Cloud Storage Forensics
Part I : Dropbox

2013. 09. 28

forensic.n0fate.com

Dropbox Forensics

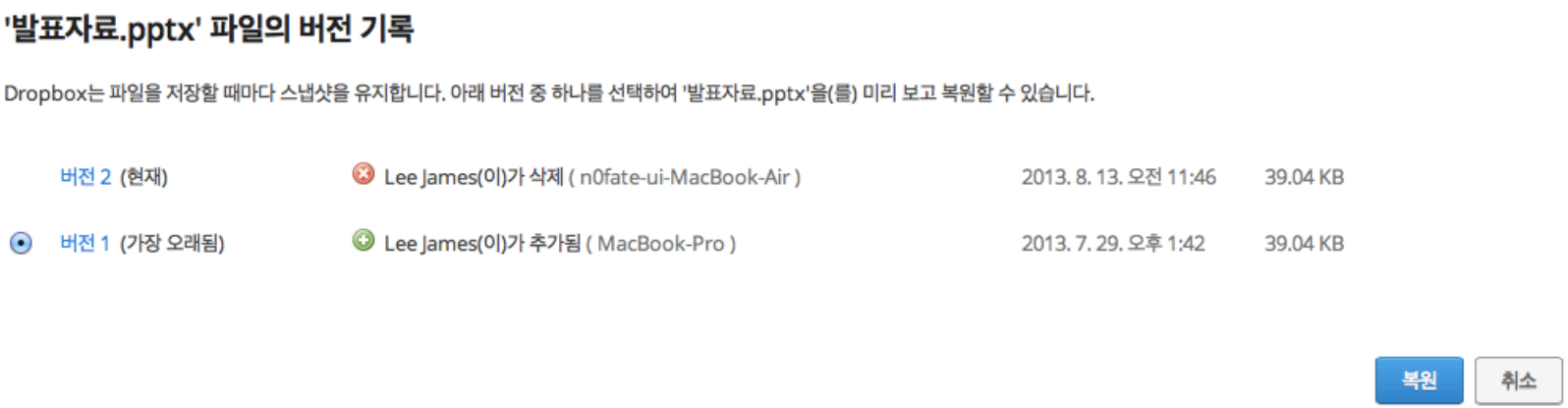
Dropbox Forensics

- Dropbox
  - 웹 기반 파일 공유 서비스
  - 총 12개의 클라이언트 지원
    - Desktop : Windows, Mac OS X, Linux
    - Mobile : iOS, Android, Symbian, Win Mobile, Blackberry
  - 한 계정 당 무료로 2GB까지 지원

