Cracking and Analyzing Apple iCloud backups, Find My iPhone, Document Storage

REcon 2013

Oleg Afonin, ElcomSoft Co. Ltd.

The need for iOS forensics

- More than 5 years on the market
- 6 iPhones, 5 iPods, 5 iPads
- 600+ million iOS devices sold worldwide
- “Smart devices” – carry a lot of sensitive data
- Corporate deployments are increasing

iOS data protection

- Device passcode

  Protects unauthorized access to the device

  Bypassing is not enough (used in encryption)

- Disk encryption

  http://images.apple.com/iphone/business/docs/iOS_Security_Oct12.pdf

- Keychain

  System-wide storage for sensitive data (keys, passwords etc.)

- Data is encrypted

iOS forensics

- Logical acquisition (iTunes backups)
- Physical acquisition
- iCloud backups and storage

iOS forensics: Logical Acquisition

- “Ask” the device to produce backup
- Device must be unlocked (by passcode or iTunes)
- Device may produce encrypted backup
- Limited amount of information

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

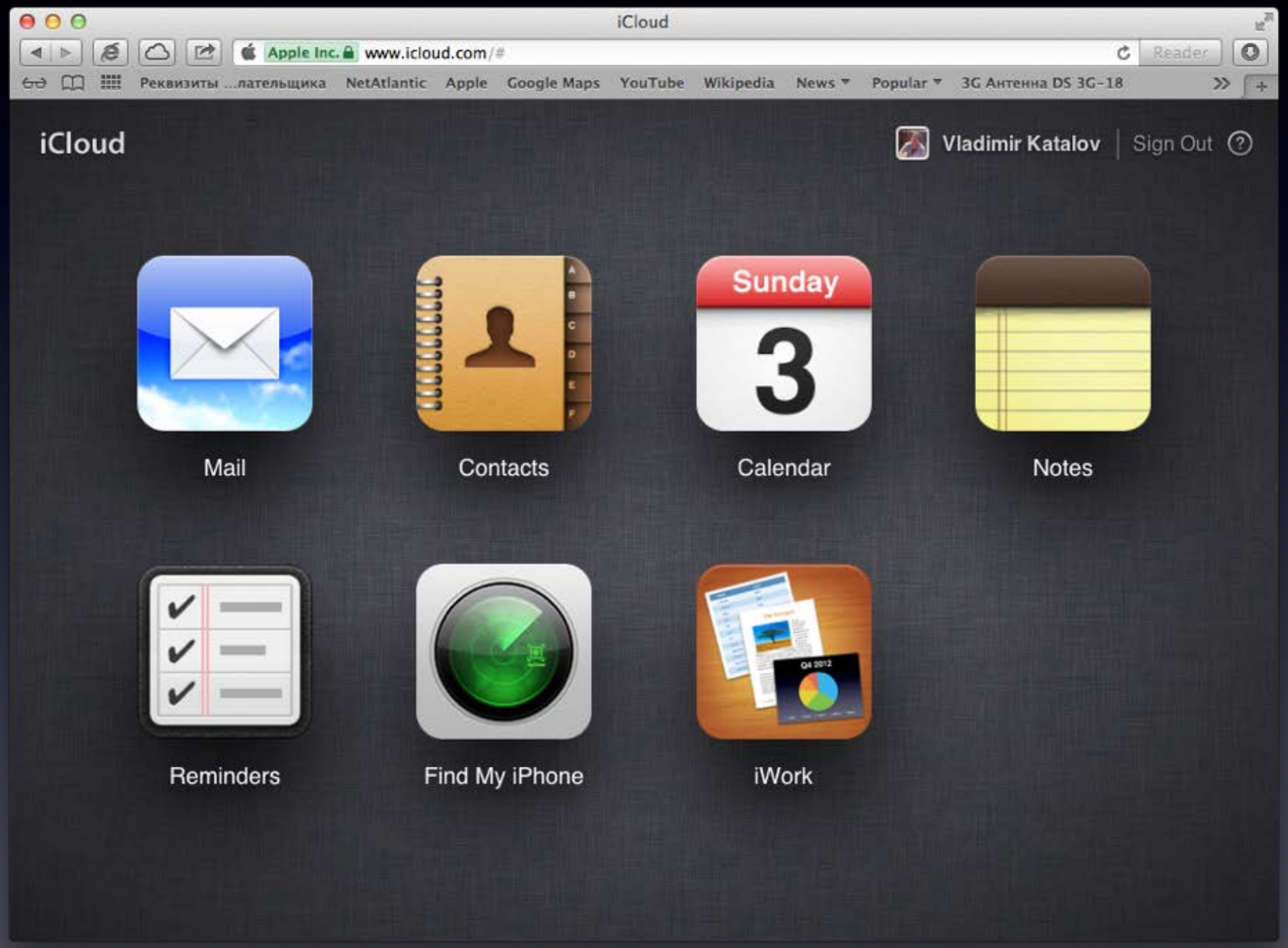
- ... but not for iPhone 4S, 5 or iPad 4 :(

iOS 4+ passcode

iCloud

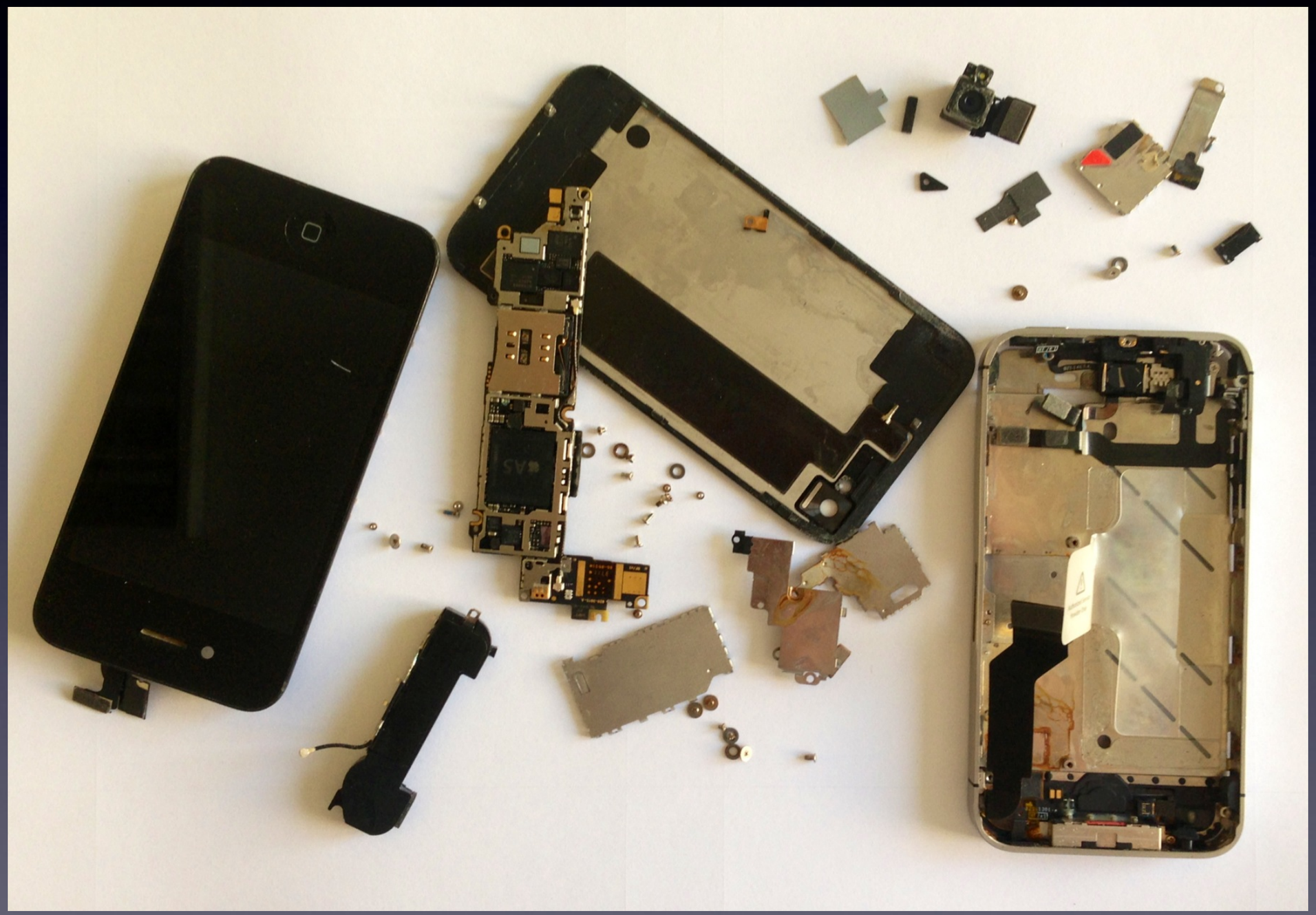
- Introduced in Oct 2011
- Introduced with iOS 5
- 5 GB free storage
- Up to 50 GB paid storage
- Over 300 million users in June 2013
- Backups, documents, notes, calendar, Find My Phone

