정 보 보 호 학 회 지
제26권 제5호, 2016. 10

맥 포렌식을 통한 아이폰 아티팩트 분석 기법

이 경 식*

요 약

아이폰은 애플컴퓨터에서 개발한 스마트폰으로 애플의 데스크톱 운영체제인 OS X를 스마트폰에 맞게 변형한 iOS 운영체제를 사용한다. iOS는 폐쇠성과 높은 보안성 기능을 내장함으로 사용자에게는 개인 정보를 안전하게 보호할 수 있는 장점을 제공하지만, 디지털 포렌식 분석가에게는 분석 시 많은 어려움을 주고 있다.

애플은 2013년 OS X 매버릭스(10.9)를 시작으로 iOS와 OS X간의 기밀 정보 동기화 및 통화/문자 메시지를 연동할 수 있는 기능을 제공하기 시작하였으며, 2016년에 공개된 시에라(10.12)에서도 클립보드 기능 공유 등의 다양한 연동 기능을 제공하고 있다. 이러한 편의 기능은 분석가에게 아이폰 분석이 어려운 상황에서 아이폰 소유주의 OS X 시스템을 분석하여 아이폰의 아티팩트를 확보할 수 있는 한가지 방법이 될 수 있다.

본 논문에서는 아이폰에서만 획득 가능했던 아티팩트인 통화 및 문자 메시지 내역, 패스워드 정보 등이 OS X와 어떻게 연동되는지 알아보고 OS X 분석 만으로 이러한 증거를 확보할 수 있는 기법을 알아보도록 한다.

Ⅰ. 서 론

현재 애플을 대표하는 제품 중 하나로 꼽히는 아이폰(iPhone)은 자사의 운영체제인 iOS를 내장한 스마트폰이다. iOS는 OS X를 스마트폰에 맞게 변형한 운영체제로 OS X가 가지는 유닉스의 안정성을 그대로 가지고 있으며, 사용자 정보를 안전하게 보관하기 위한 폐쇠적인 애플리케이션 샌드박스 정책과 하드웨어 기반의 디스크 암호화, 원격 잠금 등 다양한 보안 기능을 내장하였다.

이러한 다양한 보안 기능은 사용자에게 안전한 환경을 제공하지만 디지털 포렌식 분석가에게는 아이폰 내의 증거 수집에 어려움을 겪게 한다. 특히 통화 내역, 문자 메시지와 같은 정보는 스마트폰에만 보관되는 정보 수집이 극히 제한된다.

애플은 여러 대의 애플 제품을 사용하는 사람들의 불편함을 해소하기 위해 2013년부터 다양한 기능을 추가하기 시작하였다. 사용자가 전화와 문자 기능을 아이폰을 이용해서만 사용할 수 있었던 것을 다른 애플 제품에서도 사용할 수 있게 하였으며, 하나의 애플 제품에서 웹 사이트 로그인 정보를 저장하면 다른 제품에서 자동 로그인이 가능하게 하는 등 한 곳에서 입력한 기밀 정보를 여러 맥에서 동기화할 수 있게 하는 기능을 제공하였다.

본 논문에서는 이러한 iOS와 OS X 간의 연동 기능을 알아보고 OS X 시스템에서 연동되는 아티팩트를 수집/분석하여 아이폰의 아티팩트를 확보하는 기법을 소개한다.

Ⅱ. OS X - iOS간 연동 기능 소개

OS X는 매버릭스의 아이클라우드 키체인 기능을 시작으로 iOS와의 동기화 및 연동 기능을 제공한다. 특히 OS X 요세미티의 경우에는 셀룰러 통신이 가능한 아이폰에서만 쓸 수 있었던 전화와 문자 메시지를 다른 iOS와 OS X에서도 사용할 수 있는 연동 기능을 추가하였다. 단, 이 기능은 2012년 이후 출시된 맥 제품부터 지원한다 [1].

