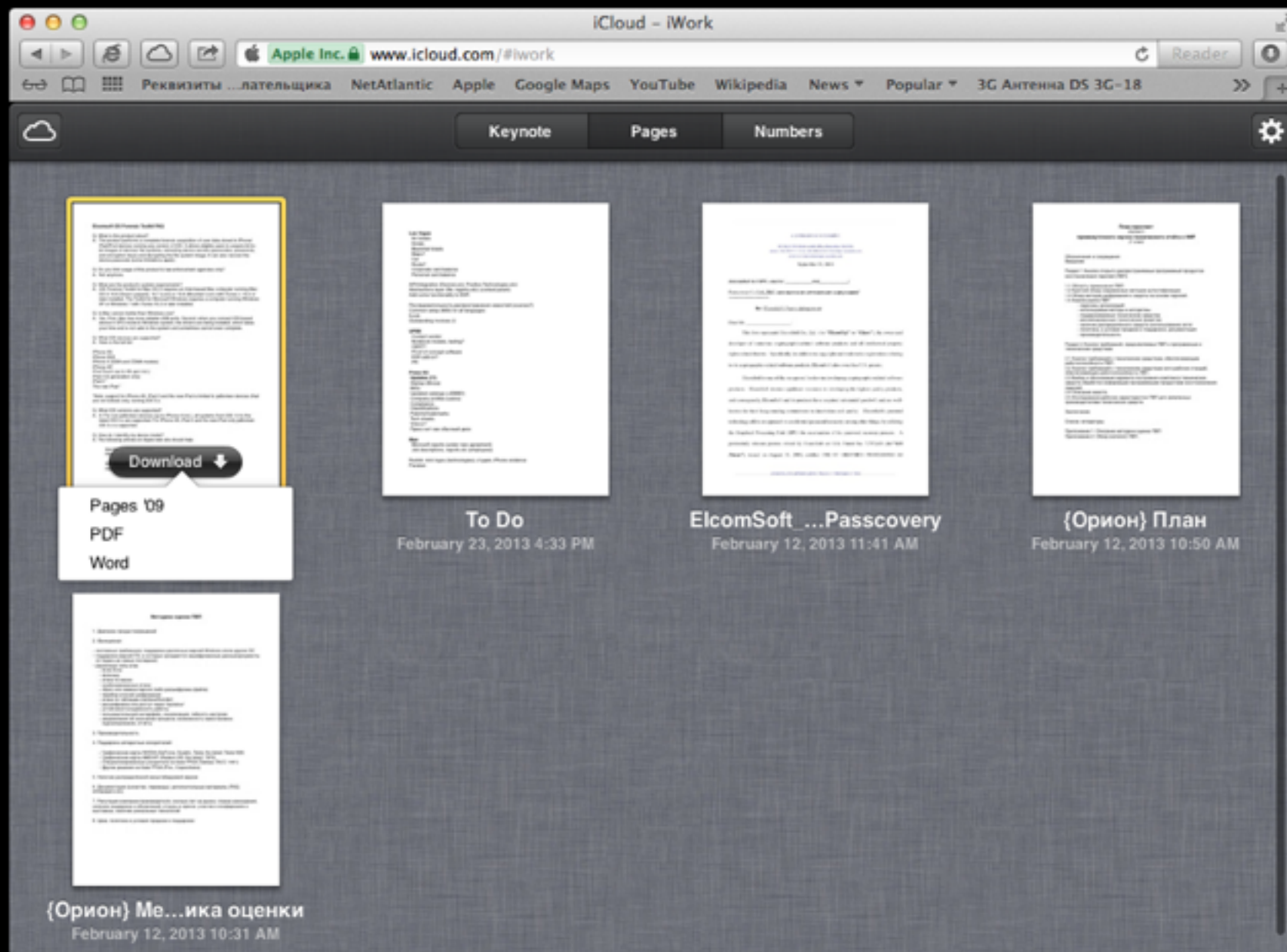
===== Device #1=====
deviceModel = SixthGen-white
modelDisplayName = iPhone
id = QVBT0mIwMiZiMDY5ODg5NDA2MTcwMDhjOWY4MWRkOWU2YWIXM2UwN2JiY2M~
deviceDisplayName = iPhone 5
name = Vladimir's iPhone 5
batteryLevel = 0.700216
locationEnabled = 1
longitude = 37.6243
latitude = 55.8114
positionType = Wifi
isOld = 0
Device found: 00:00:27.786000 ago

===== Device #3=====
deviceModel = MacBookAir3_2
modelDisplayName = MacBook Air
id = QVBT0jg3MzBFNj05LTdGRjktNTkzRC1CMzI3LUZCMkRfNjA2NjRCRA~~
deviceDisplayName = MacBook Air 13"
name = Vladimir Katalov's MacBook Air
batteryLevel = 0
locationEnabled = 1
longitude = 0
latitude = 0
positionType =
isOld = 0
Device not found