- 자동 동기화 및 사용자 간 자료 공유

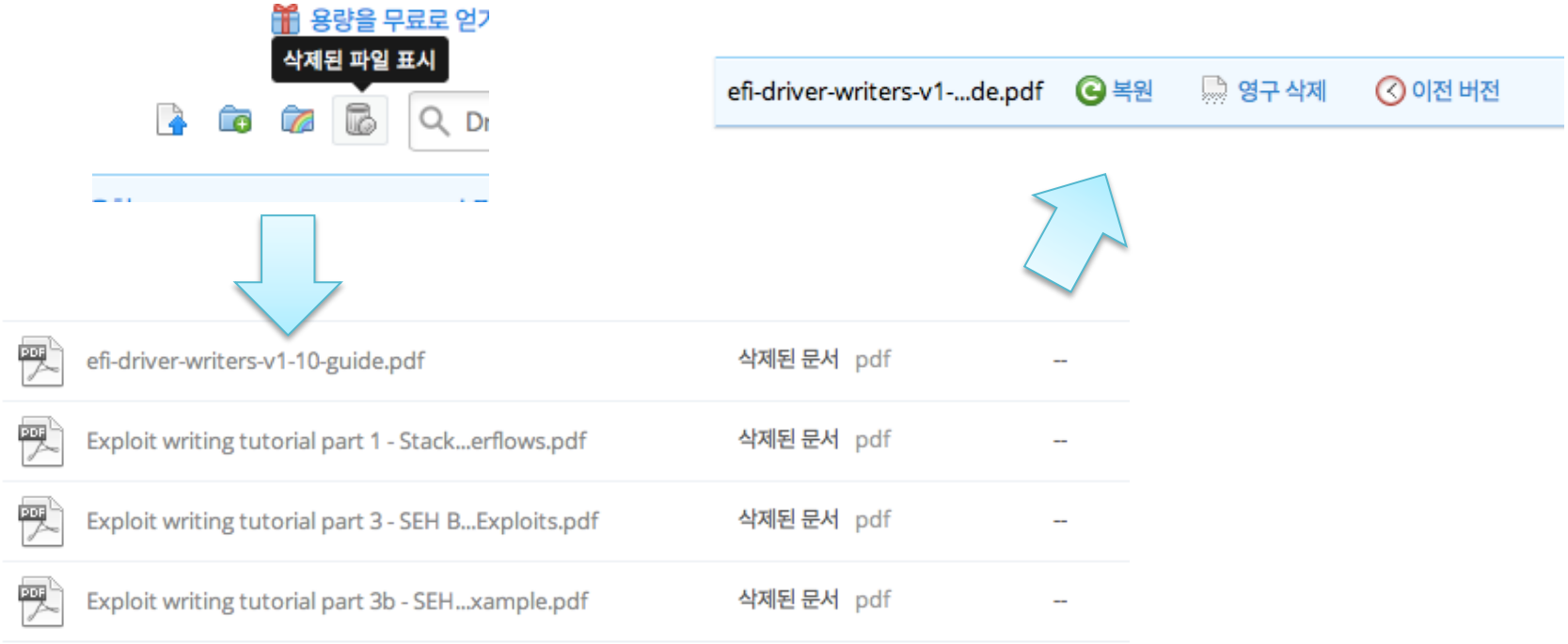
Dropbox Feature

- Previous Version
  - 각 파일에 대한 버전 기록을 유지함
  - 변경한 사용자, 호스트 명, 시간, 용량 정보



Dropbox Feature

- Recovery deleted files
  - 삭제된 데이터는 최대 30일(팩랫:무제한) 보관



Dropbox Forensics

- Dropbox의 데이터는 디스크에 저장
  - 디스크 이미지에서 각 파일을 접근할 수 있음
  - 별다른 문제 없이 분석을 진행할 수 있음

- 삭제된 파일은?
  - '.dropbox.cache'에 삭제한 파일을 기록
  - Dropbox 페이지에 버전 정보 기록

Show deleted files

- 삭제된 파일은 '.dropbox.cache'에 저장
  - 동기화 후 이동/수정/삭제된 파일 저장
  - 최대 3일간 데이터를 유지

```
n0fate-MacBook-Air:~ n0fate$ cd Dropbox/.dropbox.cache/
n0fate-MacBook-Air:.dropbox.cache n0fate$ ls
2013-08-16      2013-08-17
n0fate-MacBook-Air:.dropbox.cache n0fate$ cd 2013-08-16
n0fate-MacBook-Air:2013-08-16 n0fate$ ls
2013 디지털 포렌식 기술 동향 (deleted 60f35a91ffee07c883802a5920aa553f).pptx
2013 디지털 포렌식 기술 동향 (deleted eafa23ac8430ffa0cfb77d847926c0bf).pptx
3E4E51888FB14B239407637B07A3D035 (deleted 2bdac50f2409a961cbefaa83ada787c8).doentry
43B030297C994934B65199C78C8C8F75 (deleted b78f5a24a5cf8f2f18611a764f67b767).doentry
n0fate-MacBook-Air:2013-08-16 n0fate$ file *
2013 디지털 포렌식 기술 동향 (deleted 60f35a91ffee07c883802a5920aa553f).pptx: Zip archive
data, at least v2.0 to extract
.....<snip>...
43B030297C994934B65199C78C8C8F75 (deleted b78f5a24a5cf8f2f18611a764f67b767).doentry:
XML  document text
```

Dropbox Forensics

- 공격자가 해당 폴더 Wiping 수행한 경우?
  - 해당 디렉터리의 정보가 zero-out되기 때문에 분석할 수 없음
  - 다른 요소를 이용하여 최대한 분석 필요
- 존재할 수 있는 요소
  - 계정 정보
  - **파일 목록(존재하는 / 삭제된 파일)**
  - **파일 동기화 여부**

filecache.dbx

- SQLite3 Database format
- file_journal table (<2013)
  - Containing a listing of all directories and files
  - Synchronization information
  - Only the live files, not deleted ones
  - Recovery deleted record though SQLite3 Carving
- In early 2013 Dropbox released an update that encrypted this file