iCloud services



iCloud Control Panel

iCloud backups: why?



iCloud backup - what

- 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
- Offline web application cache/database
- Safari bookmarks, cookies, history, offline data
- ... and much more

iCloud backup - when

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

iCloud backup - how

Backups

Automatically Back Up

- (•) **iCloud**
  Back up the most important data on your iPhone to iCloud.
- ( ) **This computer**
  A full backup of your iPhone will be stored on this computer.
  - [✓] **Encrypt iPhone backup**
    This will also back up account passwords used on this iPhone.
  - Change Password...

Manually Back Up and Restore

Manually back up your iPhone to this computer or restore a backup stored on this computer.

Back Up Now | Restore Backup...

Last backed up to iCloud: Today 1:52 AM

MTS RUS 18:11 94 %

iCloud **Storage & Backup**

Storage

Total Storage	55,0 GB
Available	48,7 GB
Manage Storage	›

Change Storage Plan

Backup

iCloud Backup	ON

Automatically back up your camera roll, accounts, documents and settings when this iPhone is plugged in, locked and connected to Wi-Fi.

Back Up Now

iCloud CP: backups

Reverse-engineering iCloud backups

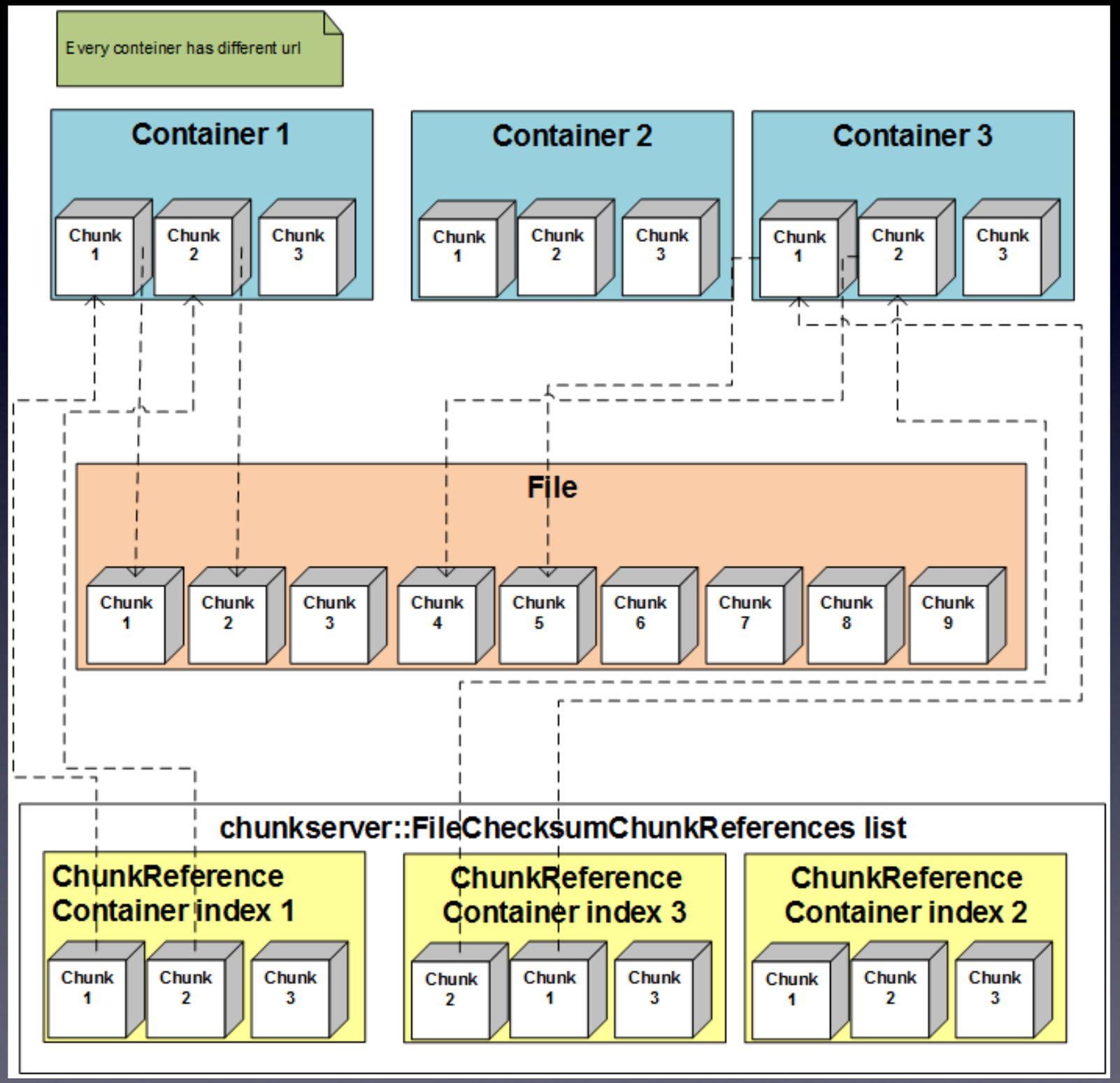
- jailbreak iPhone
- Install Open SSH, get keychain (keychain-2.db)
- [Settings] | [iCloud] | [Delete Account] | [Delete from My iPhone]
- [Settings] | [General] | [Reset] | [Reset All Settings]
- reboot
- set up Wi-Fi connection (proxy)
- replace keychain with our own trusted root certificate (need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

  key835 = AES(UID, bytes("01010101010101010101010101010101"))

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/$APPLE_ID$,

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 cXR0LnRld3RAaWNtb3VkLmNvbTqRd2VydHkxMjM0NQ==

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

query:
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)
Authorization: <authentication data>
authentication data = mime64 (dsPrsID:mmeAuthToken)
returns: list of backup IDs (backupudid)

query:
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)