===== Device #6=====
deviceModel = ThirdGen-4G
modelDisplayName = iPad
id = QVBT0jAzYiU2YzhiMjYzZWZhZmE3NWU2MTk5YzQzYz0wNDJiYTljNiRkZig~
deviceDisplayName = iPad
name = Vladimir Katalov's iPad
batteryLevel = 0.74746
locationEnabled = 1
longitude = 37.6245
latitude = 55.8113
positionType = Wifi
isOld = 0
Device found: 00:00:36.485000 ago
```



# iCloud documents



# Get files from iCloud

## To get list of files

- Authentication request (with given AppleID & password). Client gets mmeAuthToken in return; which, in order, is used to create authentication token (together with dsid). dsid (Destination Signaling Identifier) is an unique ID assigned to the user when registering at iCloud.com.
- Request to get AccountSettings. Client gets an URL (ubiquityUrl) with an address to get UUID (unique user identifier), file list, info on file tokens and for authorization.
- Request to get file list (POST). Output (for every file):
  - file name
  - file id
  - parent folder id
  - last change time
  - checksum
  - access rights

## To download given file

- Request to get file token (using file id, checksum and aliasMap).
- Authorization request. Returns information on file chunks and containers. Output: container list (with URLs) and chunk information.

# iCloud backup: packages

- KeyNote: PDF, Microsoft PowerPoint, KeyNote '09
- Pages: PDF, Microsoft Word, Pages '09
- Numbers: PDF, Microsoft Excel, Numbers '09
- Some other programs (1Password etc)

Storage: plist + content (text, media files)

Requests:

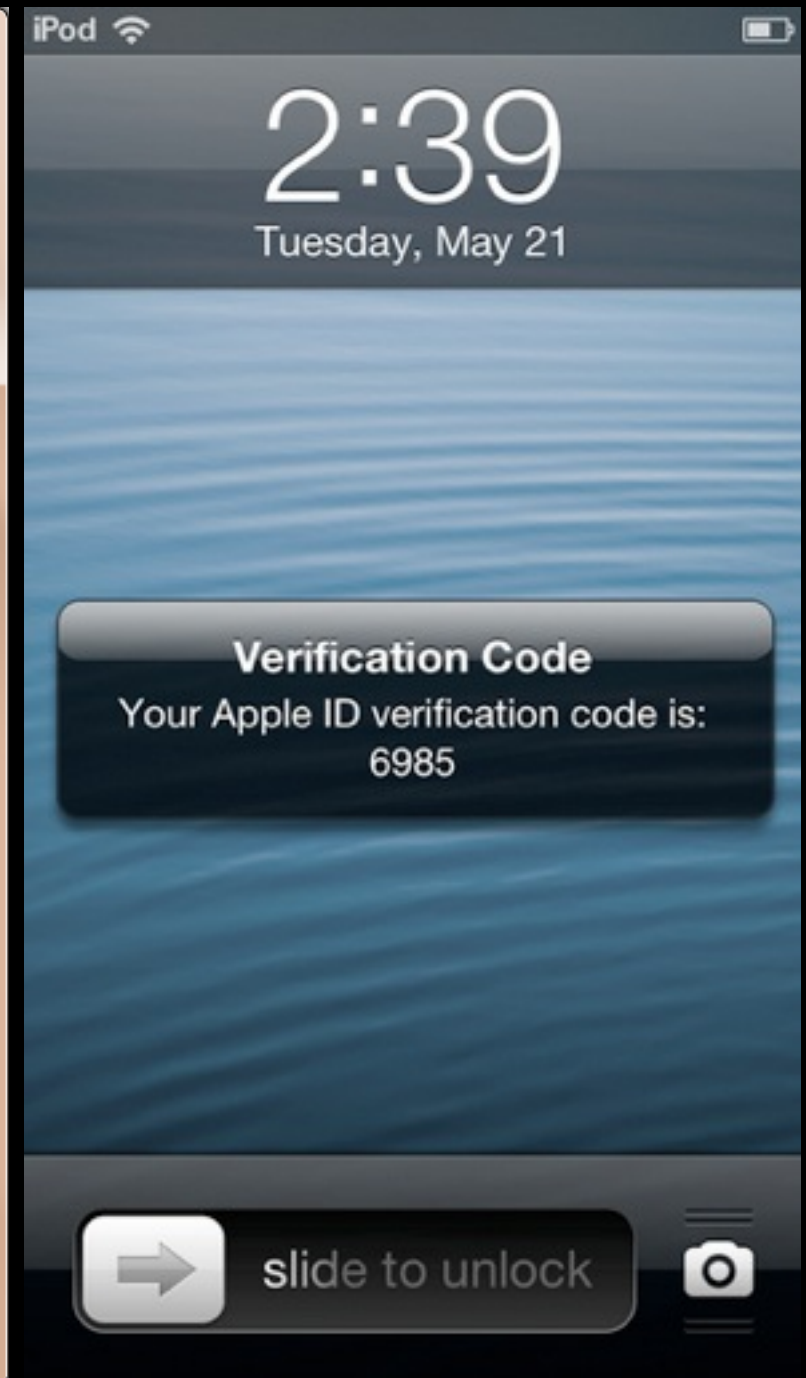
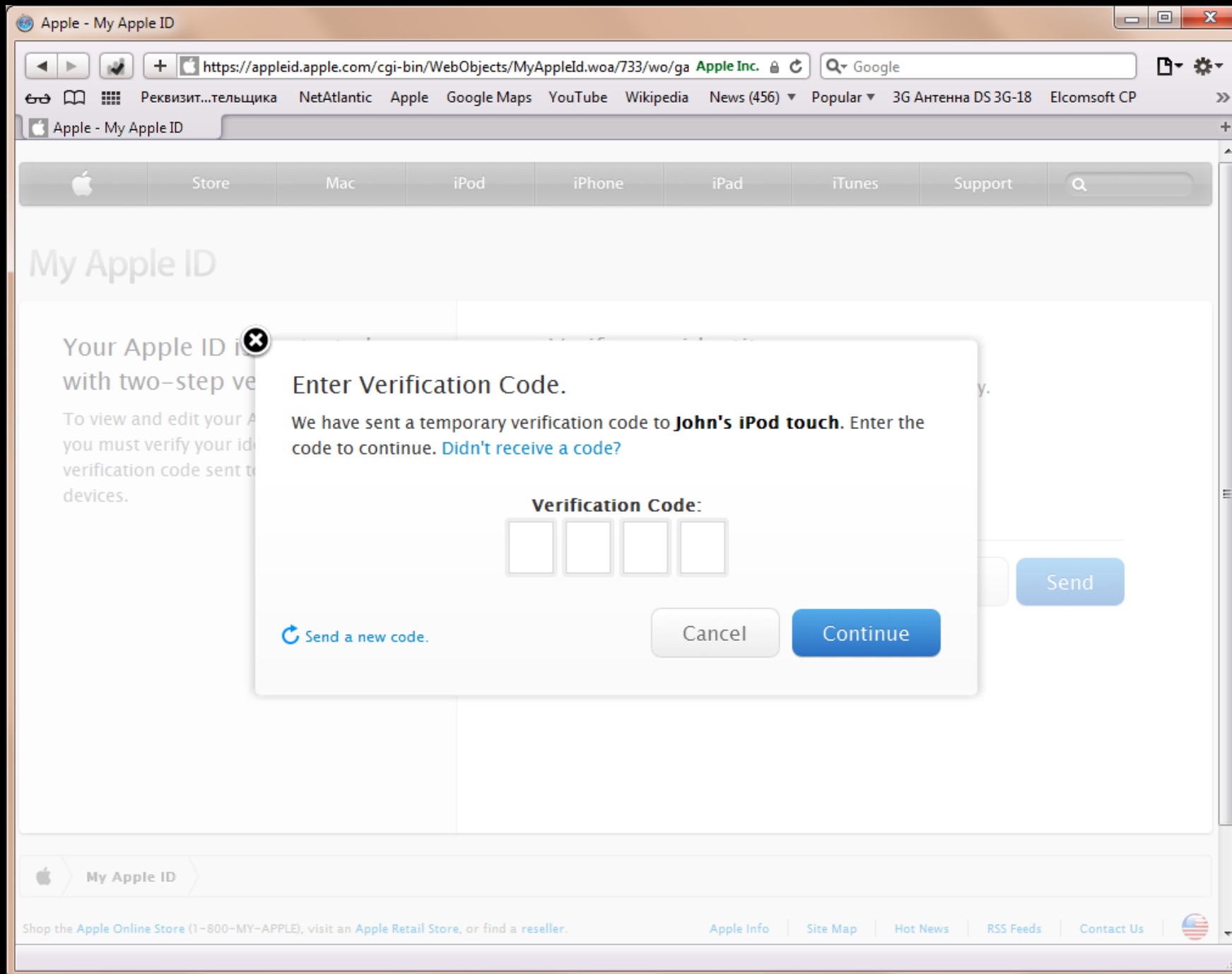
- Validate  
<https://setup.icloud.com/setup/ws/1/validate>
- Login  
<https://setup.icloud.com/setup/ws/1/login>
- Export  
[https://p15-ubiquityws.icloud.com/iw/export/\(dsid\)/export\\_document?...](https://p15-ubiquityws.icloud.com/iw/export/(dsid)/export_document?...)
- Check export status  
[https://p15-ubiquityws.icloud.com/iw/export/\(dsid\)/check\\_export\\_status?...](https://p15-ubiquityws.icloud.com/iw/export/(dsid)/check_export_status?...)
- Download converted file  
[https://p15-ubiquityws.icloud.com/iw/export/\(dsid\)/download\\_exported\\_document?](https://p15-ubiquityws.icloud.com/iw/export/(dsid)/download_exported_document?)



# iCloud docs: demo output