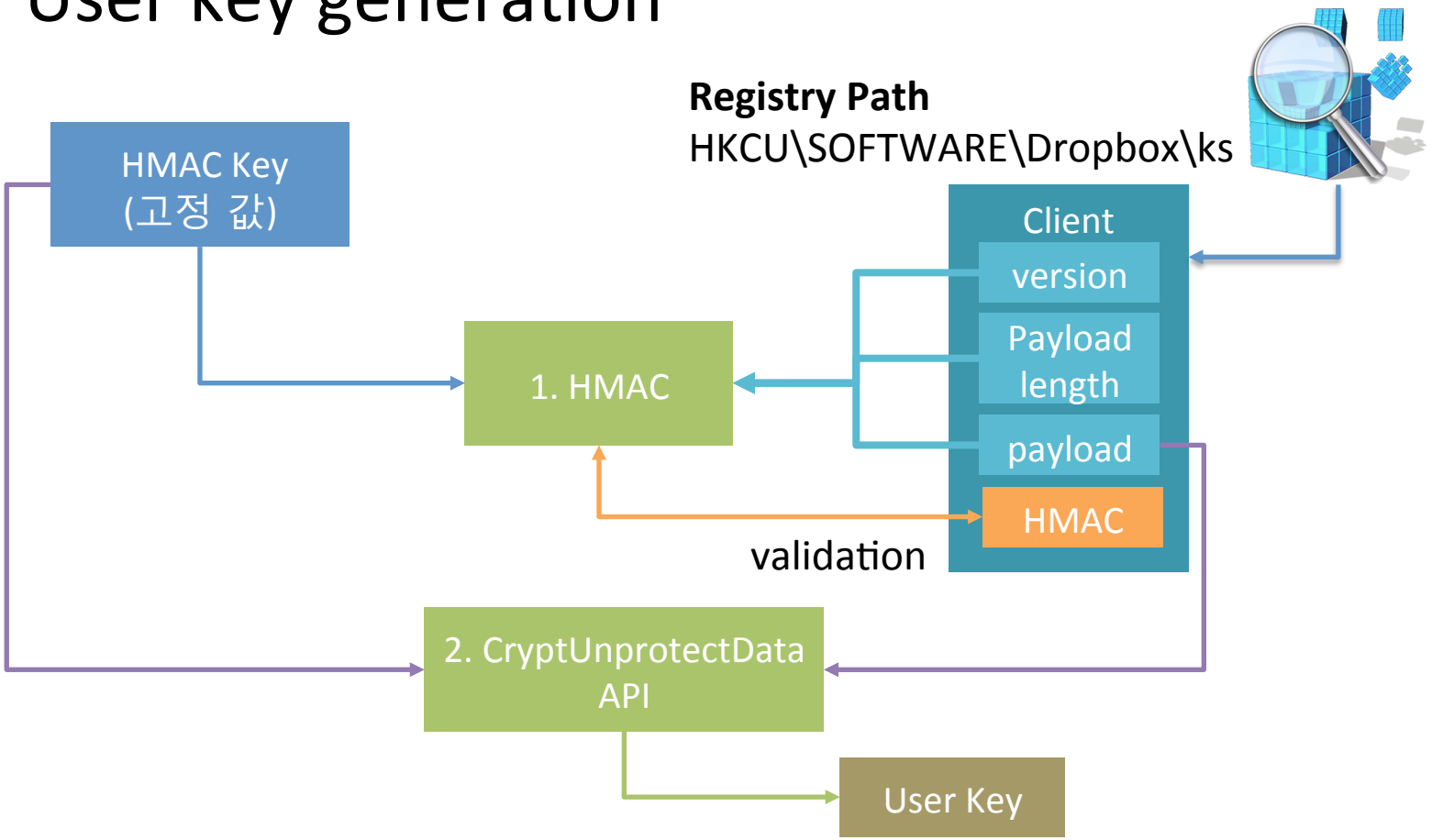
filecache.dbx

- SQLite3 DB Browser로 내용 확인 불가능
  - Hex Editor에서 정상적인 파일로 보이지 않음

- 데이터 암호화로 인해 올바른 해석 불가
  - Sqlite3 Database Encryption 기술을 이용
  - User Password 기반의 Database Key를 생성하여 모든 데이터베이스 암호화
  - 역으로 키를 생성하여 복호화를 수행해야 함.