2.1. 문자 메시지 연동

아이폰의 메시지(Message) 앱은 애플이 개발한 서비스인 아이메시지(iMessage) 외에도 통신사의 문자 메시지(SMS, MMS)를 송수신할 수 있다.

* 국방과학연구소 2본부 3부 선임연구원(n0fate@add.re.kr)

〔그림 1〕 문자메시지 연동

사용자가 아이폰에서 동일 아이클라우드로 로그인한 OS X 시스템의 문자 메시지 연동 기능을 활성화하면, 활성화한 OS X의 메시지 앱에서 아이폰과 똑같이 문자 메시지를 송수신할 수 있다.

문자 메시지는 아이클라우드를 통해 송수신되며, 기능이 동작하려면 동일한 와이파이 네트워크 내에 위치해야 한다.

2.2. 전화 연동

OS X의 전화 연동 기능은 동일한 아이클라우드 계정으로 로그인한 모든 OS X와 iOS가 아이폰에 등록된 하나의 전화번호로 송수신할 수 있다. 연동이 완료되면, 아이폰으로 오는 전화를 동일 네트워크의 동일 아이클라우드 계정으로 연동된 애플 제품에서 수신할 수 있다. 또한 내장 애플리케이션인 페이스타임(Facetime)에서 전화를 걸 수 있다.

전화 연동 기능은 OS X와 iOS가 와이파이 네트워크를 이용하여 데이터를 송수신하며 두 기기가 동일 네트워크 내에 위치해야 한다.

〔그림 2〕 전화 연동

2.3. 키체인 동기화

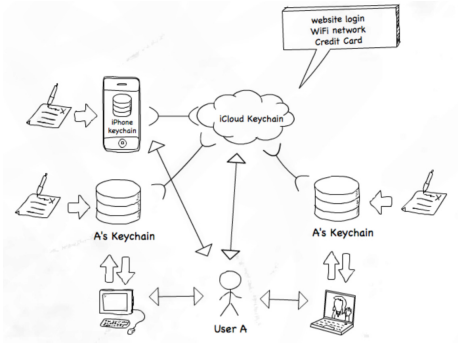
키체인 시스템(Keychain System)은 애플에서 제공하는 패스워드 관리 시스템으로 iOS, OS X에 내장되어 있다. 개발자는 애플에서 제공하는 몇 가지 API를 이용하여 키체인에 기밀 정보를 안전하게 저장할 수 있다. 키체인 시스템은 사용자에게 명시적으로 드러나지 않는다.

애플은 사용자가 여러 애플 제품에서 동일한 사이트의 인증을 여러 번 하는 문제점을 해소하기 위해 아이클라우드 키체인(iCloud Keychain)을 공개하였다. 아이클라우드 키체인은 사용자가 하나의 iOS 또는 OS X 시스템에서 인증한 웹사이트 정보, 와이파이 정보, 신용카드 정보를 동일한 아이클라우드 계정으로 인증한 기기에서 사용하기 위한 기능을 제공한다.

아이클라우드 키체인은 환경설정의 아이클라우드에서 '키체인'이 켜져 있어야만 가능하다. 아이클라우드 키체인은 2단계 인증(아이클라우드 인증과 휴대폰 또는 PIN 코드 인증)으로 활성화 할 수 있다.

OS X 요세미티부터 운영체제 설치 과정에서 아이클라우드 활성화 여부를 확인하며 이 옵션은 기본으로 활성화에 체크되어 있다.

〔그림 3〕 키체인



〔그림 4〕 아이클라우드 키체인

Ⅲ. OS X-iOS 연동 정보 분석 기법

분석가가 OS X에 저장된 아이폰 아티팩트를 분석한다면, 높은 보안성을 가진 아이폰을 분석하는데 쏟는 시간을 절약할 수 있으며, 아이폰에서 획득한 증거의 무결성 보장에도 활용할 수 있다.

이 장에서는 앞서 설명한 3가지 iOS 연동 기능의 아티팩트 위치를 알아보고 이를 분석 방법과 도구를 소개한다.