```
files_list.txt — Edited ▾  
File name: buildVersionHistory.plist  
File path: /com~apple~Pages/Documents/EIFT FAQ.pages-tef/buildVersionHistory.plist  
File id: 4222124650662430  
File size: 221 bytes  
  
File name: index.db  
File path: /com~apple~Pages/Documents/EIFT FAQ.pages-tef/index.db  
File id: 4222124650662429  
File size: 376832 bytes  
  
File name: index.viewstate  
File path: /com~apple~Pages/Documents/EIFT FAQ.pages-tef/index.viewstate  
File id: 4222124650662435  
File size: 713 bytes  
  
File name: metadata.plist  
File path: /com~apple~Pages/Documents/EIFT FAQ.pages-tef/metadata.plist  
File id: 4222124650662431  
File size: 416 bytes  
  
File name: preview-micro.jpg  
File path: /com~apple~Pages/Documents/EIFT FAQ.pages-tef/preview-micro.jpg  
File id: 4222124650662442  
File size: 1489 bytes  
  
File name: preview-web.jpg  
File path: /com~apple~Pages/Documents/EIFT FAQ.pages-tef/preview-web.jpg  
File id: 4222124650662443  
File size: 11782 bytes  
  
File name: preview.jpg  
File path: /com~apple~Pages/Documents/EIFT FAQ.pages-tef/Previews/preview.jpg  
File id: 4222124650662444  
File size: 45229 bytes  
  