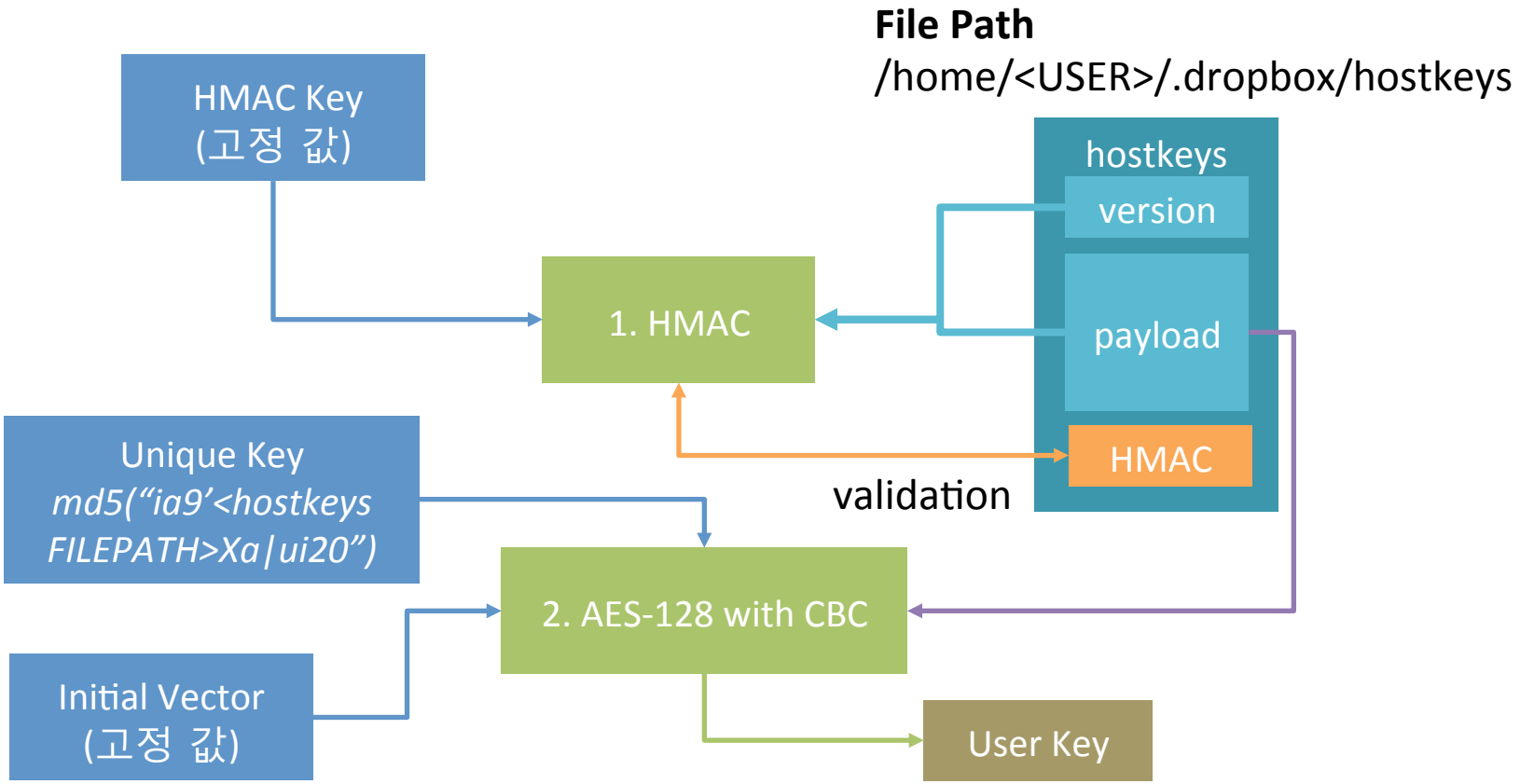
Database Key Generation (Windows)

- User key generation



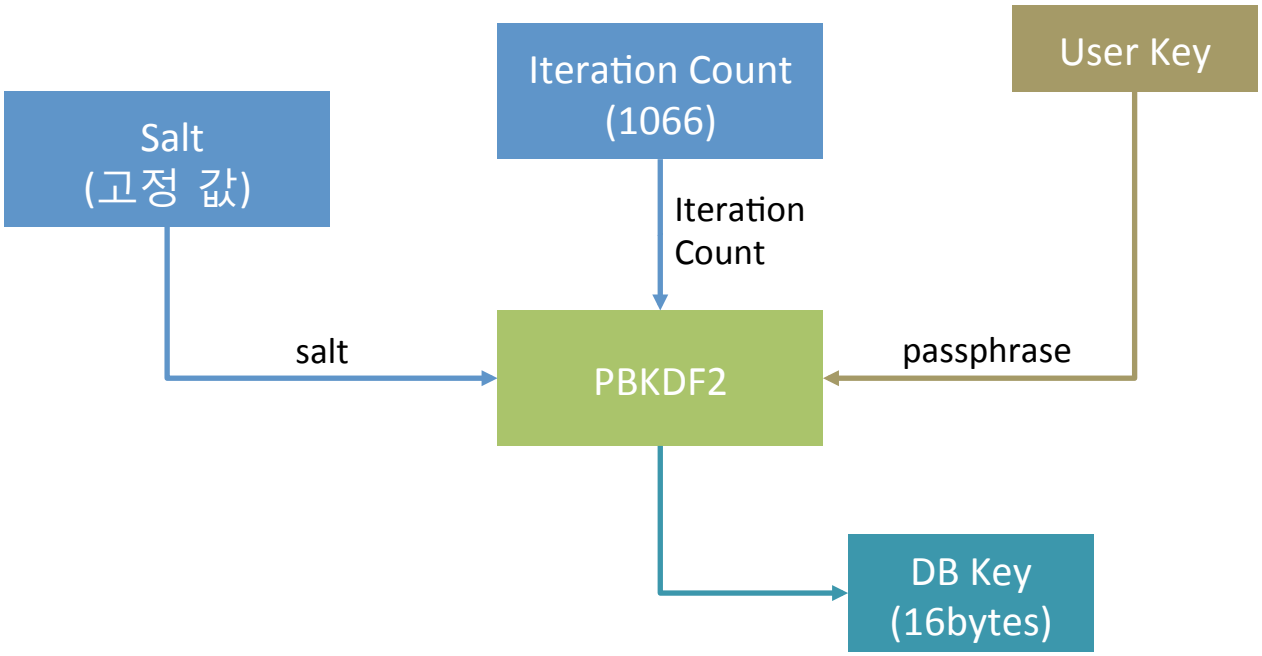
Database Key Generation (Linux)