Get file authentication tokens

HTTPS POST
https://p11-mobilebackup.icloud.com/mbs/(dsPrsID)/(backupudid)/(snapshotid)/getFiles

Get URLs for file chunks

HTTPS POST
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=0EdHy75gGHCee%2BjKePZBqz8xbWxpTxaYyASwFXVx2%2Fg%3D

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

Amazon AWS:
http://us-std-00001.s3-external-1.amazonaws.com/l9rh20QBPX4jizMAr3vY?x-client-request-id=739A222D-0FF5-44DD-A8FF-2A0EB6F49816&Expires=1371208272&byte-range=25556011-255562262&AWSAccessKeyId=AKIAIWWR33ECHKPC2LUA&Signature=PxAdegw0PLyBn7GWZCnu0bhi3Xo%3D

iCloud encryption

- Data stored at 3rd-party storage providers is encrypted
- Apple has encryption keys to that data
- Some files are further encrypted using keys from OTA (over-the-air) 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. legal enforcement)

iCloud protocol changes
(March 2013)

Added:

X-Apple-MBS-Protocol-Version: 1.7

Accept: application/vnd.com.apple.mbs+protobuf

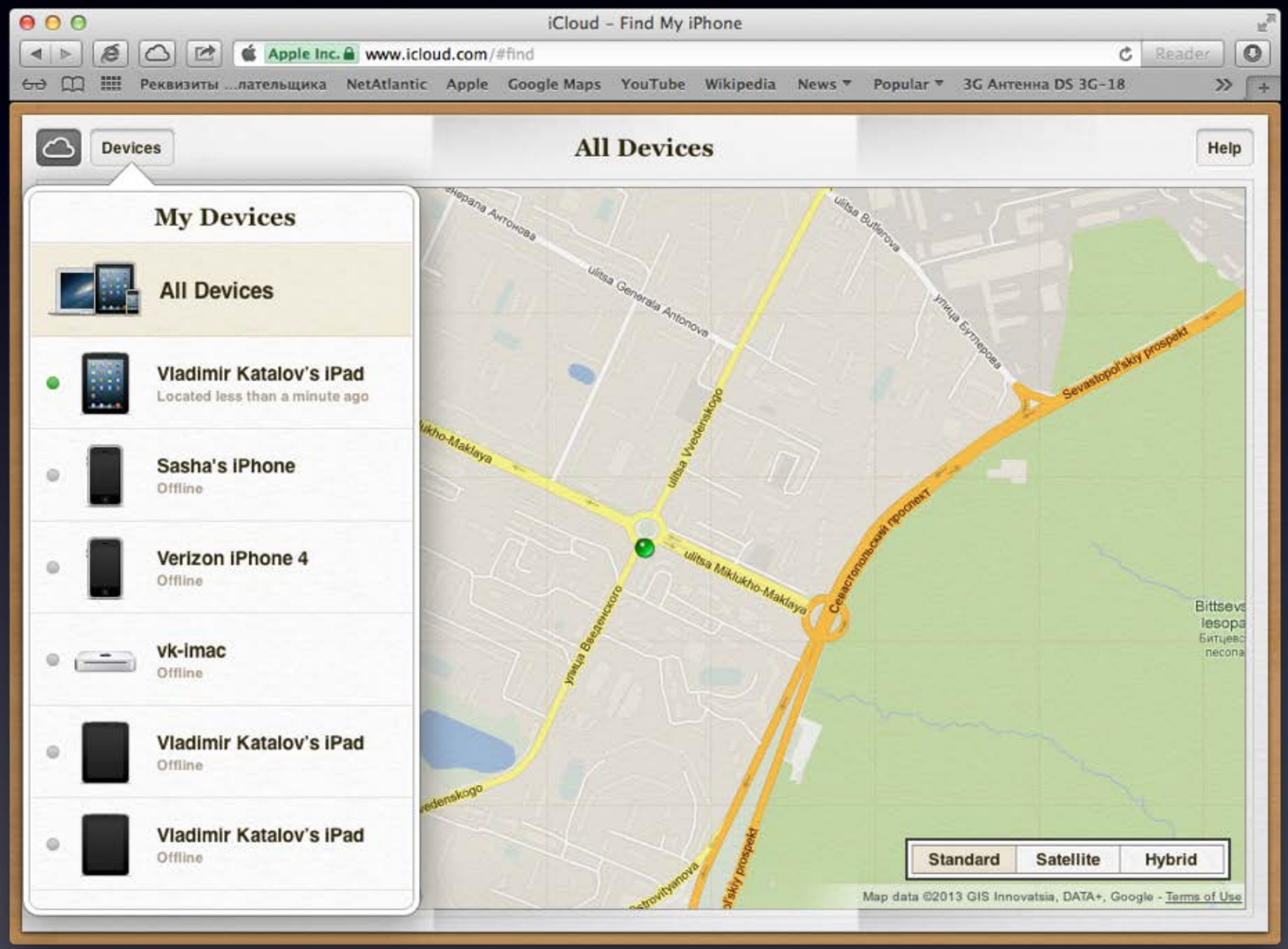
X-Apple-Request-UUID: 4EFFF273-5611-479B-A945-04DA0A0F2C3A

Changed:

X-MMe-Client-Info: <iPhone4,1> <iPhone OS;5.1.1;9B206> <com.apple.AppleAccount/1.0 (com.apple.backupd/(null))>

User-Agent: MobileBackup/5.1.1 (9B206; iPhone4,1)

Find My Phone



FindMyPhone protocol

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

Authorization:

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)