File name: EIFT FAQ.jpg  
File path: /com~apple~Pages/iWorkPreviews/EIFT FAQ.jpg  
File id: 4222124650662514  
File size: 45229 bytes
```

# Apple 2FA (two-step verification)



# Apple 2FA

## (cont-d)

Requires to verify your identity using one of your devices before you can:

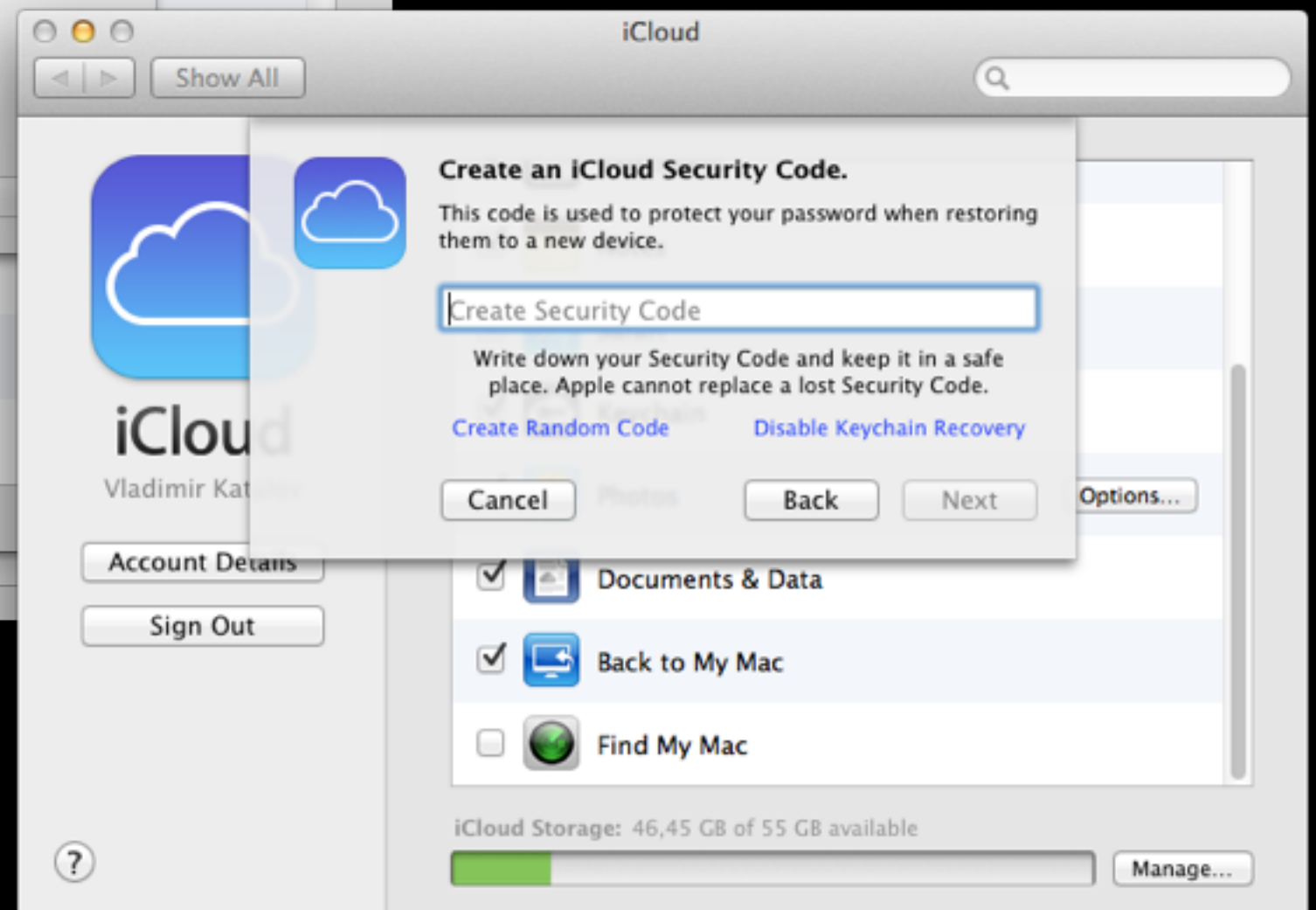
- Sign in to My Apple ID to manage your account.
- Make an iTunes, App Store, or iBookstore purchase from a new device.
- Get Apple ID-related support from Apple.

Does **NOT** protect:

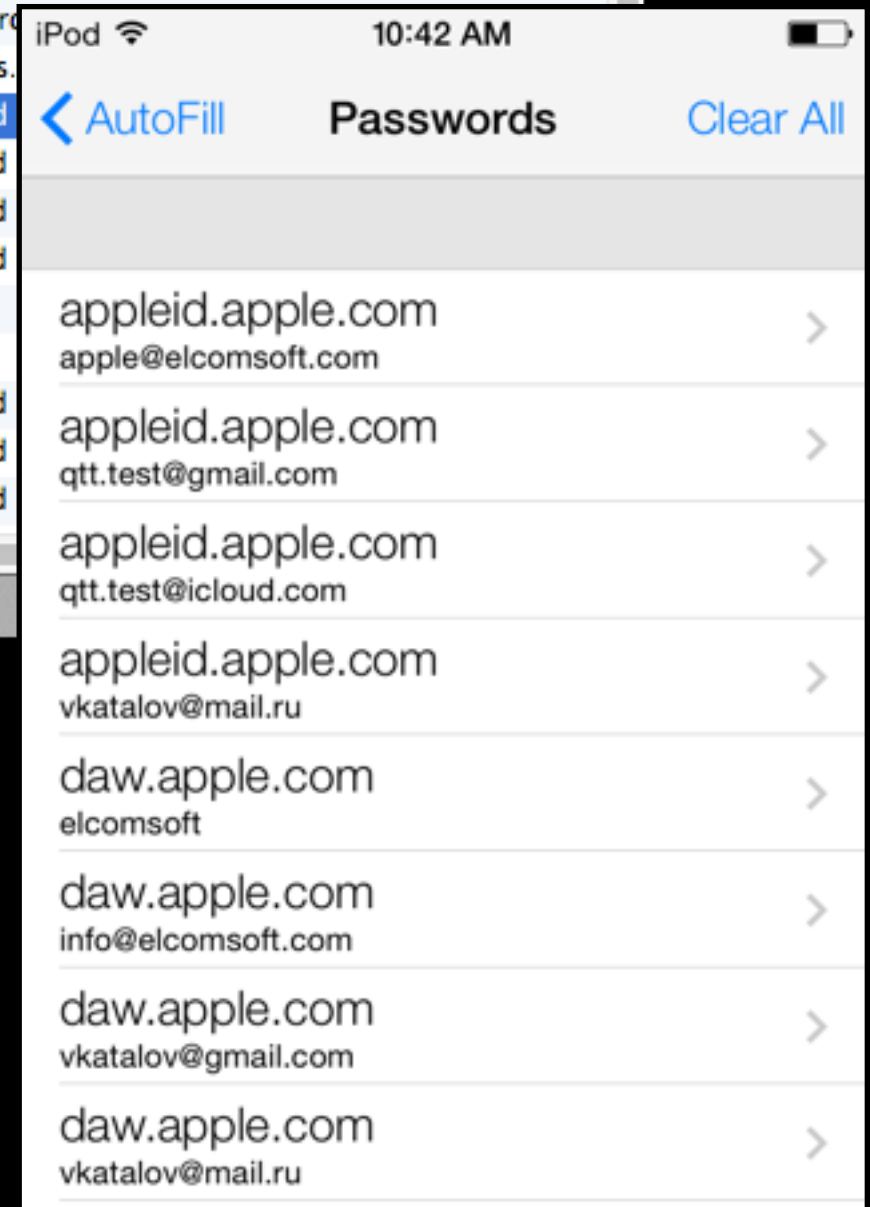
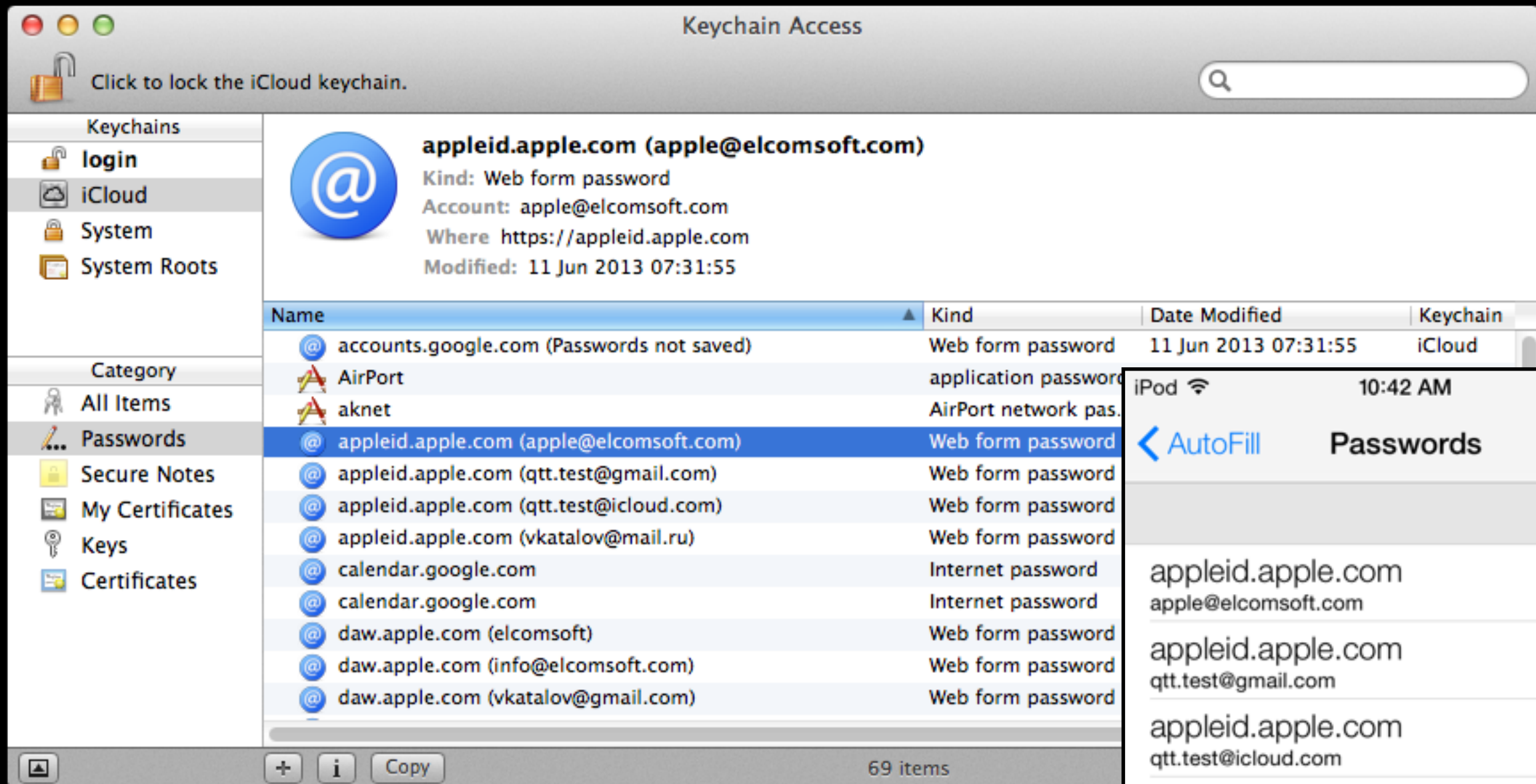
- iCloud backups
- Find My Phone data
- Documents stored in the cloud

