iCloud Keychain Forensics

Introduction to iCloud Keychain

forensic.nofate.com

Contents

- Introduction
- Keychain Management
- How to operate iCloud Keychain
- What to do with forensic analysis
- Conclusion

WWDC 2013

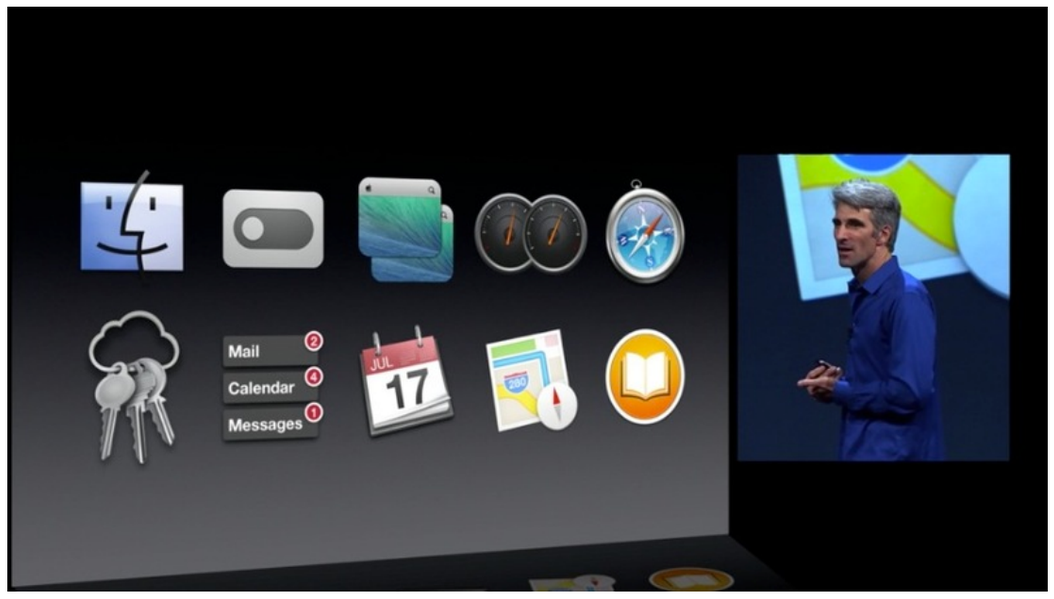

WWDC
MMXIII
wallpaper design by Dhanush R Parekh
Digital Origami
www.facebook.com/DigitalOrigami

OS X Mavericks

- Apple inc's desktop and server OS for Mac
- tenth major release of OS X.
  - in beta now
  - is scheduled for a release in Q3 - Q4

OS X Mavericks

- Emphasis on battery life
  - App Nap
- various application enhancements
- Added new iBooks, Maps applications
- iCloud keychain sync
- Linkedin sharing integration

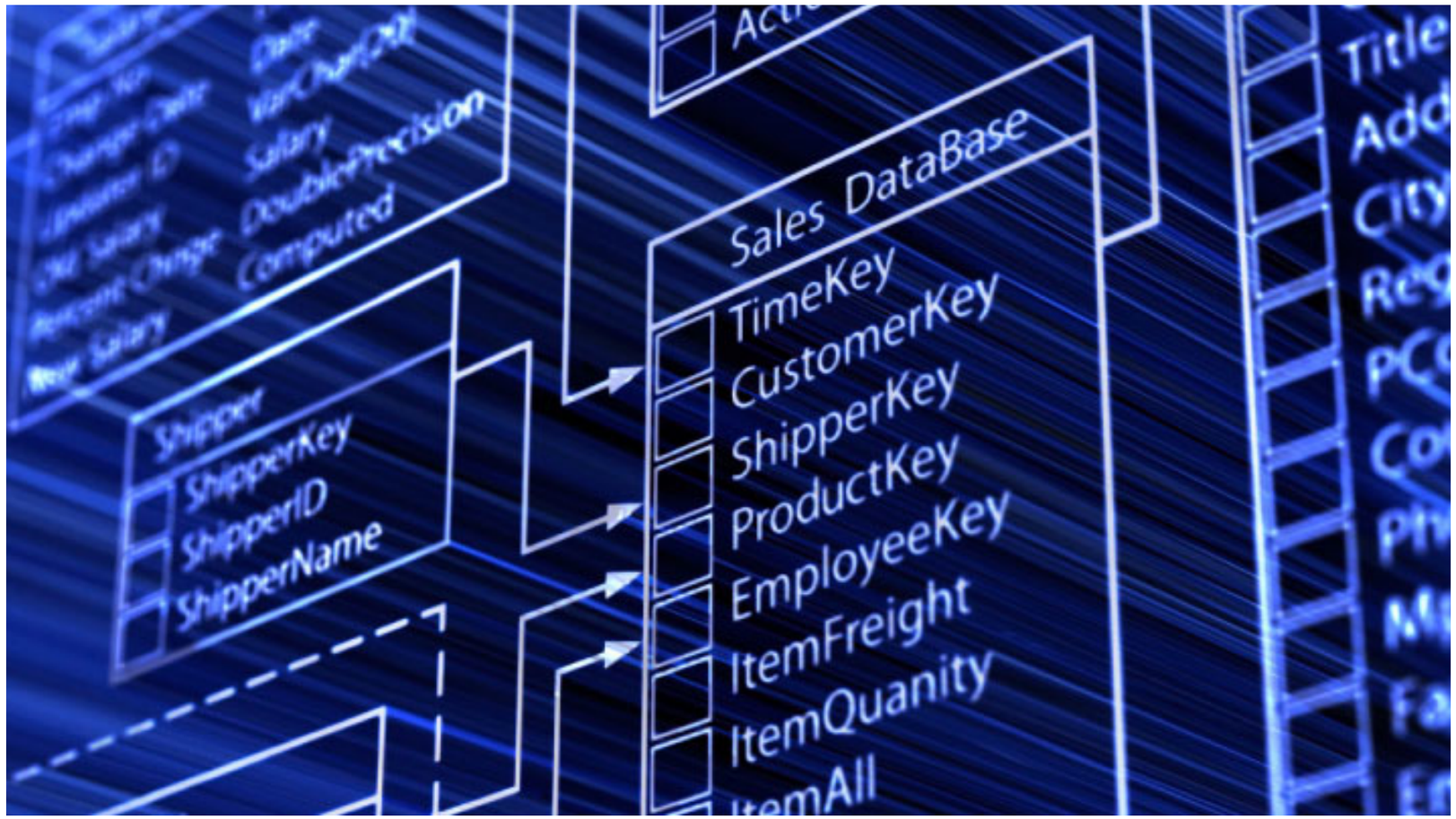


iCloud Keychain

- secure database that allows information
- 256-bit AES encryption
- stored on device and pushed from iCloud between devices
- only available on a users trusted devices
- suggest new passwords to the user

