



OS X Yosemite Artifacts

Call history and SMS analysis

forensic.nofate.com

OS X Yosemite

- Redesigned interface
 - Continuity
 - Swift
 - Free!



Continuity

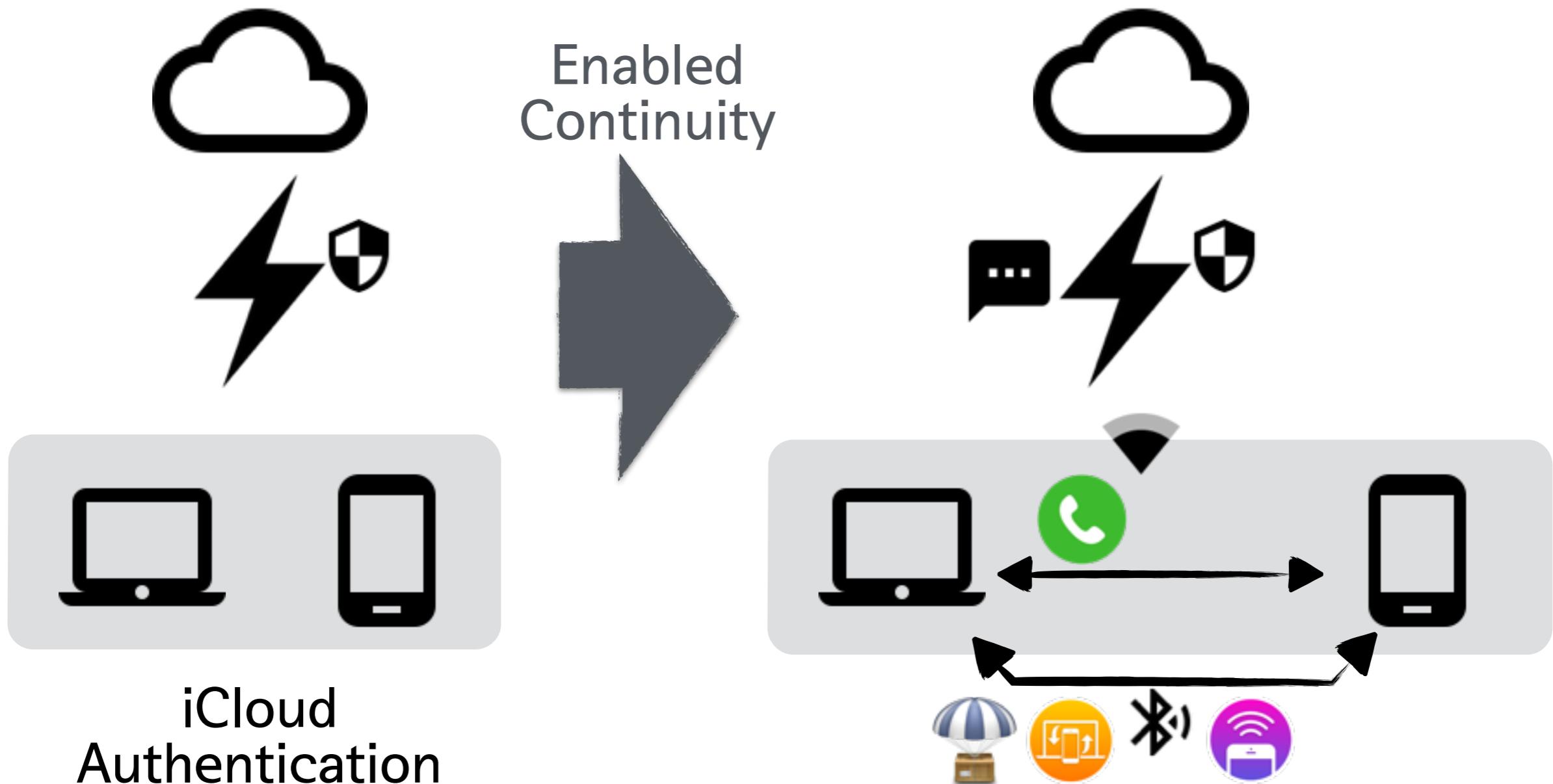


Continuity

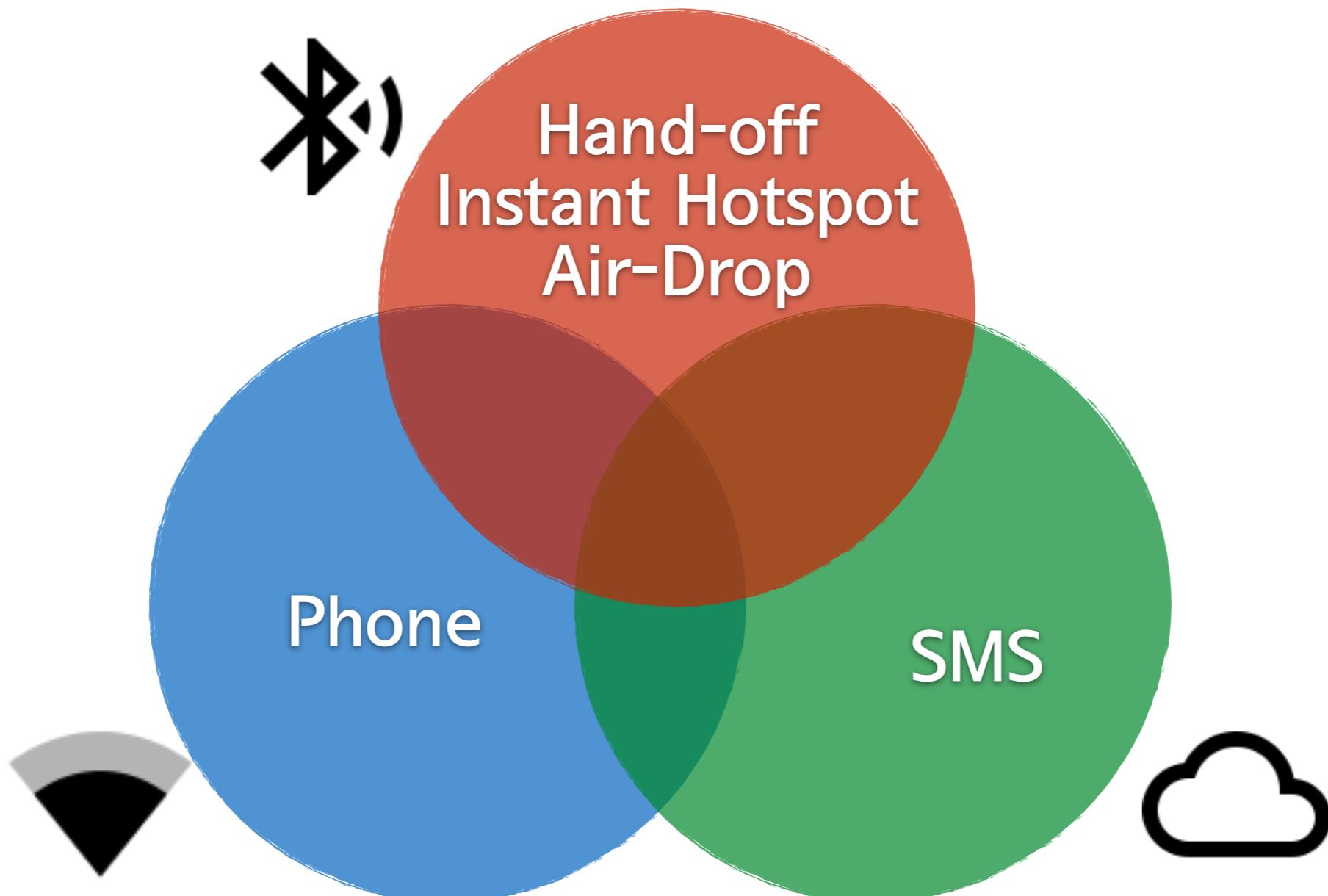
- Mac and iOS connected
 - Phone
 - SMS
 - Handoff
 - Instant Hotspot
 - AirDrop