# Apple iOS 7

## iCloud keychain



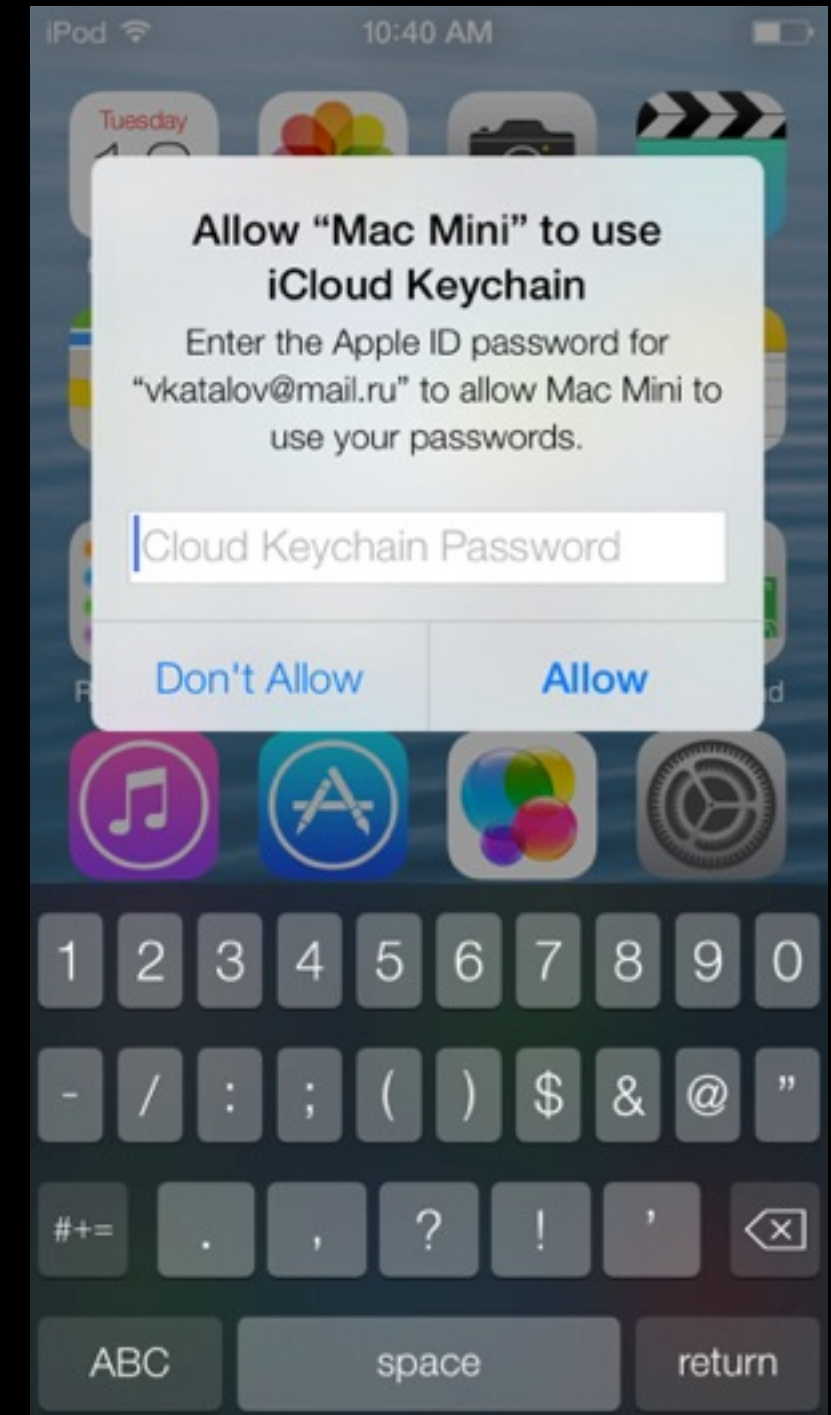
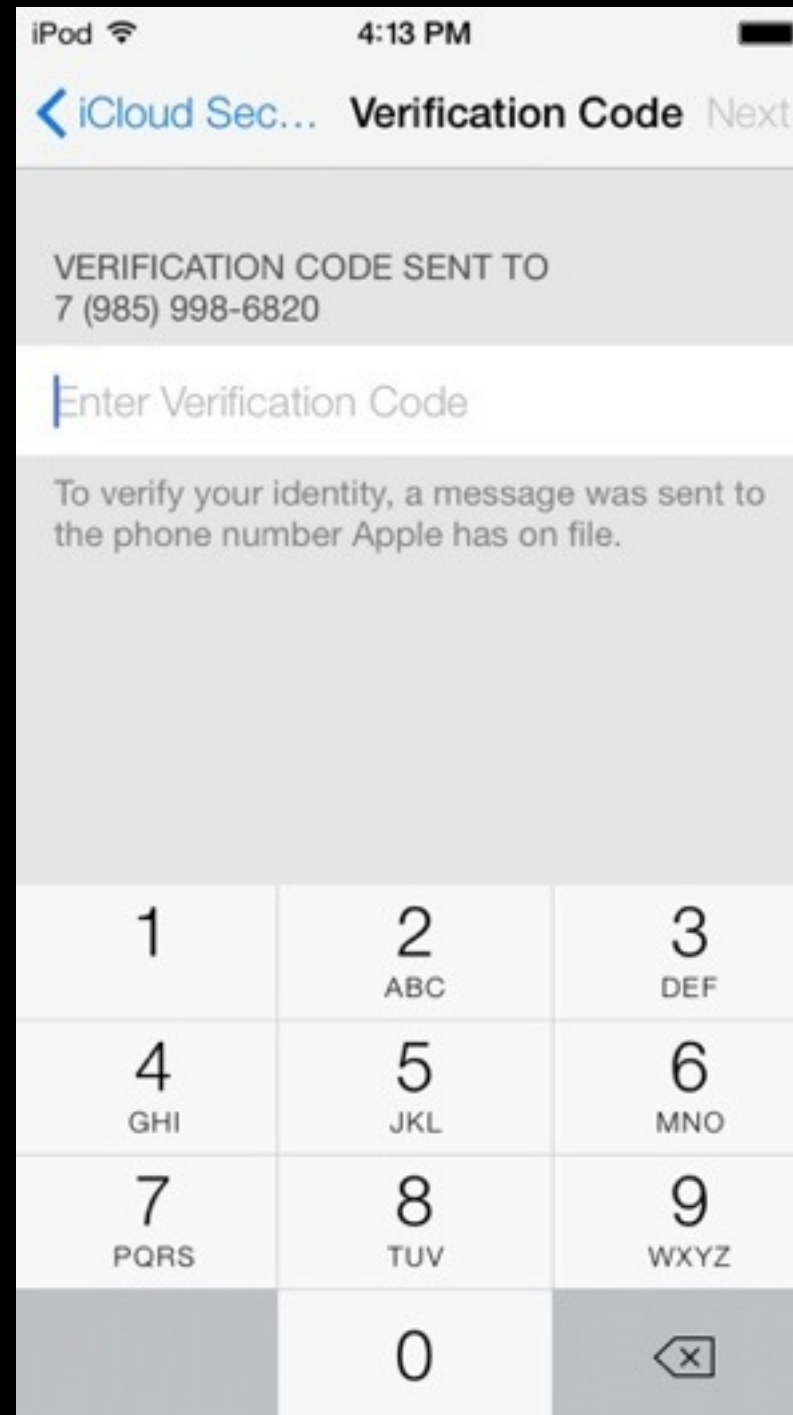
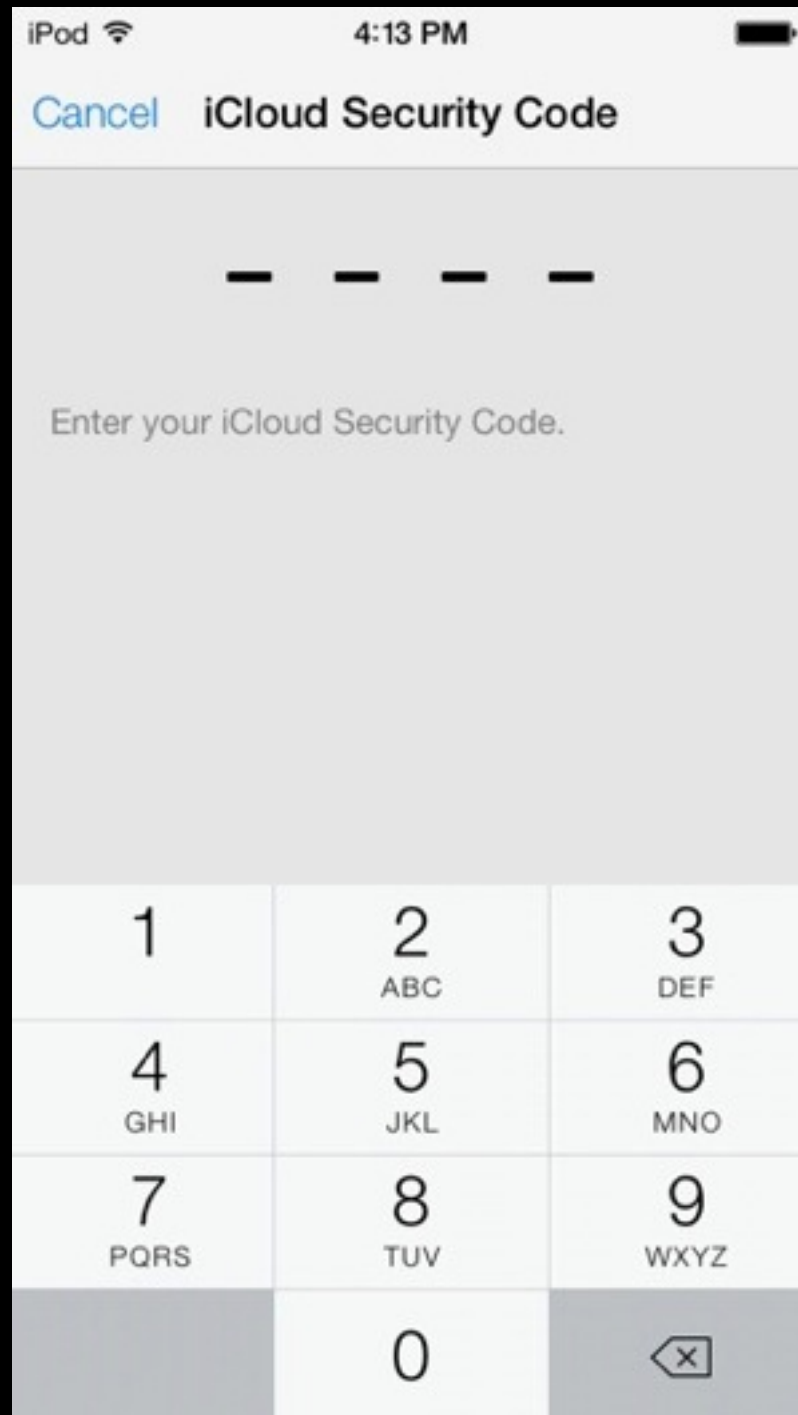
# iCloud keychain





# Apple iOS 7

## iCloud keychain - cont-d





# iCloud keychain setup



# iCloud keychain components

- `com.apple.preferences.icloud.remoteservice`

process that interacts with iCloud control

- `com.apple.sbd`

(daemon) caching and restoring keychain, get notifications  
~/Library/Keychain/keychain-2.db

- `com.apple.lakitu`

(daemon) talks to iCloud (get requests from `com.apple.sbd`, make queries to iCloud, get and decrypt responses, passes them back to `com.apple.sbd`)