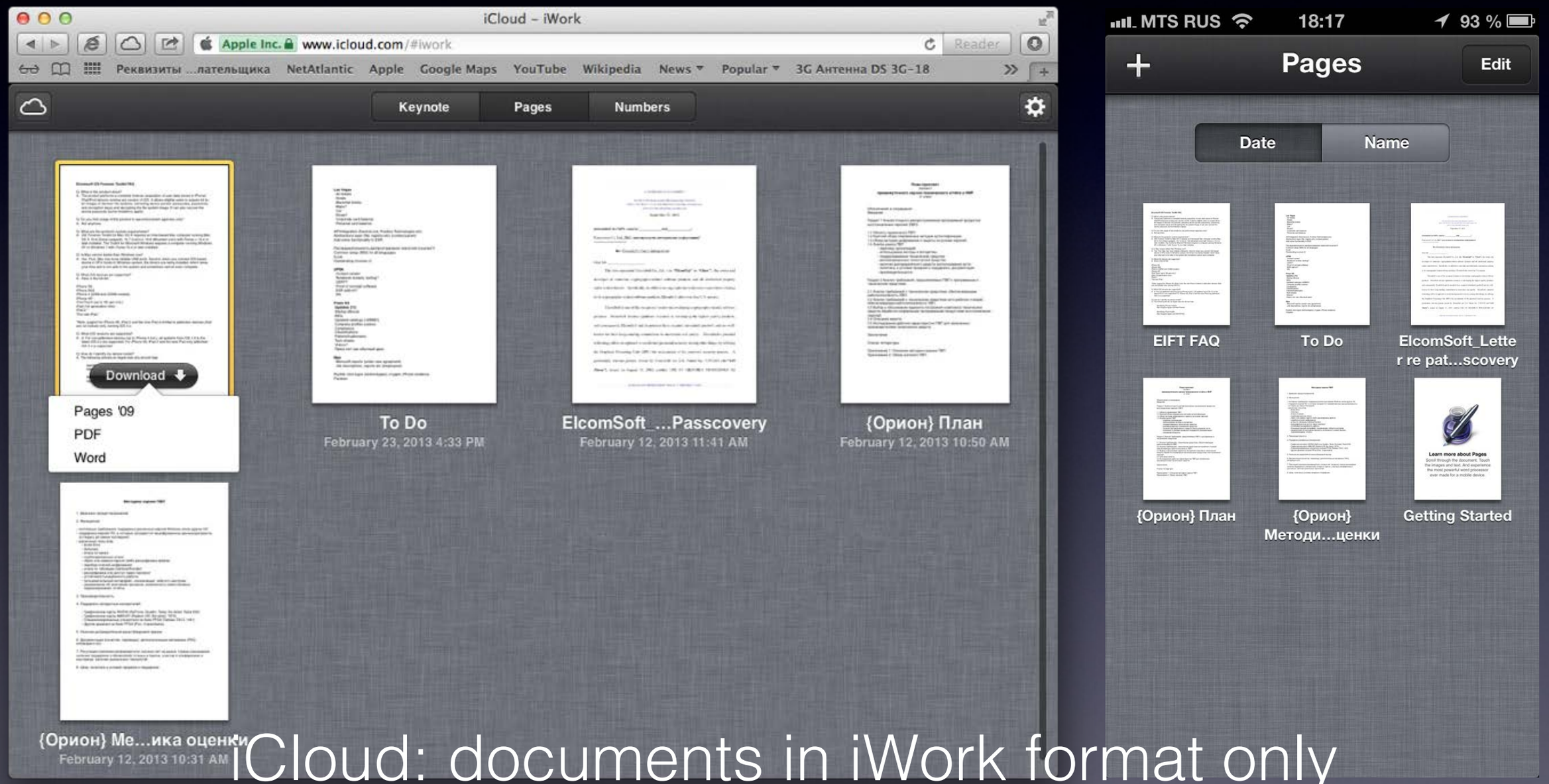
- Requesting location via Find My Phone makes push request to the iOS device if Find My Phone and Location Services are enabled
- Constant location requests quickly drain iPhone battery, device heats up, can be noticed
- Location information stored for 3 hours

FindMyPhone - demo output

locations.txt — Edited

```
====================== Device #1====================
deviceModel = SixthGen-white
modelDisplayName = iPhone
id = QVBTOmIwMjZiMDY5ODg5NDA2MTcwMDhjOWY4MWRkOWU2YWIxM2UwN2JiY2M~
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 = QVBTOjg3MzBFNjQ5LTdGRjktNTkzRC1CMzI3LUZCMkRFNjA2NjRCRA~~
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 = QVBTOjAzYjU2YzhiMjYzZWFhZmE3NWU2MTk5YzQzYzQwNDJjYTljNjRkZjg~
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
```

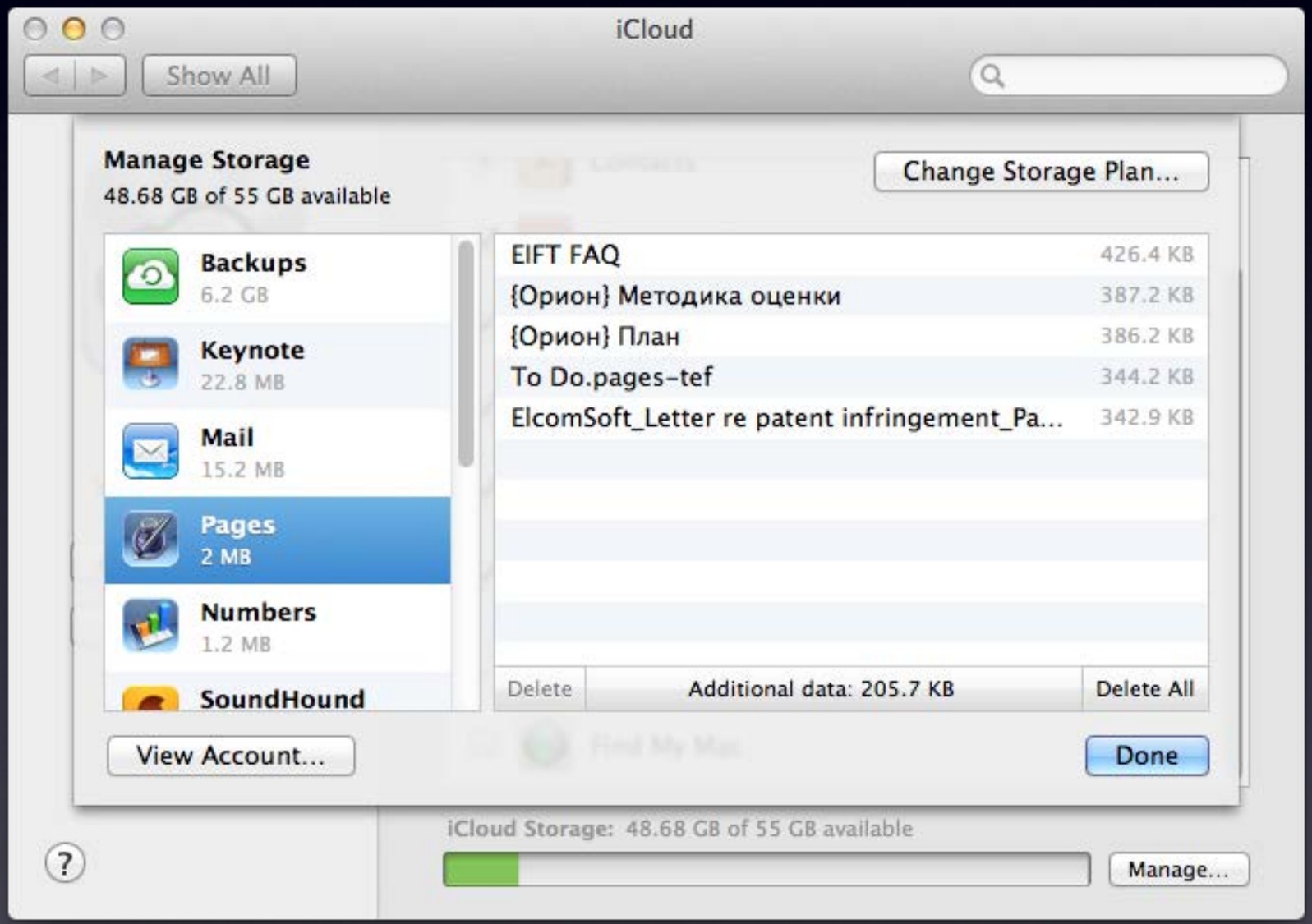
iCloud documents



iCloud: documents in iWork format only

EPBB: all formats

iCloud CP: 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 a given file

- Request to get a 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)

Many documents are stored as packages

Storage: plist + content (text, media files)

Reguests:

- 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?...
- 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?