iCloud Keychain

- Website login
- Wi-Fi network
- Credit card
- Account data

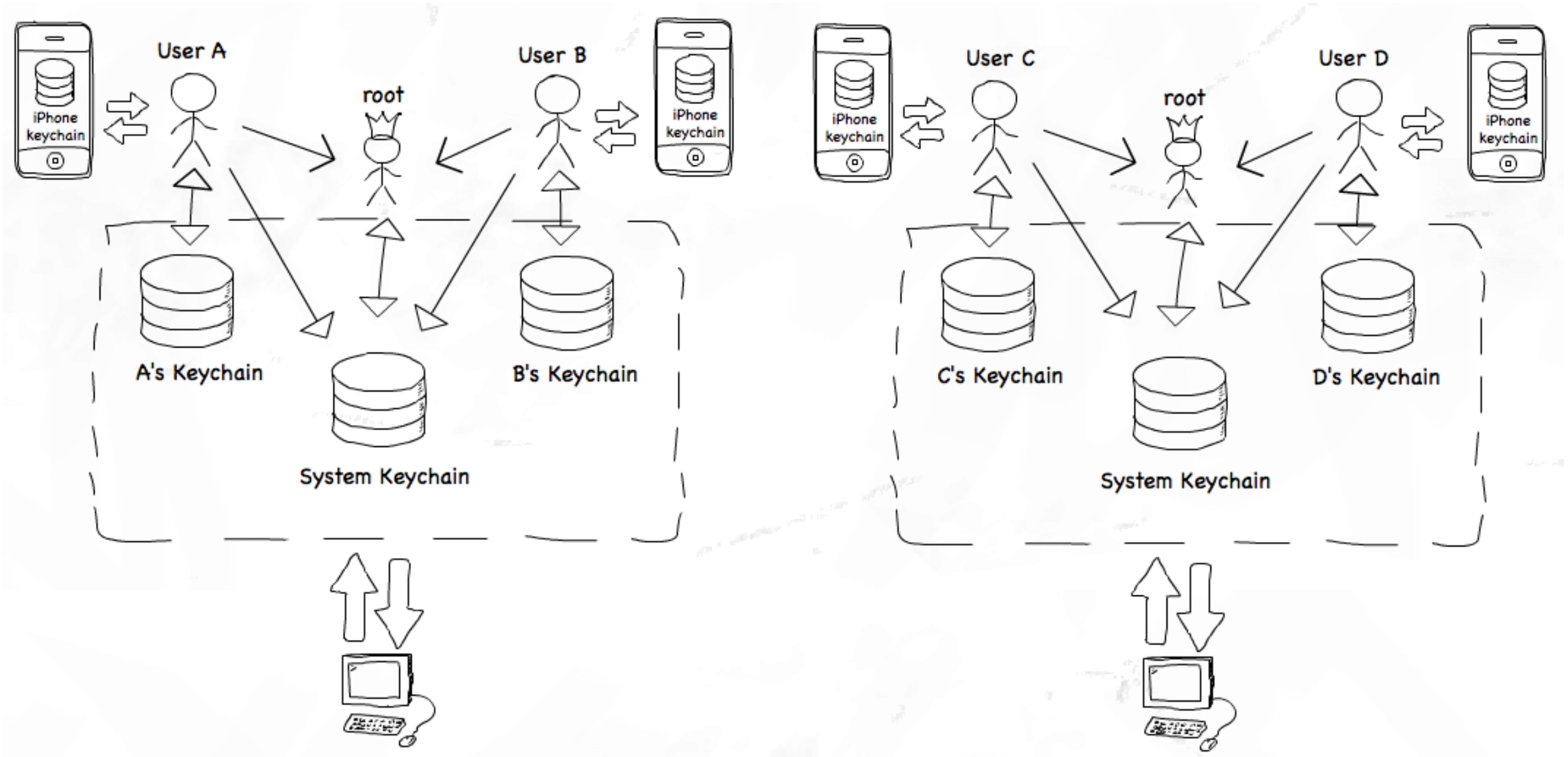


http://www.mmts.com.au/Content/images/misc/head-4.jpg

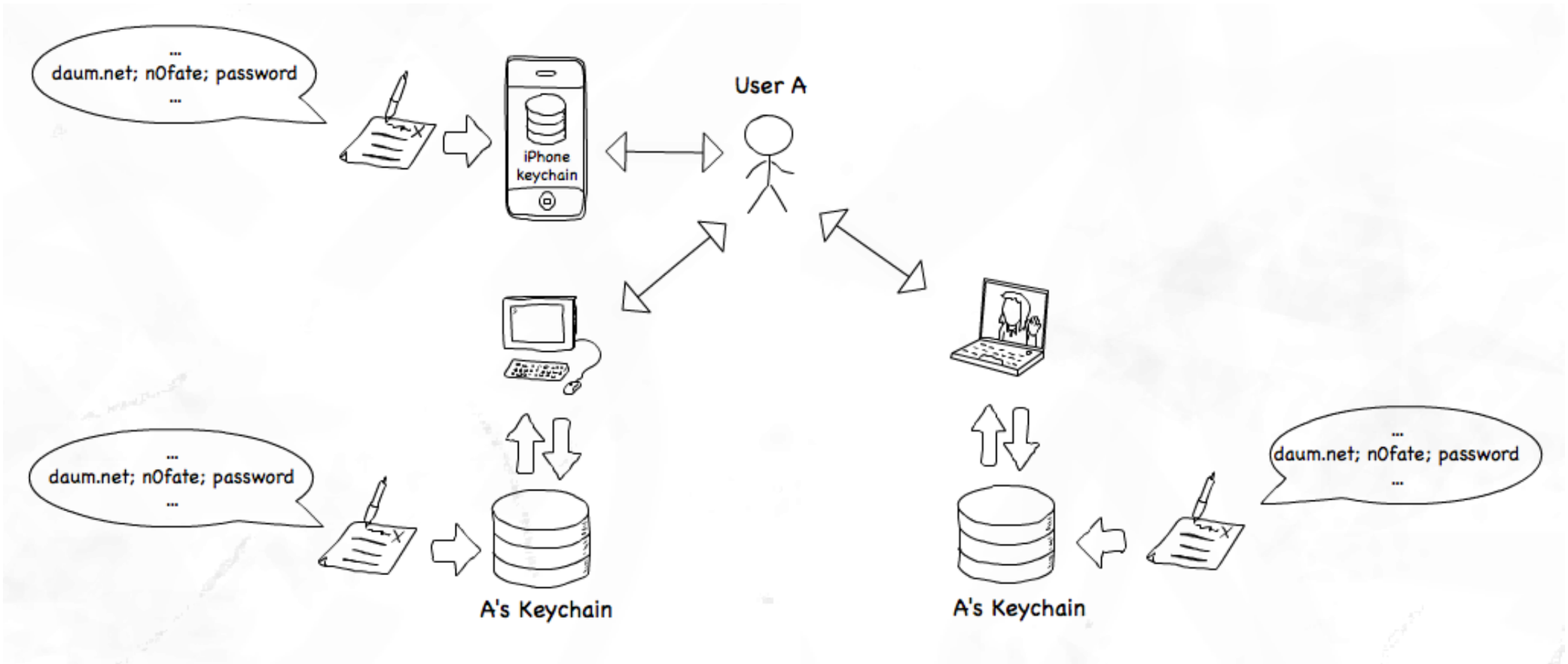