- `secd`

(daemon) caching and restoring keychain, get notifications

- `AppleKeyStore.kext`

driver to interact with KVS (key-value storage)

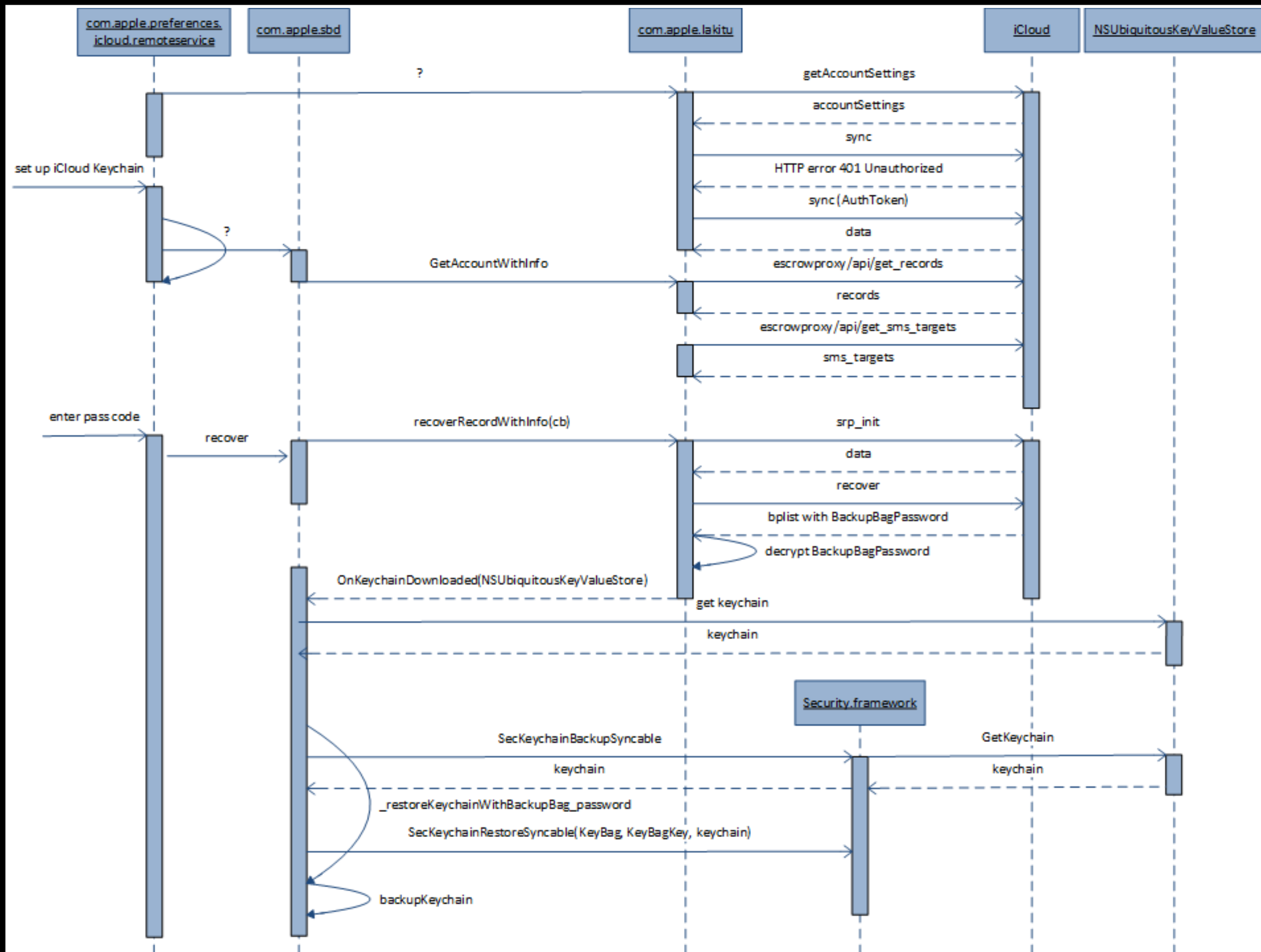
- `Security.framework`

functions to restore keychain, save it to SQLite database, send notifications (e.g. to Keychain access)

- `libcorecrypto.dylib`

encryption/decryption

# Setup iCloud keychain



# Sync (get KeyChain and KeyBag)

Query:

POST <https://p18-keyvalueservice.icloud.com/sync> HTTP/1.1  
Host: [p18-keyvalueservice.icloud.com](https://p18-keyvalueservice.icloud.com)  
uthorization: X-MobileMe-AuthToken MTc3Mzg ... meWRINDg9  
[...]  
<dict>