- User key generation



Database Key Generation (Windows/Linux)

- Database Key generation

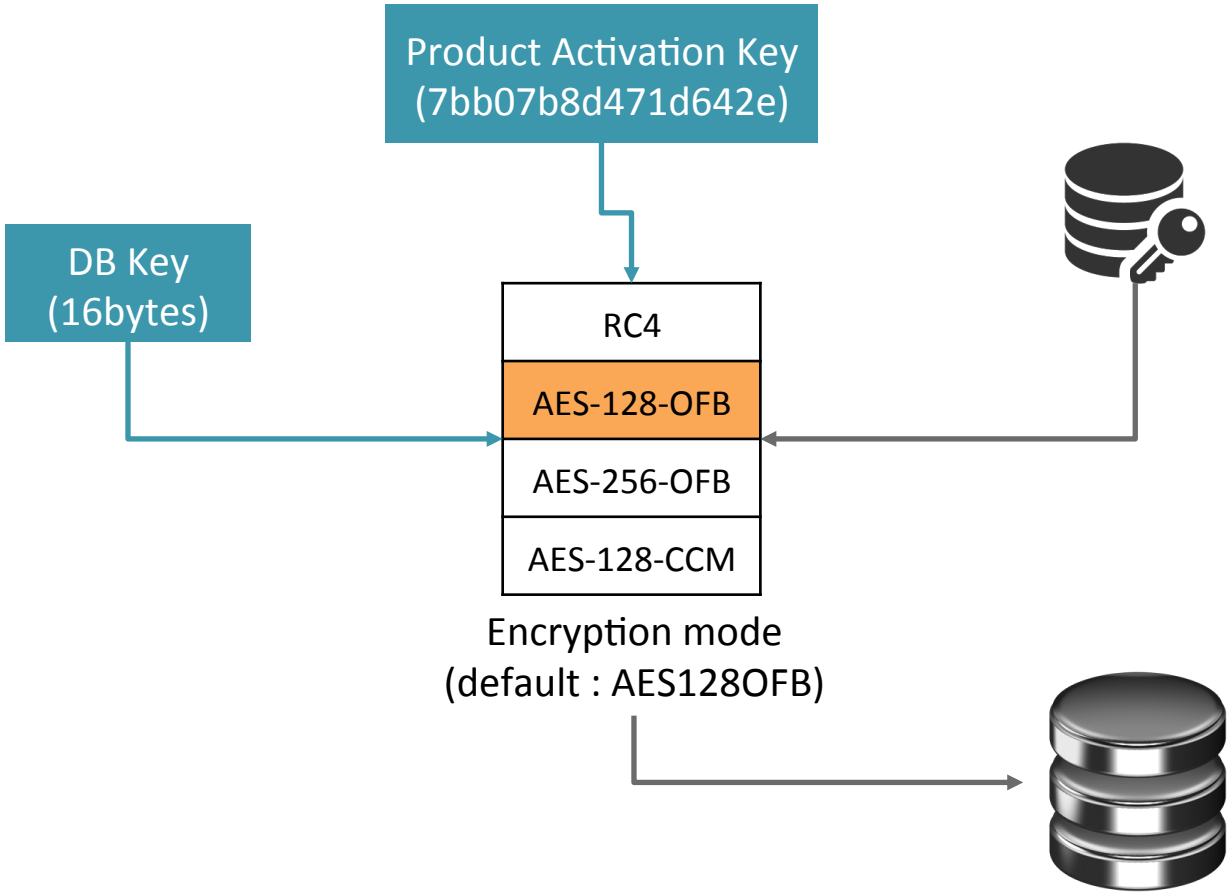


Decrypting SQLite DBX

- SQLite Encryption Extension (SEE)
  - Read and write encrypted database files
  - All data and the metadata is encrypted
  - So outside observer the database appears to contain white noise
  - Public version of SQLite will not be able to read or write an encrypted database file

Link : http://www.sqlite.org/see/doc/trunk/www/readme.wiki

Decrypting SQLite DBX



Tools (Online)