Keychain Management

forensicinsight.org

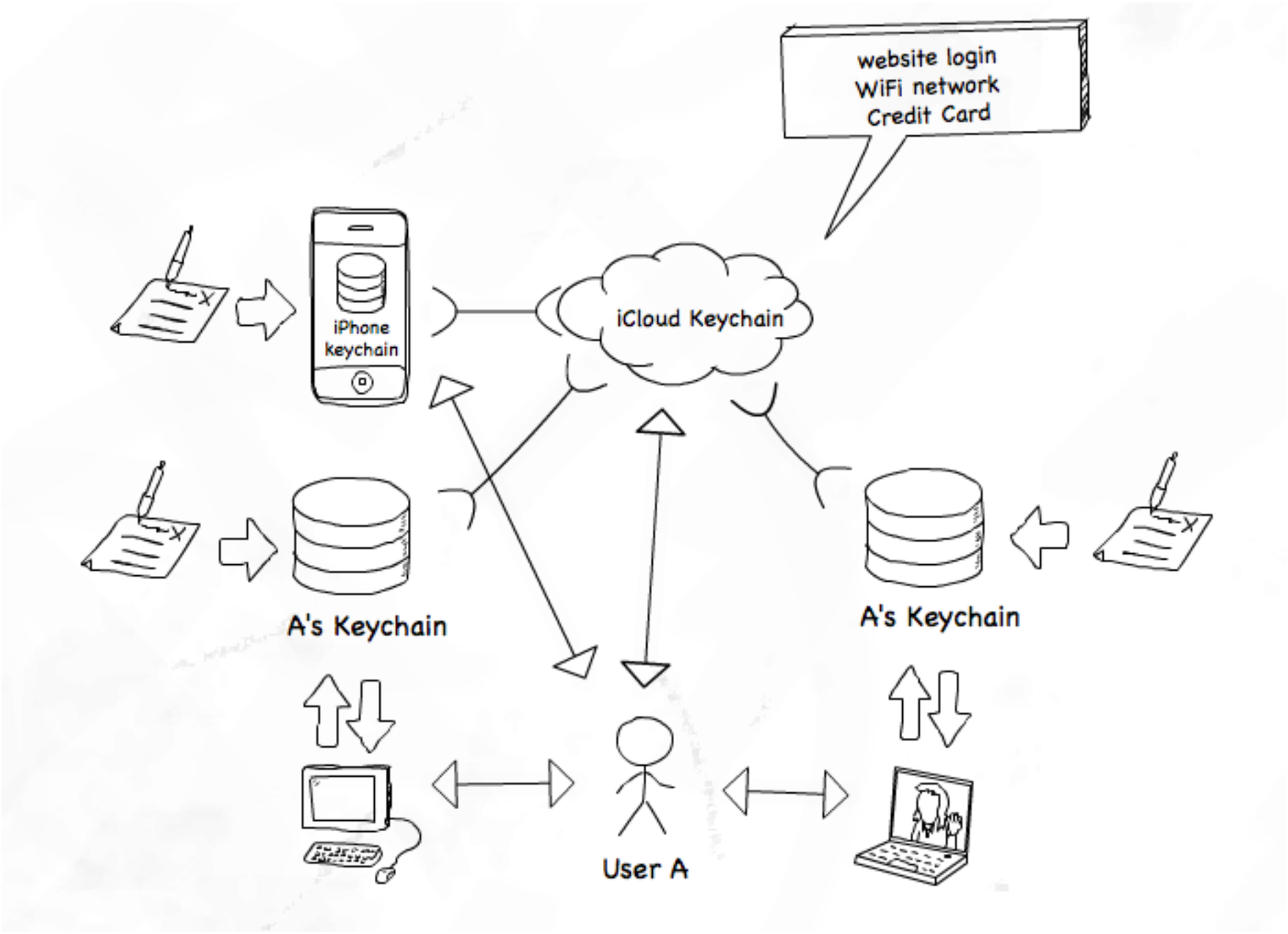
Keychain Management



Keychain Management



iCloud Keychain

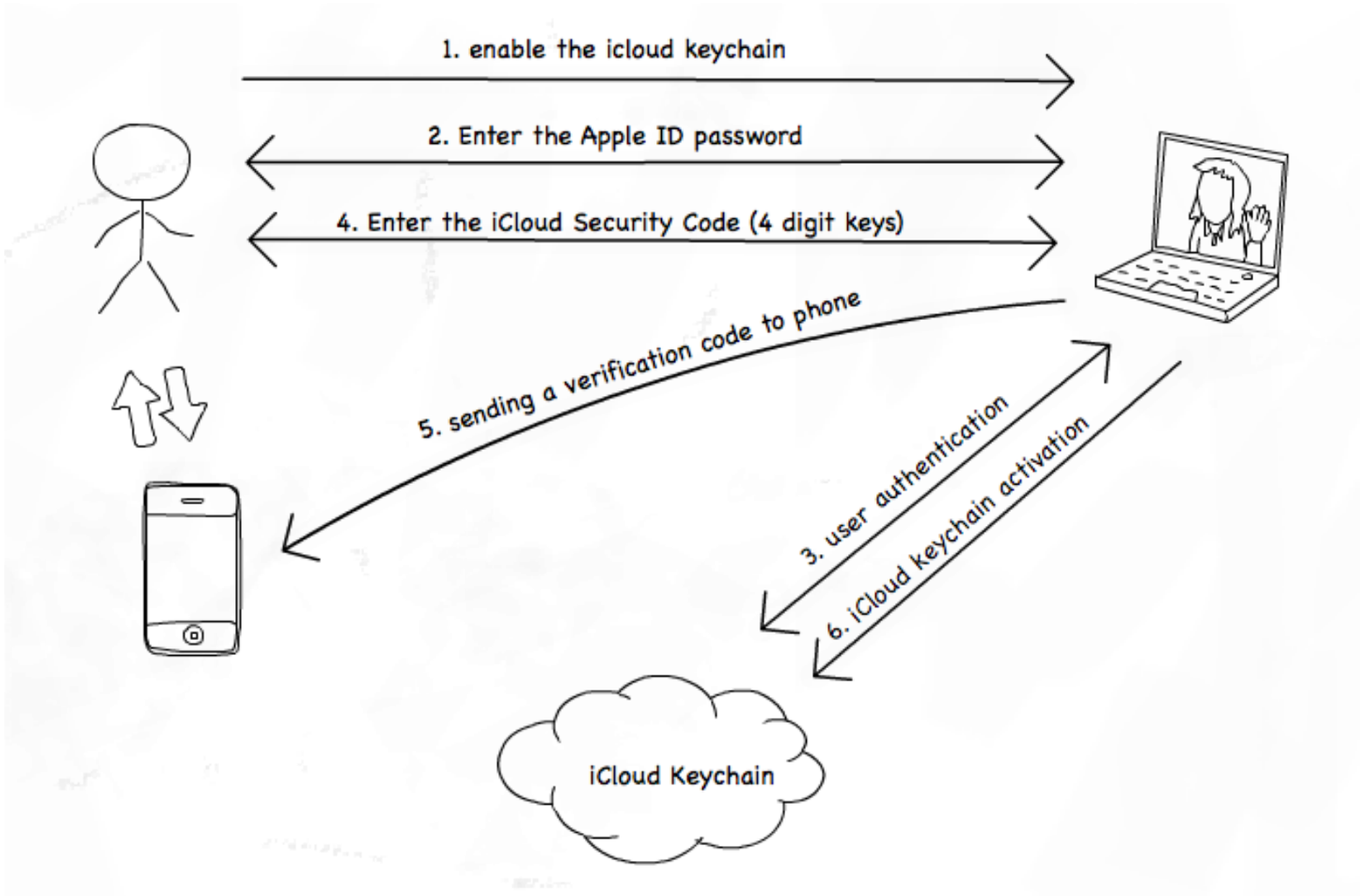