```
<key>apns-token</key>
<data>
D7wxUEz2av7JaSgJD6j2lyQKENzH0e4DGJzfOeLBbYA=
</data>
<key>apps</key>
<array>
  <dict>
    <key>bundle-id</key>
    <string>com.apple.security.cloudkeychainproxy3</string>
    <key>kvstore-id</key>
    <string>com.apple.security.cloudkeychainproxy3</string>
    <key>registry-version</key>
    <string>FT=-@RU=40c72786-6f77-4190-85d8-3ae1f4df91ca@S=1286</string>
  </dict>
  <dict>
    <key>bundle-id</key>
    <string>com.apple.sbd</string>
    <key>kvstore-id</key>
    <string>com.apple.sbd3</string>
    <key>registry-version</key>
    <string>FT=-@RU=40c72786-6f77-4190-85d8-3ae1f4df91ca@S=1259</string>
  </dict>
</array>
<key>service-id</key>
<string>iOS</string>
```

</dict>

Response:

```
<dict>
  <key>apps</key>
  <array>
    <dict>
      <key>kvstore-id</key>
      <string>com.apple.security.cloudkeychainproxy3</string>
      <key>keys</key>
      <array>
        <dict>
          <key>data</key>
          <data>AYYkF93rOBg ... AABVag==</data>
          <key>name</key>
          <string>com.apple.securebackup.record</string>
        </dict>
      </array>
      <key>bundle-id</key>
      <string>com.apple.sbd</string>
    </dict>
  </array>
  <key>timestamp</key>
  <integer>1384690786479</integer>
</dict>
```

# Get KeyBag key

srp\_init

POST https://p18-escrowproxy.icloud.com:443/escrowproxy/api/srp\_init HTTP/1.1

Host: p18-escrowproxy.icloud.com:443