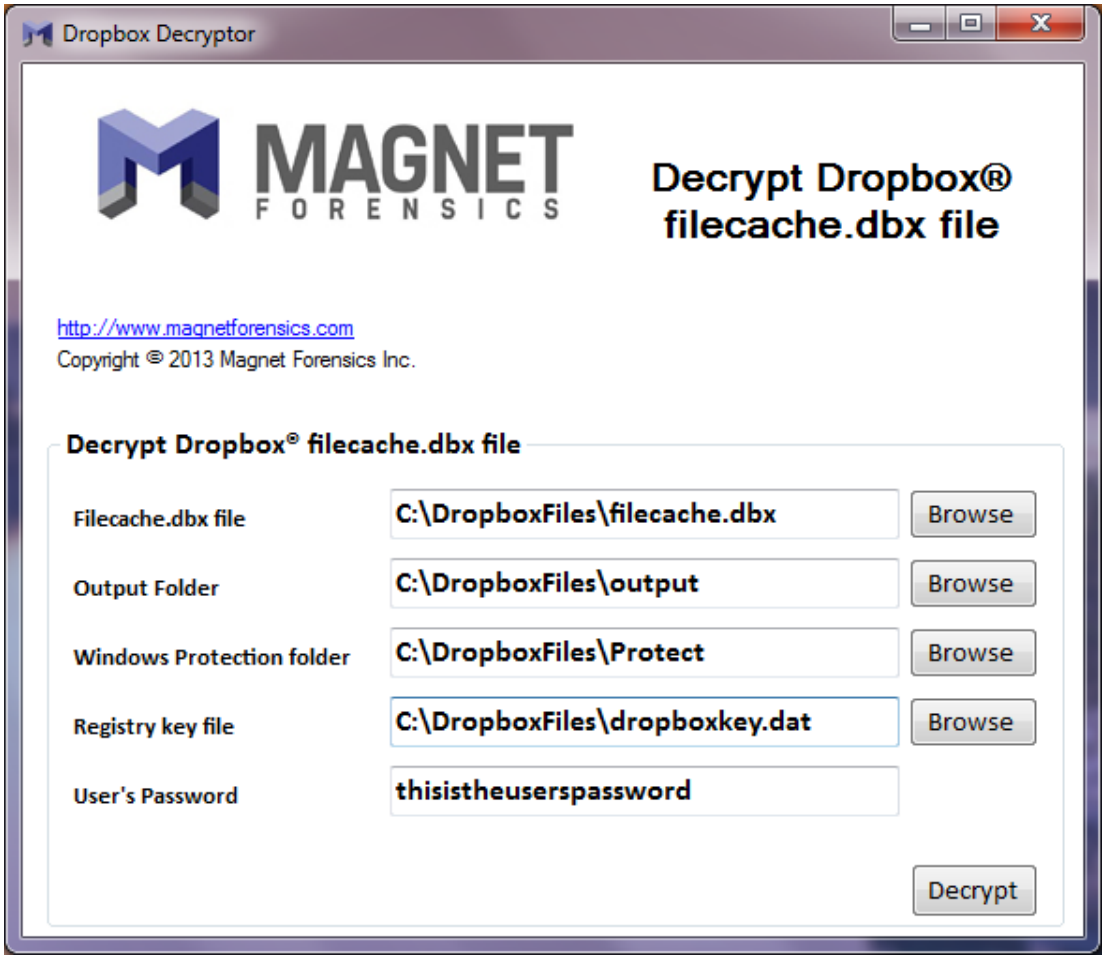
- A Critical Analysis of Dropbox Security를 발표한 newsoft 멤버가 개발
  - https://github.com/newsoft

- Tool
  - Dropbox DB Key Generator : dbx-keygen-windows/linux (Mac OS X는 없음)
  - DBX Decryptor : sqlite3-dbx

Tools (Online)

- 시연

Dropbox Decryptor (Offline)