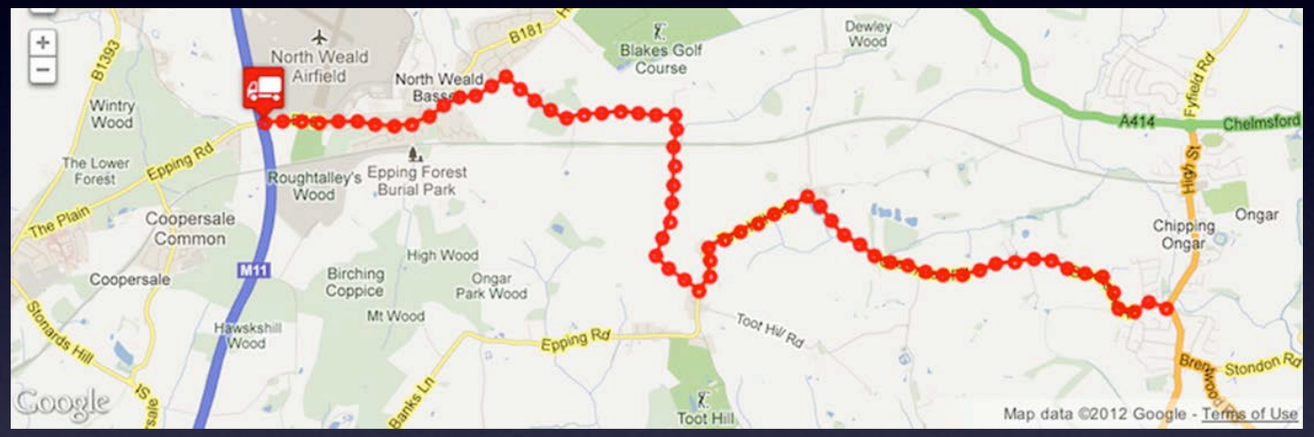
iCloud docs: demo output

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
```

Possible usage

- Backups in iCloud
  - near-realtime acquisition (SMS, iMessage, mail, call logs)
  - browse backup data without actual device
  - download only data of specific type
- Find My Phone
  - keep track
  - using Google Maps (or whatever)
  - track enter/leave pre-defined area
  - 2+ devices simultaneously (meeting alert)
- Documents in iCloud
  - open from 3rd party apps
  - track changes
  - download unsupported document data
- **Forensics!**

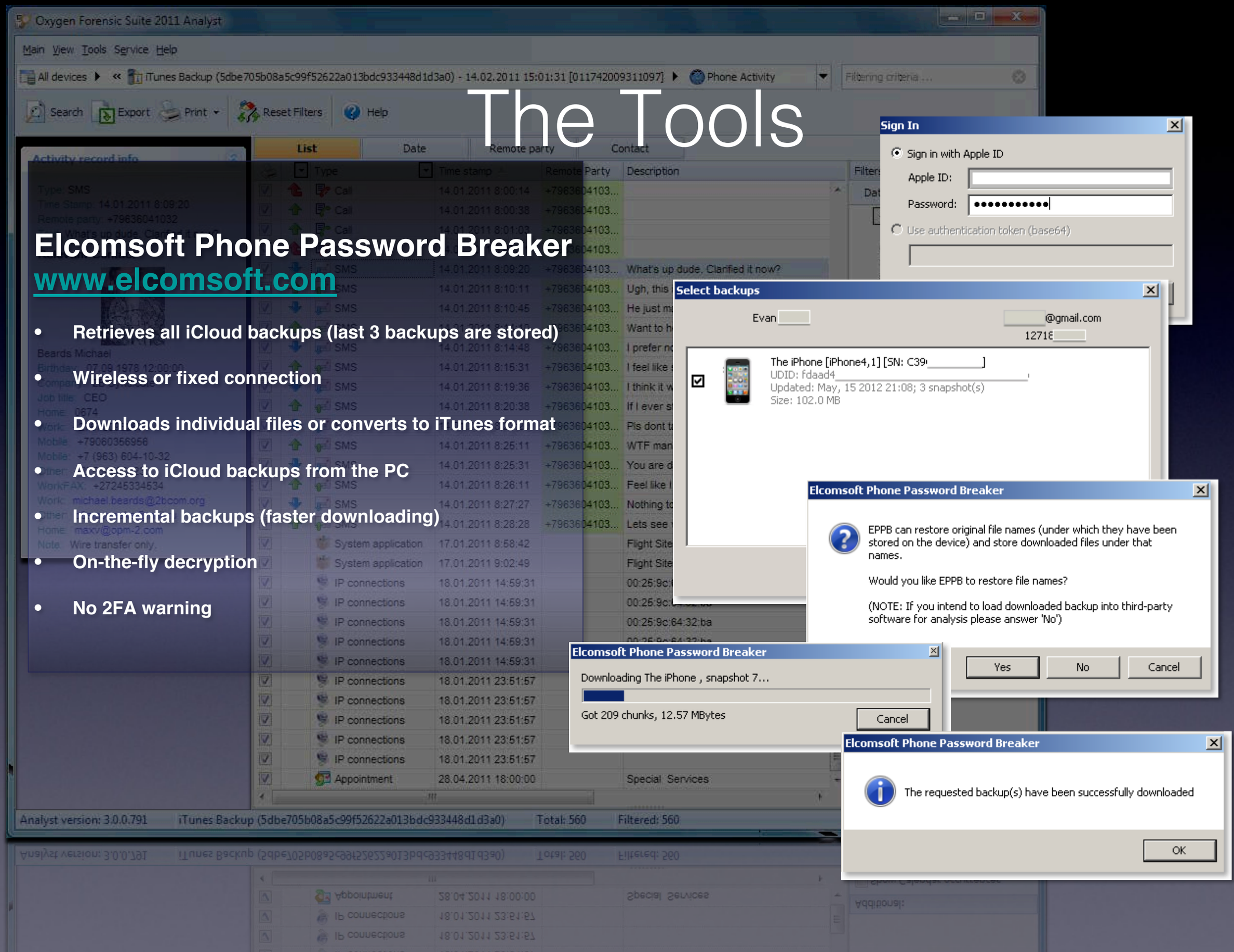


The Tools

Elcomsoft Phone Password Breaker

www.elcomsoft.com

- Retrieves all iCloud backups (last 3 backups are stored)
- Wireless or fixed connection
- Downloads individual files or converts to iTunes format
- Access to iCloud backups from the PC
- Incremental backups (faster downloading)
- On-the-fly decryption
- No 2FA warning