```
[...]
<dict>
  <key>blob</key>
  <string>dSyhi0M/...CQ==</string>
  <key>command</key>
  <string>SRP_INIT</string>
  <key>label</key>
  <string>com.apple.securebackup.record</string>
  <key>phoneNumberToken</key>
  <string>AQAAAABSidUhUkYydkSNDx8dc4r/QMudn0Q1ctg=</string>
  <key>version</key>
  <integer>1</integer>
</dict>
</plist>
```

HTTP/1.1 200 OK

```
[...]
<plist version="1.0">
  <dict>
    <key>respBlob</key>
    <string>AAABiAAA...638rrzw8=</string>
    <key>dsid</key>
    <string>1773825601</string>
  </dict>
</plist>
```

recover

POST https://p18-escrowproxy.icloud.com:443/escrowproxy/api/recover HTTP/1.1

Host: p18-escrowproxy.icloud.com:443

```
[...]
<dict>
  <key>blob</key>
  <string>AAAAYAAA ... +m8</string>
  <key>command</key>
  <string>RECOVER</string>
  <key>version</key>
  <integer>1</integer>
</dict>
```

Ответ:

HTTP/1.1 200 OK

```
[...]
  <dict>
    <key>respBlob</key>
    <string>AAADKAA...1FHUaEwbQ==</string>
  </dict>
```

# Apple iCloud: Conclusion

- Balance between security, privacy and convenience
- iCloud security risks
- Use additional encryption
- Better 2FA implementation
- Need further work
  - My Photo Stream
  - Photo Sharing
  - 3rd party apps data
  - Back To My Mac
  - Frequent locations
  - Touch ID (iPhone 5S)
  - iCloud keychain

***After all, does Apple (read: NSA) have access to your data? ;)***



# Thank you!

*Vladimir Katalov, ElcomSoft Co. Ltd.  
(twitter: @vkatalov)*

<http://www.elcomsoft.com>  
<http://blog.crackpassword.com>  
Facebook: ElcomSoft  
Twitter: @elcomsoft