http://img1.mxstatic.com/wallpapers/2259dd4bc3feca7ad64e6c63ed41f155_large.jpeg

How to operate iCloud Keychain

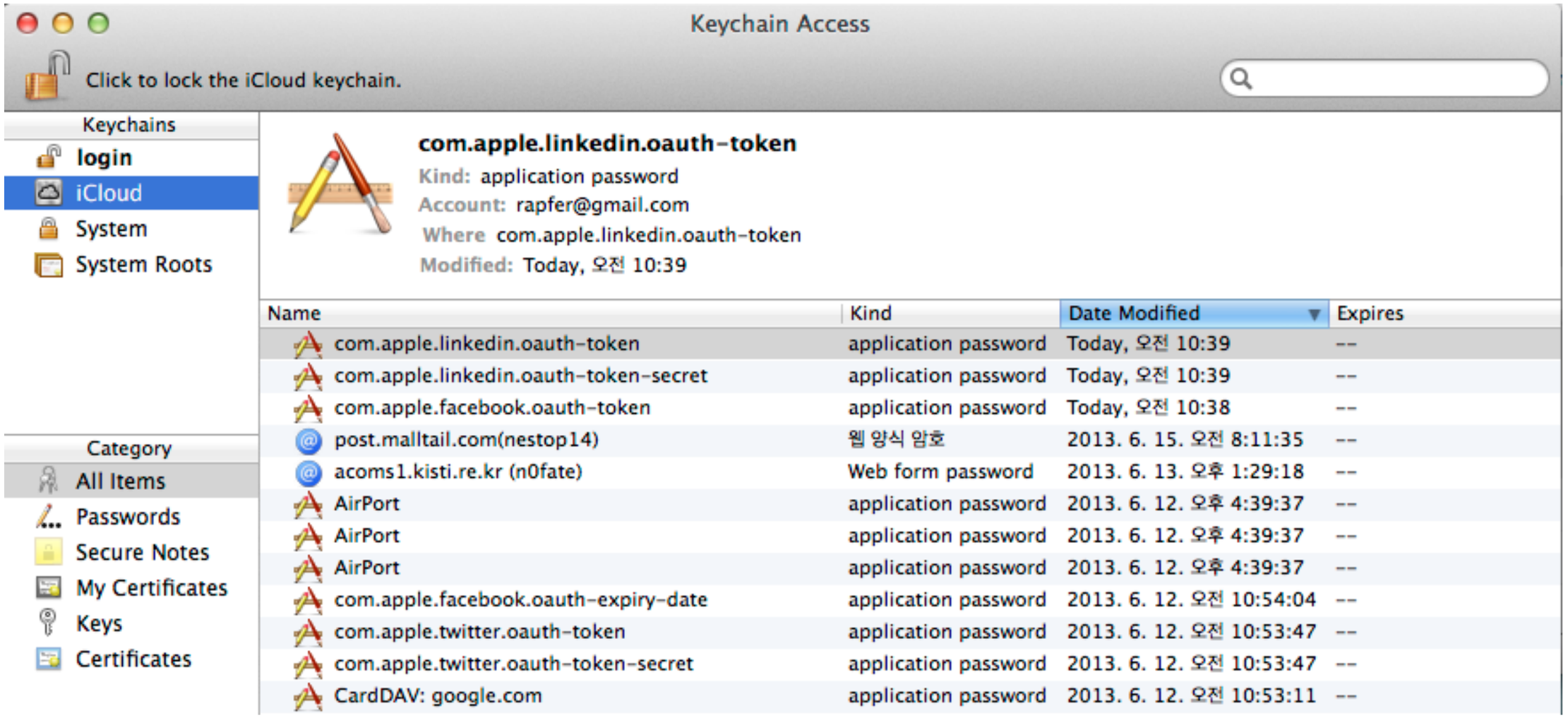
forensicinsight.org

Synchronization

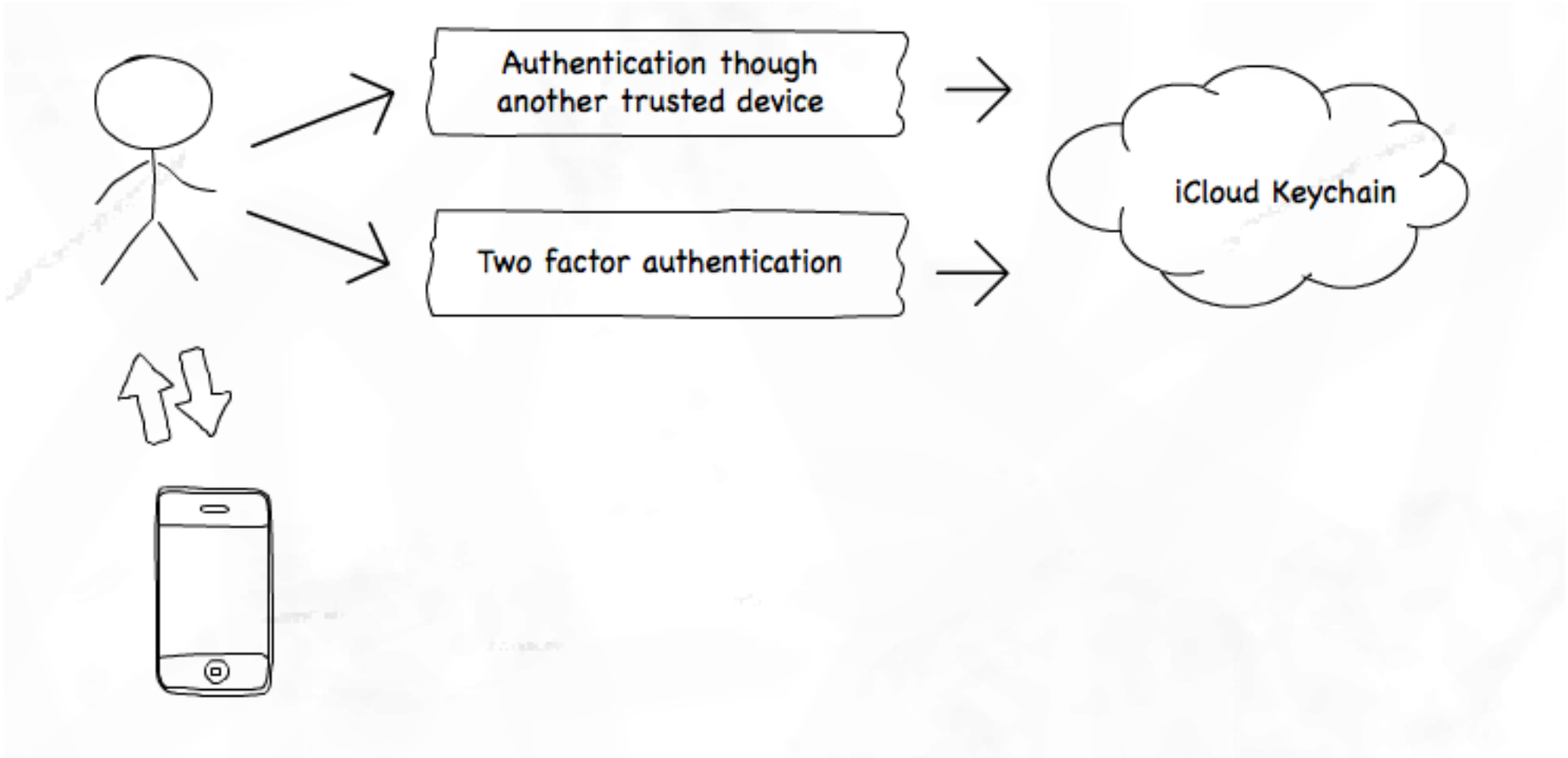