Oxygen Forensic Suite
www.oxygen-forensic.com

- **Comprehensive forensic analysis**
- **Built-in and third-party applications**
- **Deleted data analysis (from application databases)**
- **Calls, messages, contacts, event log, tasks, GPS locations**
- **Timeline: all user and system activities in a single view**
- **Communication circles**
- **Multiple devices analysis**
  investigates interactions among users of multiple mobile devices

Apple 2FA

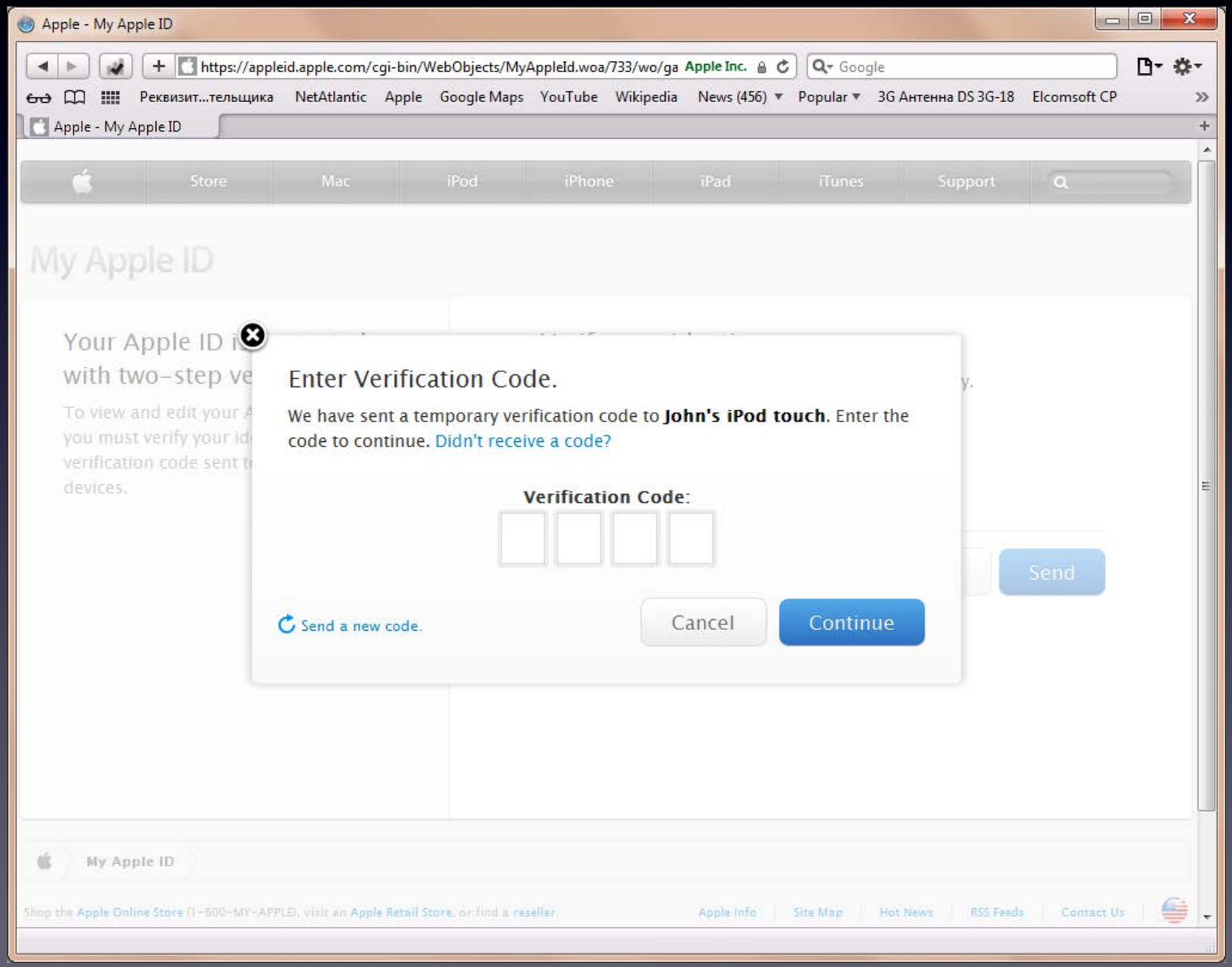
Requires to verify your identity using one of your devices before you can:

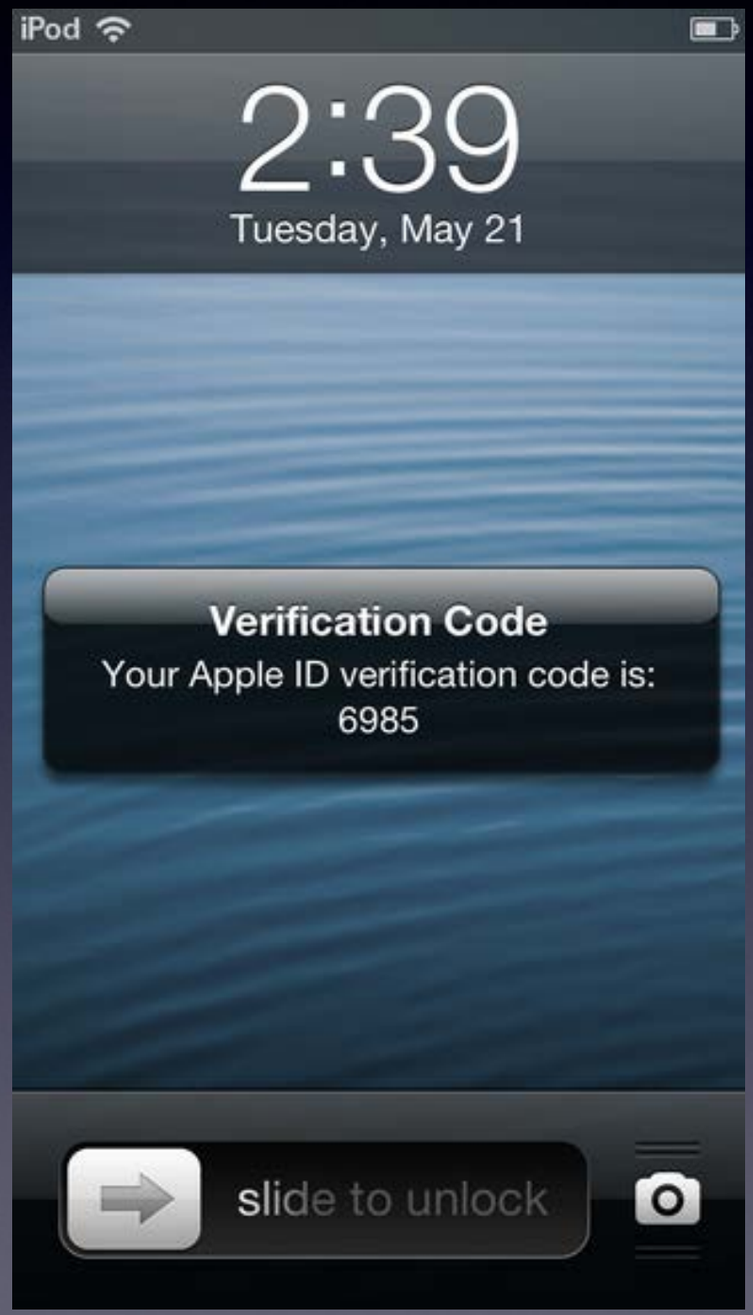
- Sign in to My Apple ID to manage your account.
- Make an iTunes, App Store, or iBookstore purchase from a new device.
- Get Apple ID-related support from Apple.

Does NOT protect:

- iCloud backups (could it ever?)
- Find My Phone data (the only authorized device stolen?)
- Documents stored in the cloud
- iCloud backups restored onto a new iOS device = email from Apple