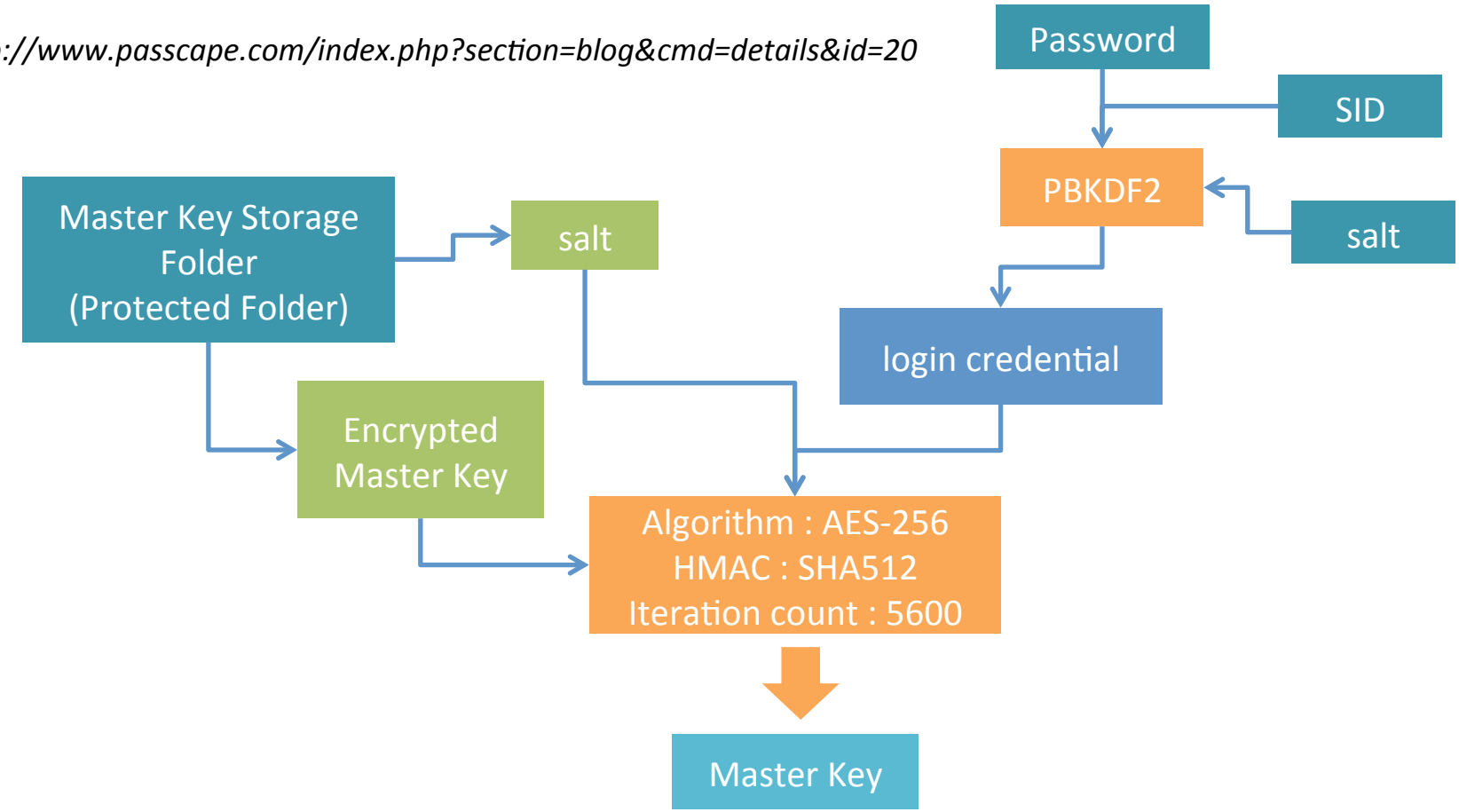
Dropbox Decryptor

- When/Who : March, 1, 2013, Magnet Forensics

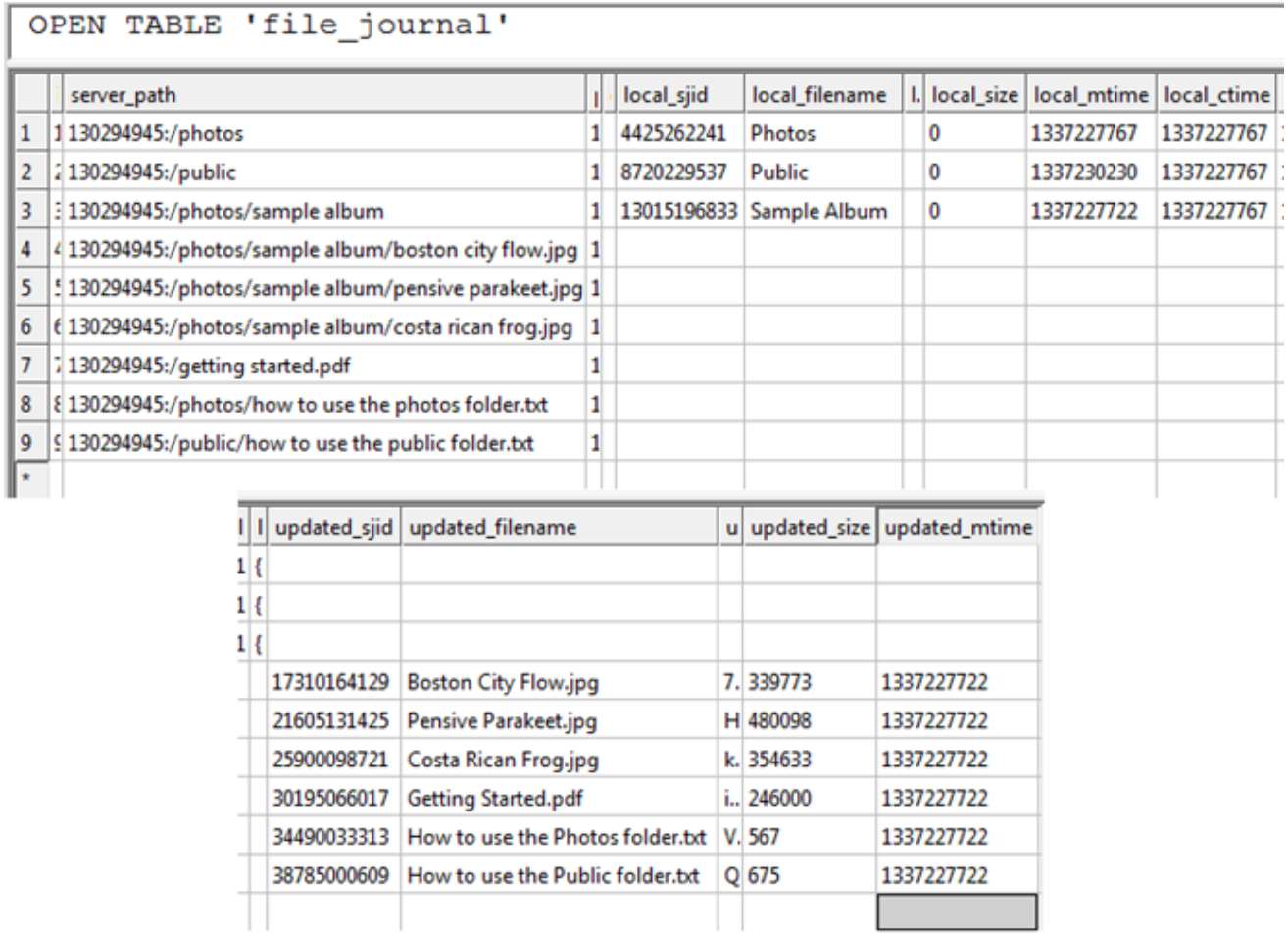
- Requirements
  - filecache.dbx file
    - [root]\Documents and Settings\username\Application Data\Dropbox on XP, or [root]\Users\Jad\AppData\Roaming\Dropbox on Vista
  - The entire protect folder for that user
    - [root]\Documents and Settings\username\Application Data\Microsoft on XP, or [root]\Users\Jad\AppData\Roaming\Microsoft on Vista/7
  - A file containing the raw bytes from the Dropbox 'client' value under the 'ks' key in registry
    - registry/NTUSER.dat file (full path is HKEY_CURRENT_USER\Software \Dropbox\ks
  - User's windows login password

Dropbox Decryptor CryptProtectData

http://www.passcape.com/index.php?section=blog&cmd=details&id=20



Dropbox Decryptor



```
OPEN TABLE 'file_journal'
```

	server_path	l	local_sjid	local_filename	l.	local_size	local_mtime	local_ctime
1	130294945:/photos	1	4425262241	Photos		0	1337227767	1337227767
2	130294945:/public	1	8720229537	Public		0	1337230230	1337227767