- Initialization : Two-factor authentication

Synchronization

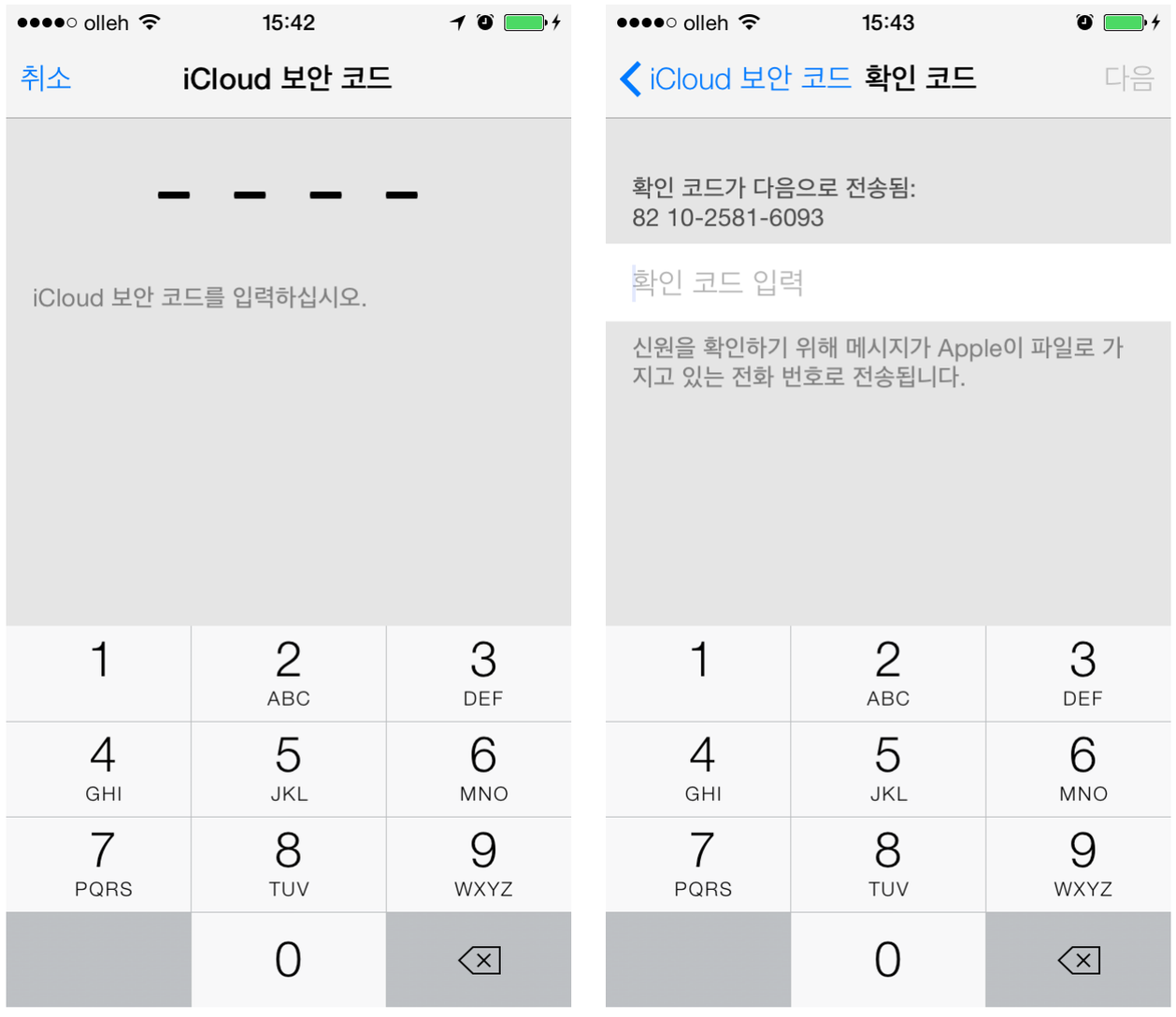


Synchronization

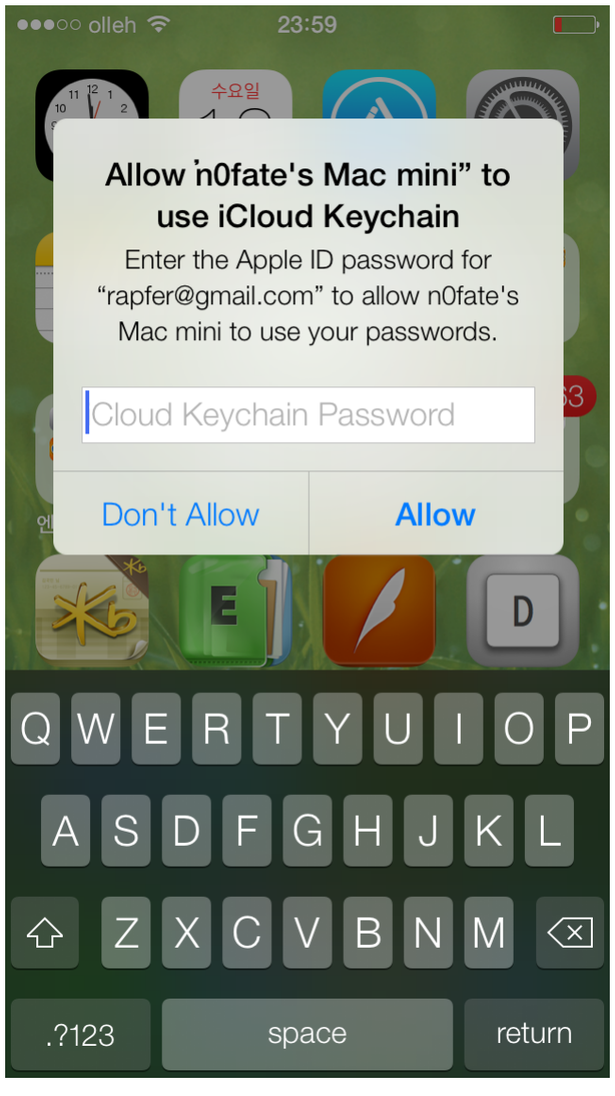


- connecting new device (e.g. iPhone)