- iCloud backups retrieved with EPPB = no email

Apple 2FA
(Two-step Verification)





Apple iOS 7 what's new

Disabling location services in iOS7 now requires Apple ID password
(better chances of finding stolen devices)

Keychain can be synced between Max OS X and iOS

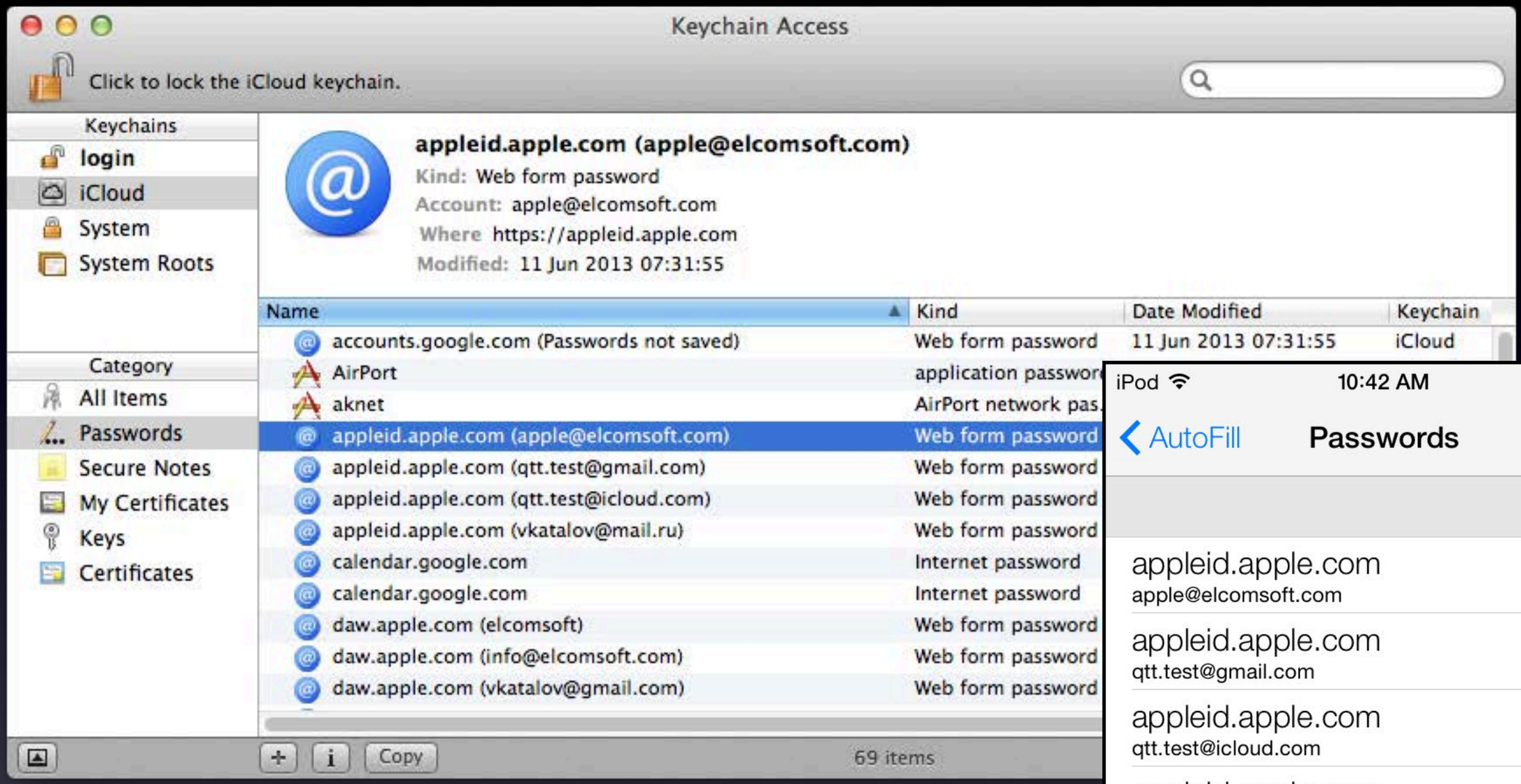
Keychain can be stored in iCloud, requires separate password

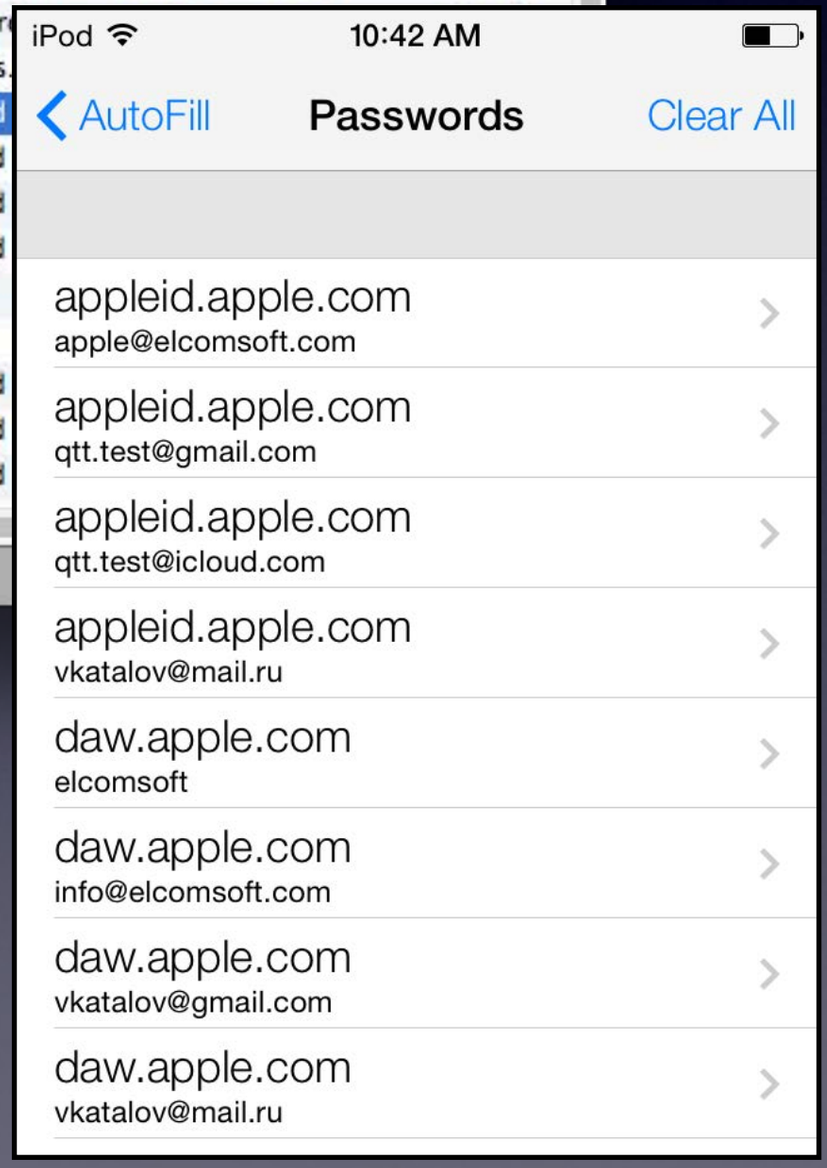
Icons Downright Ugly

Apple iOS 7

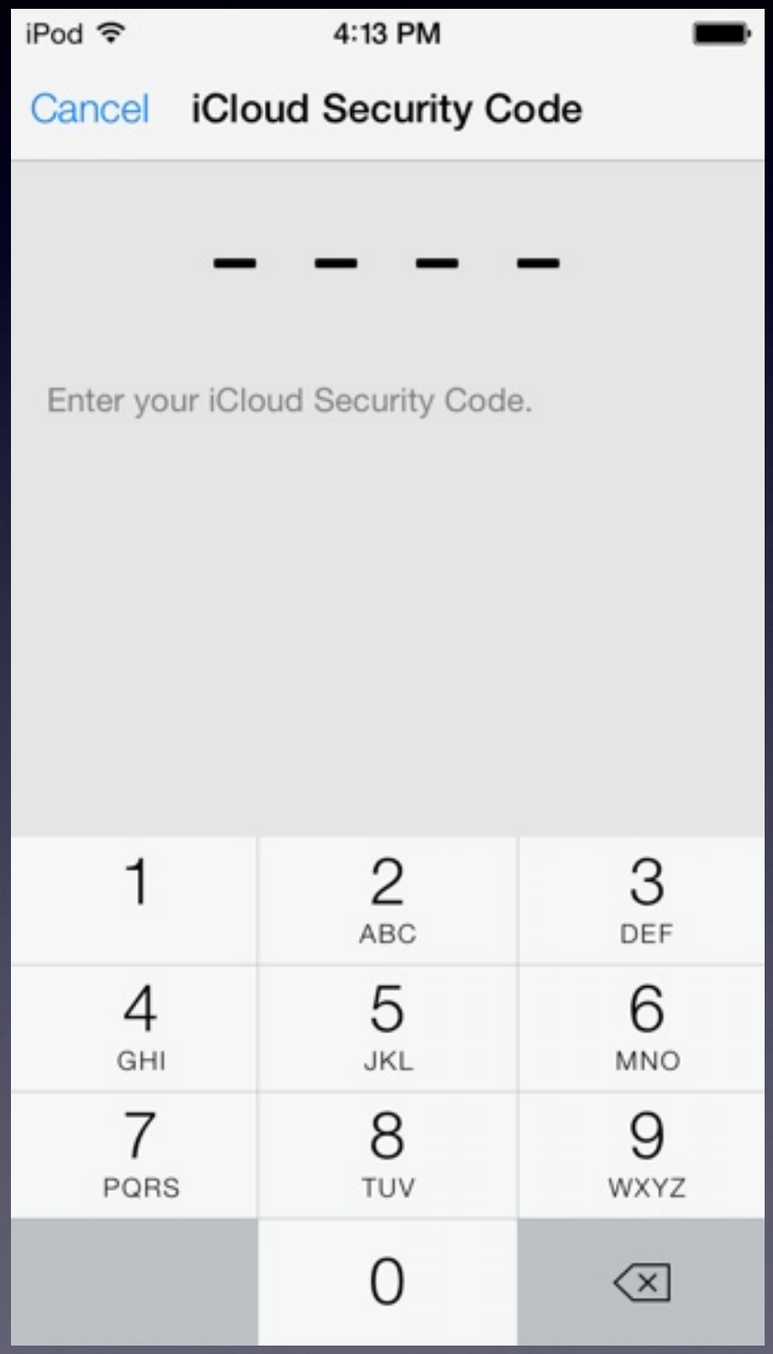
iCloud
Show All
Create an iCloud Security Code.
This code is used to protect your password when restoring them to a new device.
Enter a 4-digit Security Code
More Recovery Options
Cancel
Back
Account Details
Sign Out
Documents & Data
Back to My Mac
Find My Mac
iCloud Storage: 46,45 GB of 55 GB available
Create Security Code
Write down your Security Code and keep it in a safe place. Apple cannot replace a lost Security Code.
Create Random Code
Disable Keychain Recovery
Next
Options...