Continuity

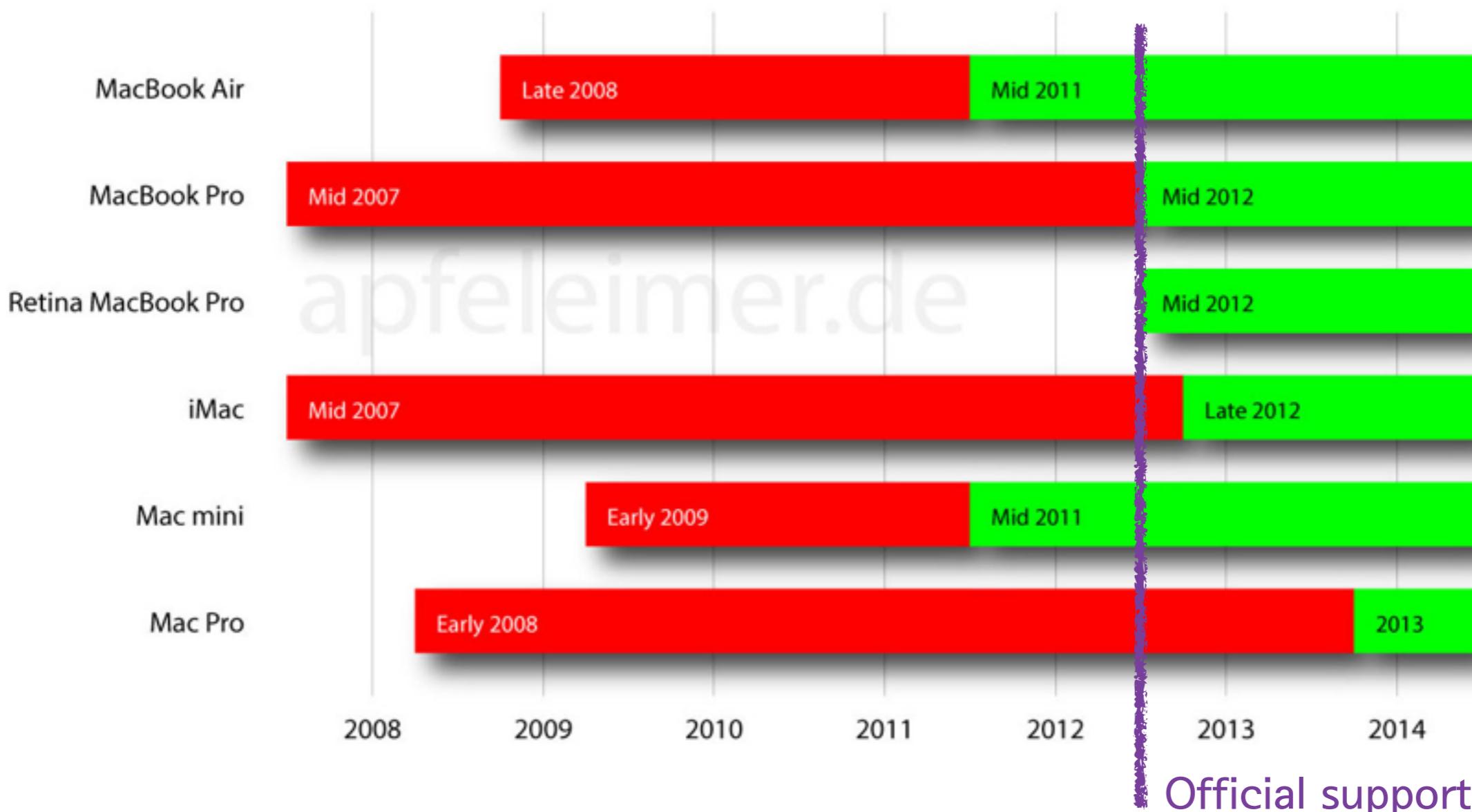


Requirement



Requirements

OS X Yosemite - Bluetooth 4.0 / LE





Call history and SMS analysis

SMS DB analysis



Path : ~/Library/Messages/chat.db

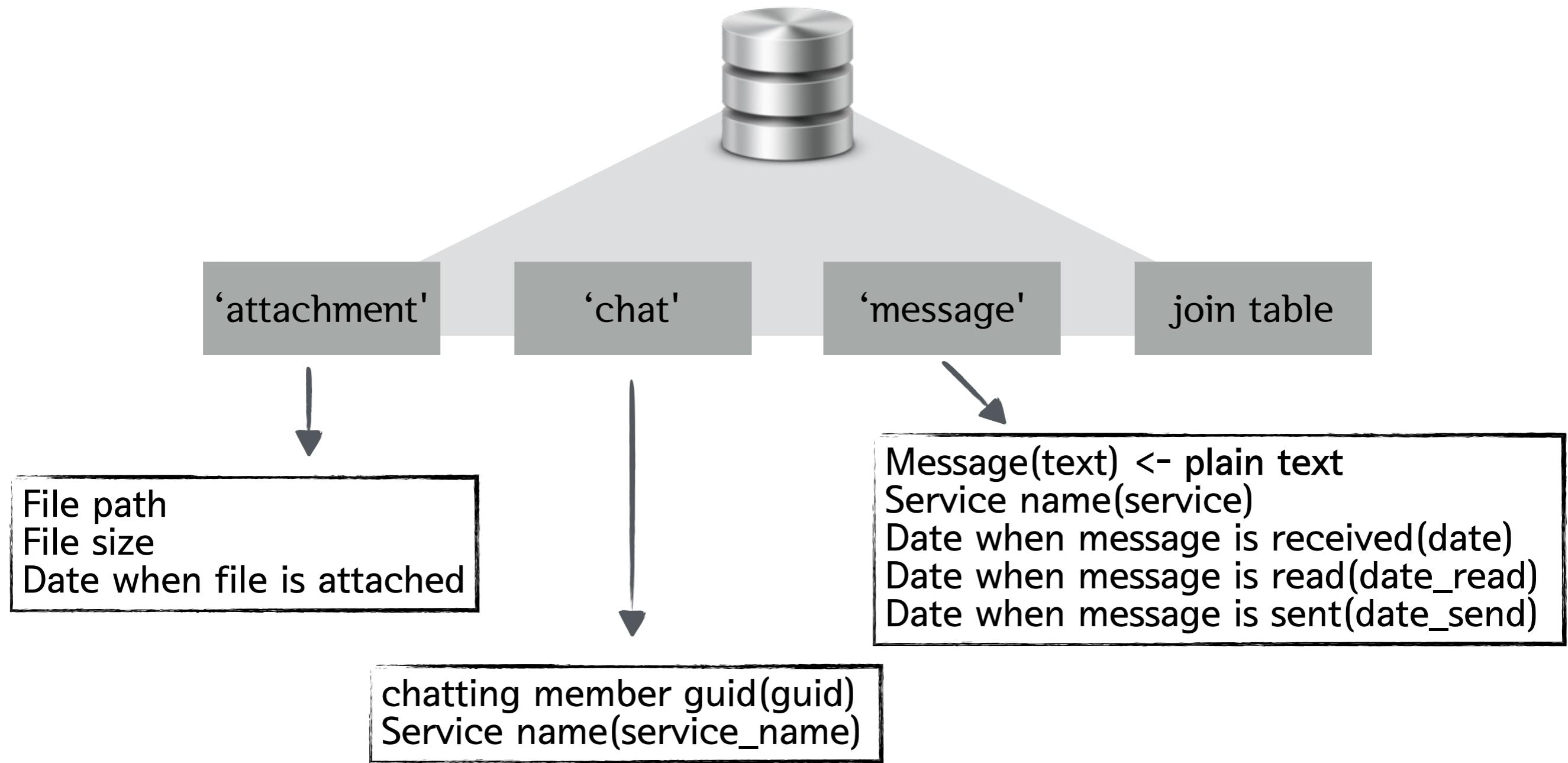


DB : SQLite3 enabled WAL mode



Attachment :
~/Library/Messages/Attachments

SMS DB analysis



Call history analysis



전화 하기.

Mac에서 전화를 거는 일 역시 정말 간단합니다. '연락처', '캘린더', '메시지', Spotlight, Safari에서 전화번호를 클릭하기만 하면 되죠. '캘린더' 이벤트에서 직접 컨퍼런스 콜에 들어가면 Mac이 암호를 자동으로 입력해줍니다. 통화를 시작하려면 FaceTime에서 iPhone 통화 내역을 찾거나, 직접 전화번호를 입력하면 됩니다.