Synchronization



Two factor authentication



Auth though trusted device

forensicinsight.org

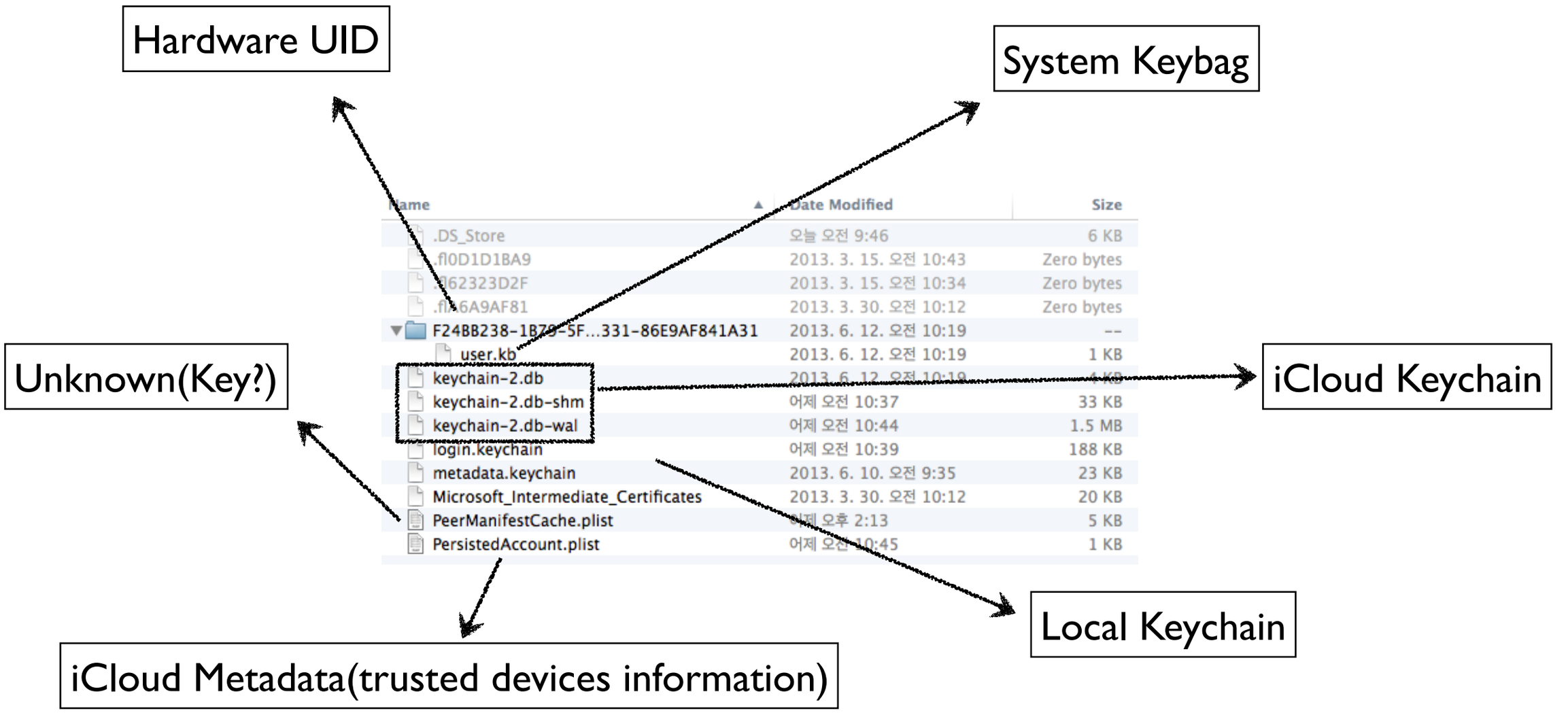
http://www.sapphire.net/images/uploaded/6Sapphire09.jpg