3.1. 문자 메시지 내역 분석

OS X는 메시지 앱을 이용하여 문자 메시지를 관리한다. 메시지 앱은 각 사용자 계정마다 하나의 데이터베이스를 가지고 있으며, 데이터베이스 파일은 '{사용자 홈 디렉터리}/Library/Messages/chat.db' 에 저장되어 있다. 이 파일은 SQLite3 포맷으로 되어 있으며 저널링 방식으로 WAL(Write-ahead Logging)을 사용하므로, 삭제된 데이터 확보를 위해 저널링 데이터를 분석하고 데이터베이스에 최종 상태를 기록하는 체크포인트 수행한 데이터베이스와 비교 분석하는 과정이 필요하다.

메시지 앱으로 전송한 이미지나 파일의 경우, '{사용자 홈 디렉터리}/Library/Messages/Attachments/'에 일정한 규칙으로 만들어진 디렉터리 내에 전송된 파일이 그대로 저장되어 있다. 이와 관련된 정보도 메시지를 저장한 데이터베이스 파일(chat.db)의 'attachment' 테이블에 파일 경로와 파일 크기, 첨부한 시간이 기록되어 있다.

〔표 1〕 메시지 앱 주요 테이블과 필드 설명

테이블	필드	설명
attachments	filename	첨부된 파일이 저장된 경로
	total_bytes	첨부된 파일 크기
	created_date	파일의 생성시간
	start_date	파일의 전송 시간
chat	chat_identifier	송신자(전화번호, 아이메시지 아이디 등)
	service_name	송수신 방법(SMS, iMessage 등)
message	text	메시지 내용
	date	작성한 시간
	date_read	메시지를 읽은 시간
	date_delivered	메시지를 전송 완료한 시간

문자 메시지를 보관하는 메시지 앱 데이터베이스의 주요 테이블과 필드 정보는 [표 1]과 같다.

문자 메시지 아티팩트의 경우에는 모든 데이터가 평문으로 저장되어 있으므로 SQLite3 데이터베이스 분석 도구를 이용하여 증거를 획득할 수 있다.

3.2. 통화내역 분석

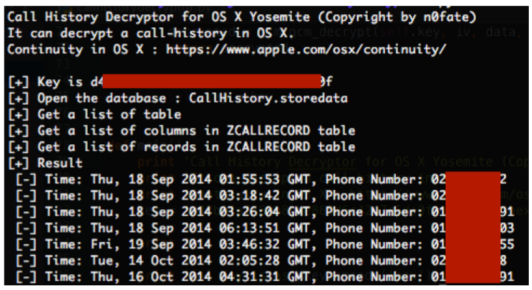
스마트폰에서 통화 관련 정보를 수집할 때는 스마트폰 소유주가 누구와 통화했는지 알기 위해 통화 내역을 수집한다. OS X의 경우에는 자신이 수신한 통화 정보를 페이스타임 애플리케이션의 통화 내역에 기록해둔다. OS X에서 보관하는 통화 내역은 아이폰에서 수신한 통화 내역 외에도 페이스타임 통화내역까지 저장하고 있다.

통화 내역도 문자 메시지와 같이 각 사용자 계정마다 하나의 데이터베이스 파일을 가지고 있으며, '{사용자 홈 디렉터리}/Library/Application Support/CallHistoryuDB/CallHistory.storedata'에 저장되어 있다. 이 파일도 저널링 모드로 WAL을 사용하고 있으므로 저널링 파일에 대한 추가적인 분석도 필요하다. 통화 내역 데이터베이스에서 포렌식적으로 의미있는 아티팩트는 'ZCALLRECORD' 테이블에 저장되어 있다. 이 테이블에서 분석에 필요한 주요 필드는 [표 2]와 같다.