Call history analysis



Path : ~/Library/Application Support
/CallHistoryDB/CallHistory.storedata

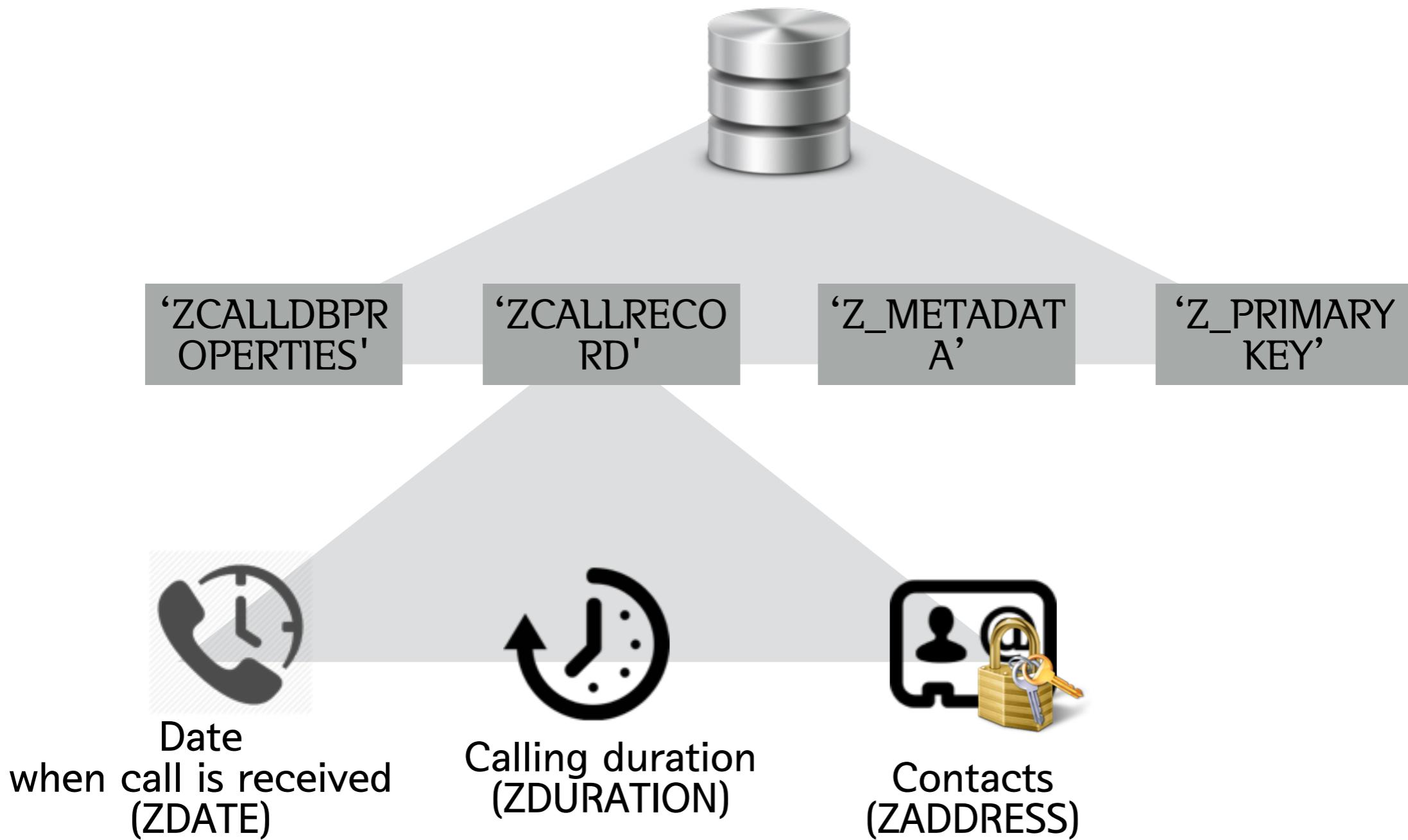


DB : SQLite3 enabled WAL mode

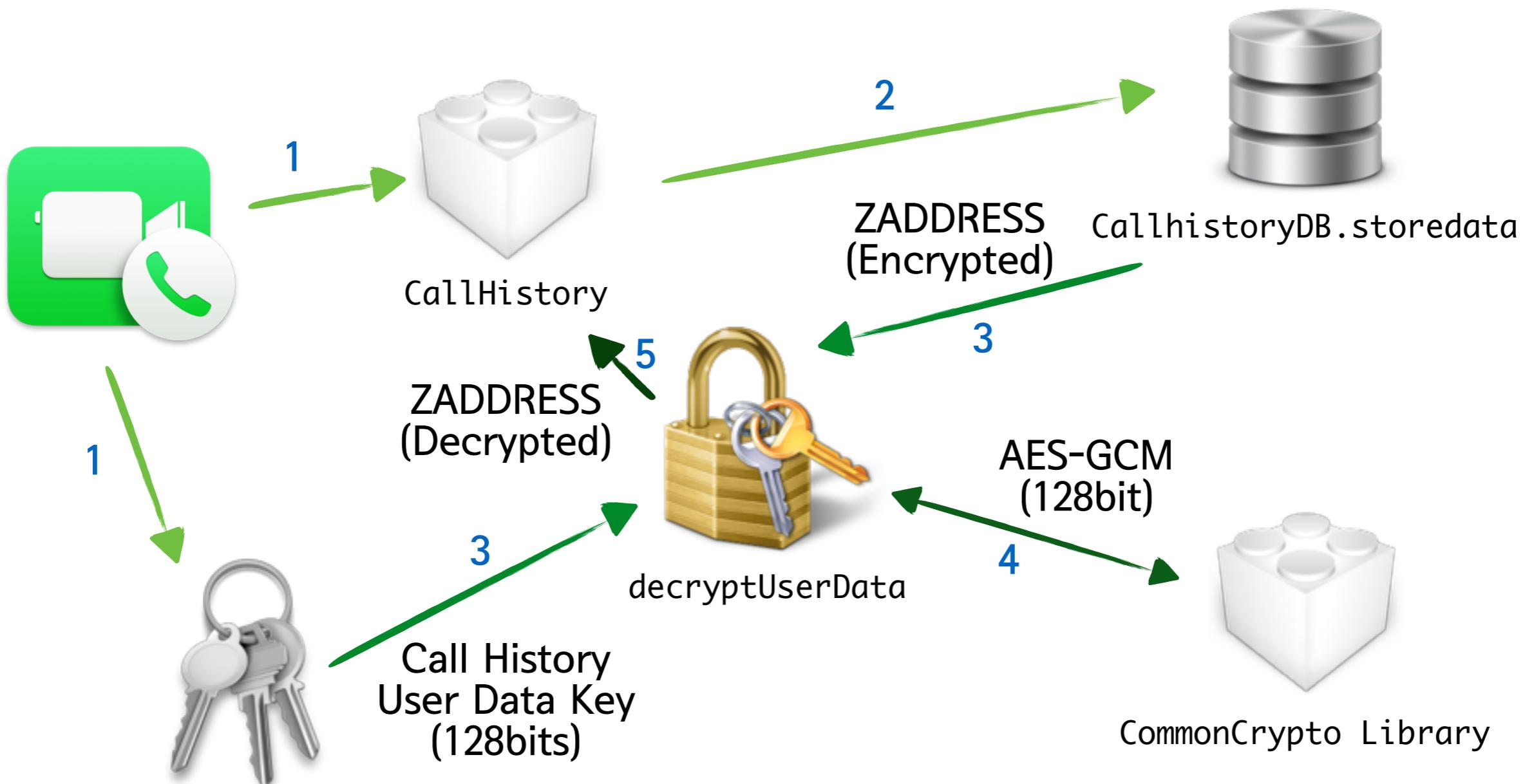


Encrypted Sensitive information

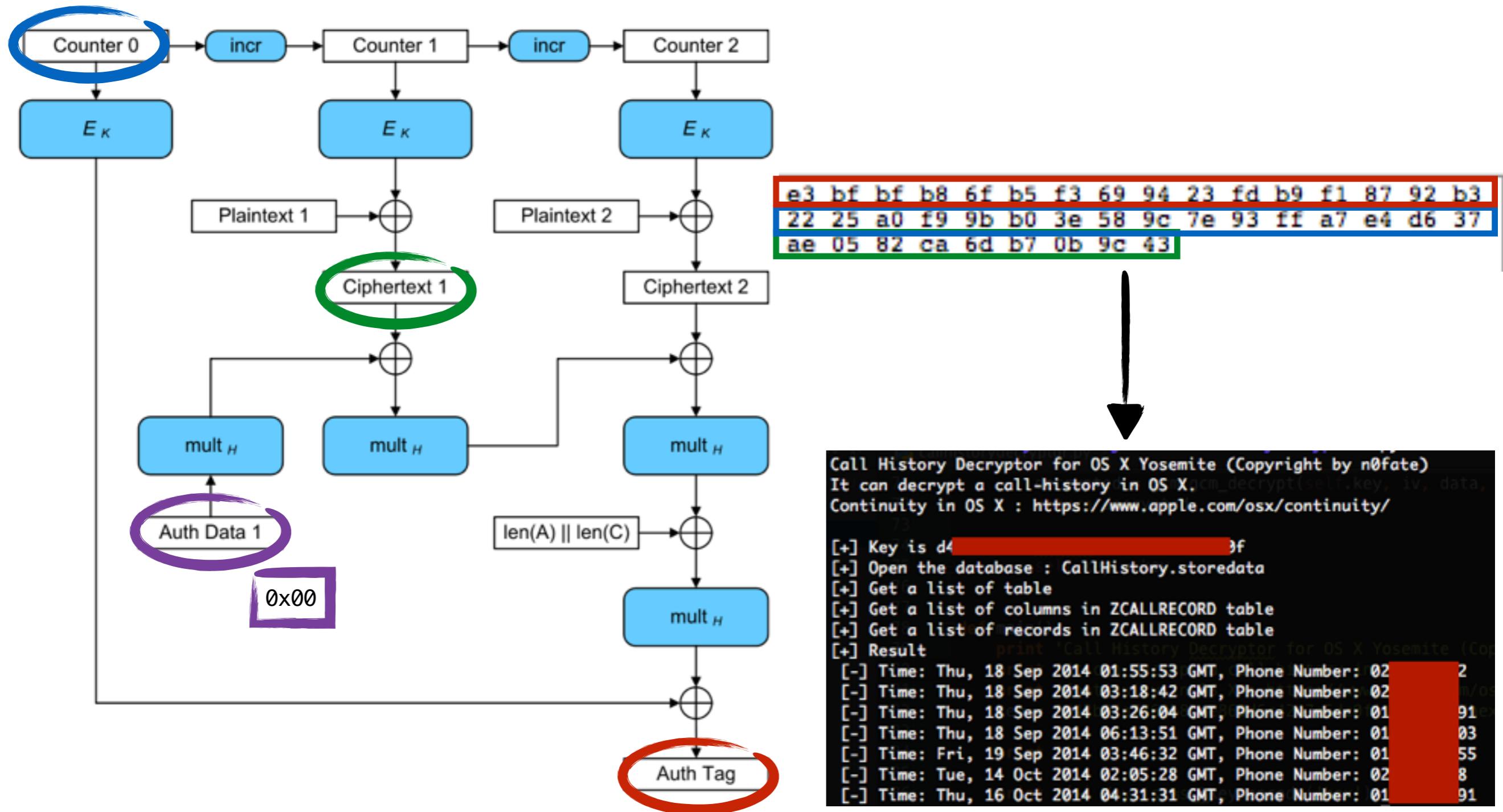
Call history analysis



Call history analysis



Call history analysis



Demo

```
Call History Decryptor for OS X Yosemite (Copyright by n0fate)