Manage...

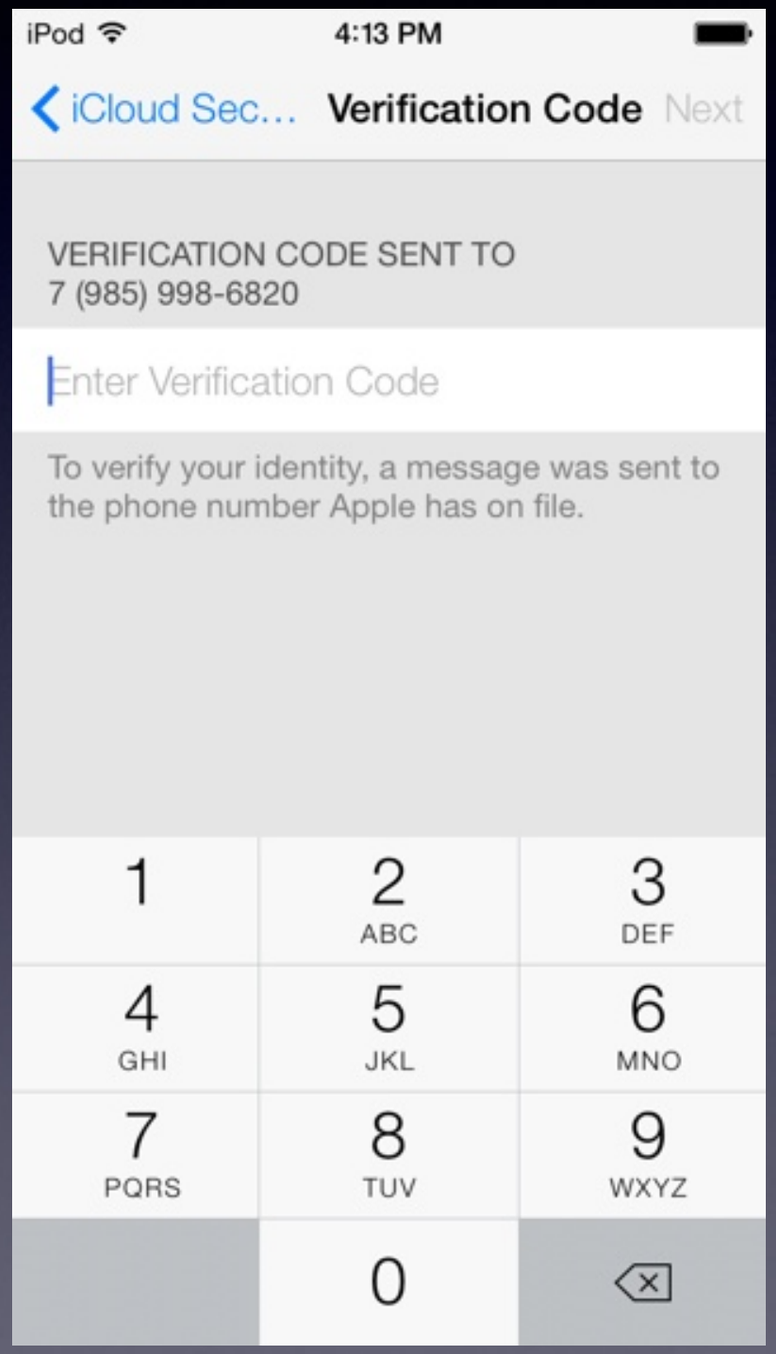
iCloud keychain





iCloud keychain - cont-d





Conclusion

- Balance between security, privacy and convenience
- iCloud security risks
- Use additional encryption
- Better 2FA implementation
- Need further work (photo streams, 3rd party apps data: 1Password etc)

Windows Phone backups

What is saved:

- Internet Explorer Favorites
- List of installed apps
- Theme and accent configuration
- Call history
- App settings (where applicable - email and accounts, lock screen etc)
- Test messages (SMS conversations)
- Photos (good quality - uses data allowance)

Can get with LiveSDK:

- Basic user information
- Contacts
- Calendars
- Files, photos, videos, documents

Download full backup?

Thank you!

Cracking and Analyzing Apple iCloud backups, Find My iPhone, Document Storage

REcon 2013

Oleg Afonin, ElcomSoft Co. Ltd.

http://www.elcomsoft.com

http://blog.crackpassword.com

Facebook: ElcomSoft

Twitter: @elcomsoft