What to do with forensic analysis

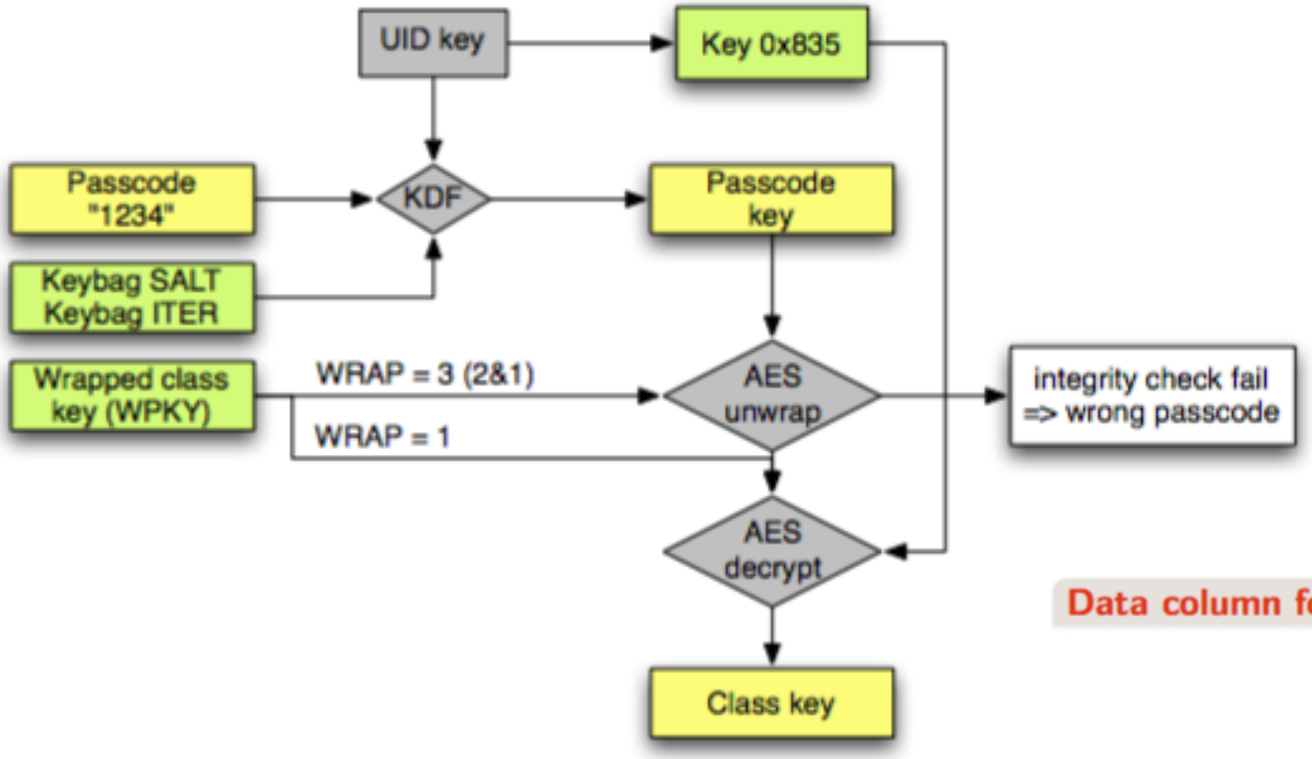
Step

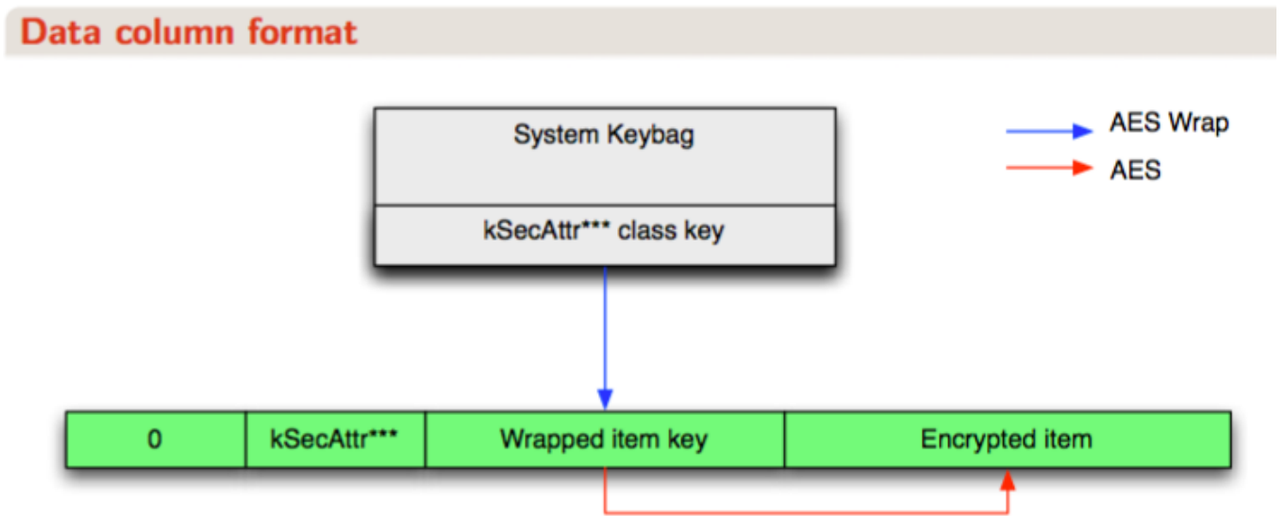
- 키체인 구조 분석
- 암호화 기법 분석
- 데이터 복호화 및 검증

키체인 구조 분석


Hardware UID
System Keybag
Name
Date Modified
Size
.DS_Store
오늘 오전 9:46
6 KB
.fl0D1D1BA9
2013. 3. 15. 오전 10:43
Zero bytes
.fl62323D2F
2013. 3. 15. 오전 10:34
Zero bytes
.fl86A9AF81
2013. 3. 30. 오전 10:12
Zero bytes
F24BB238-1B79-5F...331-86E9AF841A31
2013. 6. 12. 오전 10:19
--
user.kb
2013. 6. 12. 오전 10:19
1 KB
keychain-2.db
keychain-2.db-shm
어제 오전 10:37
33 KB
keychain-2.db-wal
어제 오전 10:44
1.5 MB
login.keychain
어제 오전 10:39
188 KB
metadata.keychain
2013. 6. 10. 오전 9:35
23 KB
Microsoft_Intermediate_Certificates
2013. 3. 30. 오전 10:12
20 KB
PeerManifestCache.plist
어제 오후 2:13
5 KB
PersistedAccount.plist
어제 오전 10:45
1 KB
Unknown(Key?)
iCloud Keychain
Local Keychain
iCloud Metadata(trusted devices information)

Understanding iOS Keychain



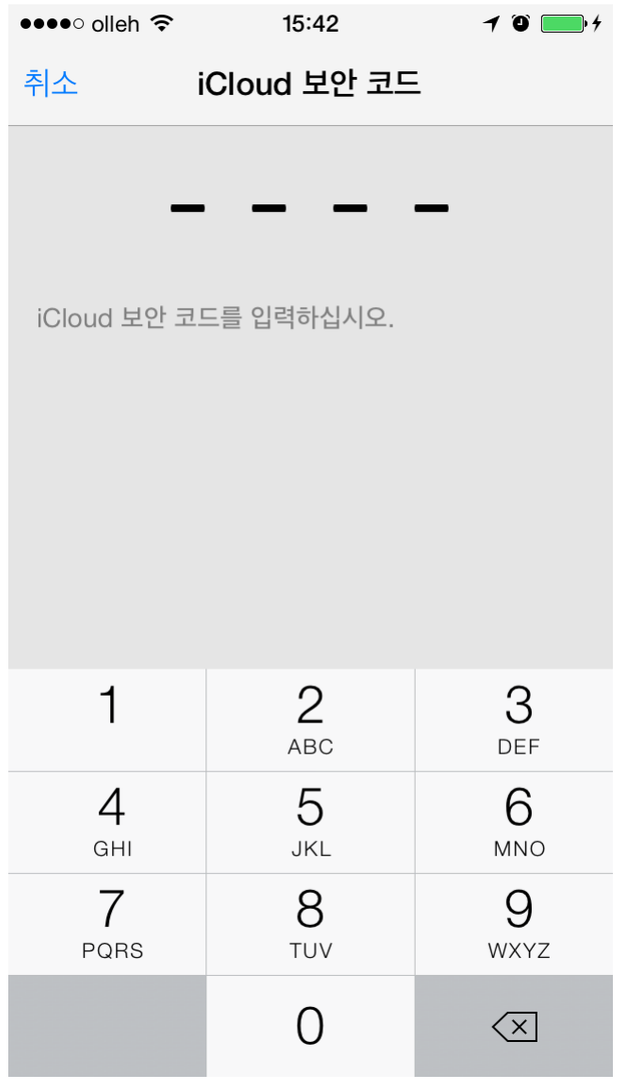