It can decrypt a call-history in OS X.
Continuity in OS X : https://www.apple.com/osx/continuity/
[+] Key is d4[REDACTED]0f
[+] Open the database s: CallHistory.storedatabase
[+] Get a list of table
[+] Get a list of columns in ZCALLRECORD table
[+] Get a list of records in ZCALLRECORD table
[+] Result      print 'Call History Decryptor for OS X Yosemite (Cop
[-] Time: Thu, 18 Sep 2014 01:55:53 GMT, Phone Number: 02[REDACTED]2
[-] Time: Thu, 18 Sep 2014 03:18:42 GMT, Phone Number: 02[REDACTED]m/os
[-] Time: Thu, 18 Sep 2014 03:26:04 GMT, Phone Number: 01[REDACTED]91ex
[-] Time: Thu, 18 Sep 2014 06:13:51 GMT, Phone Number: 01[REDACTED]03
[-] Time: Fri, 19 Sep 2014 03:46:32 GMT, Phone Number: 01[REDACTED]55
[-] Time: Tue, 14 Oct 2014 02:05:28 GMT, Phone Number: 02[REDACTED]8
[-] Time: Thu, 16 Oct 2014 04:31:31 GMT, Phone Number: 01[REDACTED]91
```

Q & A

nofate@nofate.com