3	130294945:/photos/sample album	1	13015196833	Sample Album		0	1337227722	1337227767
4	130294945:/photos/sample album/boston city flow.jpg	1						
5	130294945:/photos/sample album/pensive parakeet.jpg	1						
6	130294945:/photos/sample album/costa rican frog.jpg	1						
7	130294945:/getting started.pdf	1						
8	130294945:/photos/how to use the photos folder.txt	1						
9	130294945:/public/how to use the public folder.txt	1						
*								

l	l	updated_sjid	updated_filename	u	updated_size	updated_mtime
1	{					
1	{					
1	{					
		17310164129	Boston City Flow.jpg	7.	339773	1337227722
		21605131425	Pensive Parakeet.jpg	H	480098	1337227722
		25900098721	Costa Rican Frog.jpg	k.	354633	1337227722
		30195066017	Getting Started.pdf	i..	246000	1337227722
		34490033313	How to use the Photos folder.txt	V.	567	1337227722
		38785000609	How to use the Public folder.txt	Q	675	1337227722

Q & A

Homepage : forensic.n0fate.com

E-Mail : n0fate@n0fate.com

Reference

- Florian LEDOUX,Nicolas RUFF. Application Security Forum 2012. A Critical Analysis Dropbox Security. 2012.
- Dhiru Kholia, Przemyslaw Wegrzyn. Looking inside the (Drop) box. 2013.