Reference : iPhone data protection in depth, HITB 2011

UID / Passcode?

Hardware Overview:

Model Name:	MacBook Pro
Model Identifier:	MacBookPro5,5
Processor Name:	Intel Core 2 Duo
Processor Speed:	2.53 GHz
Number of Processors:	1
Total Number of Cores:	2
L2 Cache:	3 MB
Memory:	8 GB
Bus Speed:	1.07 GHz
Boot ROM Version:	MBP55.00AC.B03
SMC Version (system):	1.47f2
Serial Number (system):	W[redacted]66E
Hardware UUID:	F24[redacted]86E9AF[redacted]
Sudden Motion Sensor:	
State:	Enabled



iCloud Keychain

- File Format : SQLite3
- Prior to v3.7.0, atomic commit and rollback is a rollback journal
- Beginning with v3.7.0, a new “Write-Ahead Log” option is available

Write-Ahead Logging

- 원본 컨텐츠를 데이터베이스 파일에 보존
- 변경된 내용은 WAL에 추가 됨
- COMMIT :WAL에 추가함
- WAL는 shared memory를 사용하여 성능을 높임

Write-Ahead Logging

- Checkpointing : WAL 파일에 추가된 모든 트랙젝션을 원본 데이터베이스에 반영
  - WAL파일이 1000페이지의 사이즈에 도달하면 자동으로 Checkpoint

DEMO

Q & A

nofate@nofate.com