분석가는 SQLite 포맷을 분석, [표 2]의 3개의 필드를 추출하여 통화 내역을 확보할 수 있다. 단, 송신자 정보를 암호화하여 보관하는 ZADDRESS 필드를 복호화하는 과정이 추가적으로 필요하다. 해당 필드의 암호화 알고리즘은 'AES-GCM'을 사용하고 있으며, 자세한 내용은 저자가 분석한 내용을 발표한 자료[2]에서 확인할 수 있다. 저자가 공개한 통화 내역 분석 도구[3]를 이용하면 통화 내역 분석 및 암호화된 데이터 복호화를

〔표 2〕 통화 내역의 주요 필드 설명

테이블	필드	설명
ZCALLRECORD	ZDATE	전화 송/수신 시간
	ZDURATION	통화한 시간
	ZADDRESS	송신자(전화번호, 아이메시지 아이디), 암호화되어 있음



〔그림 5〕 Call History Decryptor 수행 결과

수행하여 그 결과를 사용자에게 보여준다.

도구 실행에는 통화 내역 데이터베이스 파일(CallHistory.storedate)과 복호화 키가 필요하다. 복호화 키는 키체인 데이터베이스의 'Call History User Data Key' 키에 저장되어 있다. 두 정보를 입력으로 주면 데이터를 복호화할 수 있다.

3.3. 아이클라우드 키체인 분석

아이클라우드 키체인은 OS X 매버릭스에서 추가된 기능으로 키체인에서 기밀 정보를 동기화하기 위한 기능을 제공한다. 아이클라우드 키체인은 키체인의 모든 데이터를 이전하는 것이 아니라 사파리 웹 브라우저의 사용자 아이디/패스워드, 결제한 신용카드 정보, 와이파이 접속 정보, 이메일 계정과 같이 애플이 동기화가 필요하다 판단되는 키만 동기화하고 있다. 만약 애플리케이션 개발자가 아이클라우드 키체인을 통해 키를 동기화하도록 개발한 경우에는 해당 키도 아이클라우드 키체인에 저장된다. 즉, 분석가는 동일한 아이클라우드로 로그인한 OS X의 아이클라우드 키체인을 분석하여 iOS에서 생성한 기밀 정보를 확보할 수 있다.

아이클라우드 키체인은 '{사용자 홈 디렉터리}/Library/Keychains/[UUID]/'에 저장되어 있다. 여기에서 UUID는 각 맥 고유 식별자인 'IOPlatformUUID'이다.

아이클라우드 키체인은 키를 저장하는 데이터베이스 파일과 데이터베이스 내의 데이터를 암호화하는 키 저장소인 키백(Keybag)으로 이루어져 있다. 'keychain-2.db'가 데이터베이스 파일이며, 키백 파일은 'user.kb'이다. 데이터 암복호화 알고리즘에는 애플이 낸 특허[4]를 변형한 알고리즘을 사용한다. 자세한 알고리즘과 분석 내용은 저자가 발표한 자료[5]에 서술되어 있다.

아이클라우드 데이터베이스 파일에서 키를 저장하는 테이블은 [표 3]과 같이 iOS의 키체인 데이터베이스의 테이블 이름과 동일한 이름을 가진다.

각 테이블에는 여러 필드가 있으나, data 필드에 모든 정보를 암호화하여 보관하기 때문에 data 필드만 분석하면 아이클라우드 키체인의 사용자 키 및 메타 정보를 모두 확보할 수 있다. 복호화하여 획득 가능한 필드 중 주요 필드는 [표 4]와 같다.

이러한 아이클라우드 정보를 분석하는 도구로는 저

〔표 3〕 각 테이블 정보

테이블	설명
genp	일반적인 내용을 저장
inet	인터넷 계정 정보가 저장되는 테이블(사파리, 이메일, SNS 인증 정보)
keys	공개 키 쌍(공개키, 개인키)가 저장되는 테이블
cert	인증서 저장

〔표 4〕 주요 컬럼 정보

필드	설명
cdat	레코드 생성 시간, 유닉스 타임
mdat	레코드의 최종 수정 시간, 유닉스 타임
acct	계정 이름
data	다른 모든 필드 및 패스워드 정보를 암호화하여 저장
srvr	기밀 정보가 사용되는 서버 주소
sync	활성화된 경우, 해당 레코드가 아이클라우드 서버를 통해 동기화
tomb	삭제된 레코드 정보. 활성화되어 있으면 해당 정보를 사용하지 않는 것으로 판단

```
n0fate@MacBook-Pro:~/iChainbreaker$ python iChainbreaker.py -h
usage: iChainbreaker.py [-h] -p PATH -k KEY [-x EXPORTFILE]

Tool for iCloud Keychain Analysis by @n0fate

optional arguments:
  -h, --help            show this help message and exit
  -p PATH, --path PATH  iCloud Keychain Path(~/Library/Keychains/[UUID]/)
  -k KEY, --key KEY     User Password
  -x EXPORTFILE, --exportfile EXPORTFILE
                        Write a decrypted contents to SQLite file (optional)
n0fate@MacBook-Pro:~/iChainbreaker$
```

〔그림 6〕 아이클라우드 키체인 복호화 도구

자가 개발한 ‘iChainbreaker’가 있다. 본 도구는 오픈소스로 Github를 통해 다운로드할 수 있다[6].

‘iChainbreaker’는 아이클라우드 데이터베이스와 키백이 저장된 디렉터리와 사용자 패스워드를 인자로 데이터를 복호화하여 포렌식적으로 의미있는 정보를 사용자에게 보여준다. ‘-x’ 옵션에 파일을 지정하면 복호화한 정보를 SQLite3 포맷으로 저장한다.

Ⅳ. 결 론

스마트폰은 디지털 포렌식 분야의 주요 분석 대상이지만 임베디드 기기의 제한적 인터페이스와 제조사의 다양한 보안 기능(디스크 암호화, 지속적인 보안 패치 등)로 인해 데스크톱/랩톱에 비해 분석 기법이 제한적이다.

본 논문에서는 이러한 문제를 해결하기 위한 한가지 방법으로 데스크톱 운영체제와 모바일 장치간의 연동 기능을 활용한 데이터 분석을 제안하였다.

기존 아이폰 장치를 분석해서만 확보할 수 있었던 통화 내역, 문자 메시지를 데스크톱 운영체제인 OS X에서 확보하는 방법과 아이폰에서 저장된 웹 브라우저의 로그인 정보, 이메일 계정, 와이파이 정보 등도 OS X에서 확보할 수 있는 방법을 소개하였다.

최근에 발표된 맥 운영체제인 macOS 시에라에는 본 논문에서 소개한 연동 및 동기화 아티팩트 외에도 다양한 공유 기능이 추가되었다. 이렇게 새롭게 추가된 아티팩트에 대한 지속적인 분석이 필요하다.

참 고 문 헌

[1] macOS 업그레이드 하기, http://www.apple.com/kr/macos/how-to-upgrade/ (검색 2016년 10월 9일).

[2] n0fate, OS X Yosemite Artifacts, https://forensic.n0fate.com/wp-content/uploads/2015/08/Forensic-artifacts-for-OS-X-YosemiteENG.pdf, Oct, 31, 2014.

[3] Github, https://github.com/n0fate/OS-X-Continuity/, (검색 2016년 10월 9일).

[4] Michael Lambertus Hubertus Brouwer; Mitchell David Adler, System and method for content protection based on a combination of a user pin and a device specific identifier, US 12/797,587, Oct, 13, 2011.

[5] n0fate, 맥 키체인 포렌식 분석, FIOS 2015, Aug, 22, 2015.

[6] Github, https://github.com/n0fate/iChainbreaker/, (검색 2016년 10월 9일).

〈저자소개〉

이 경 식 (Kyeongsik Lee)
정회원

2009년 2월 : 세종대학교 컴퓨터 공학과 졸업
2011년 2월 : 고려대학교 정보경영공학과 석사
2011년 1월~현재 : 국방과학연구소 선임연구원

관심분야 : 정보보호, 디지털 포렌식