Journal of The Korea Institute of Information Security & Cryptology ISSN 1598-3986(Print)
VOL.28, NO.2, Apr. 2018 ISSN 2288-2715(Online)
https://doi.org/10.13089/JKIISC.2018.28.2.295

국내 스마트폰 제조사별 PC 백업 방법 분석 연구*

김 상 후,† 류 재 철‡
충남대학교

The Analysis of Smartphone Backup Method through PC*

Sangwho Kim,† Jae-Cheol Ryou‡
Chungnam National University

요 약

스마트폰은 전화, 문자와 같은 연락수단 외에도 일정관리, 문서작성, 카메라 등 다양한 기능을 이용할 수 있어 수많은 정보를 저장하게 되었다. 이러한 정보들은 개인정보와 같은 중요한 내용을 다수 포함하고 있기 때문에, 스마트폰 교체나 랜섬웨어와 같은 위협으로부터 대비하기 위하여 백업을 해두어야만 한다. 본 논문에서는 여러 백업 방법 중 PC를 이용한 방법에 대해 분석을 수행하고, 백업 파일로부터 연락처와 같은 개인정보가 유출될 수 있는 가능성을 확인한다. 이를 통해 PC 백업 방법의 문제점을 점검하거나, 보다 안전한 백업 기술을 강화하는데 활용할 수 있을 것으로 기대된다.

ABSTRACT

Smartphone can save many data because it provide various function such as call, message, calendar, document, camera, and so on. They include a number of important things like personal information. Thus it is necessary to backup the data to deal with smartphone change and a threat like ransomware. In this paper, we analyze the backup method using PC among several backup methods and check the possibility of leakage of personal information such as contacts from backup file. It is expected to be used to check the problems of the PC backup method or to strengthen the more secure backup technology.

Keywords: Smartphone Backup, File Encryption

I. 서 론

스마트폰은 휴대성이 좋고 다양한 기능을 이용할 수 있어 연락처뿐만 아니라 일정, 개인정보, 문서 등 중요 데이터들도 많이 저장이 되고 있다. 이러한 데이터들은 랜섬웨어 등의 위협으로부터 보호하고, 스마트폰을 교체해도 지속적인 사용을 위해 데이터 백업을 해두어야 한다.

스마트폰 내 데이터를 백업하는 방법은 크게 세 가지가 존재한다. 가장 기본적인 방법은 PC와 스마트폰을 USB 케이블로 연결하고, 제조사가 제공하는 백업프로그램을 이용하여 데이터를 백업하는 것이다. 다음은 클라우드 서비스를 이용하는 것으로 스마트폰이 네트워크에 반드시 연결되어 있어야 한다는 조건이 필요하다. 마지막은 가장 최근에 지원하기 시작한 방법으로 스마트폰에서 다른 스마트폰으로 바로 데이터를 백업 및 복원하는 방법이 있다. 이 경우 지원하는 스마트폰이 한정적이며 시간이 오래 걸린다는 특징이 있다. 본 논문에서는 세 가지 방법 중 가장 오래 전부터 사용되어 온 PC를 이용한 백업에 대한 분석 연구를 수행하였다. 분석을 위해 우선 각 백업 프로그램을 이용하여 스마트폰 내 데이터를 백업하였고, 이때 생성되는 백업파일들의 확장자, 포맷 등을

Received(11. 08. 2017), Modified(01. 08. 2018), Accepted(01. 10. 2018)
* 본 연구는 충남대학교 학술연구비에 의해 지원되었음
† 주저자, whoyas2@cnu.ac.kr
‡ 교신저자, jcryou@home.cnu.ac.kr(Corresponding author)

분석하였다. 필요 시 역공학을 통해 백업 프로그램 코드를 분석하였으며, 이를 통해 백업 파일 생성방법을 확인하고 백업파일로부터 원본 데이터 추출을 시도하였다.

국내에서 주로 사용되는 스마트폰 종류는 크게 안드로이드와 애플의 아이폰이 있으며, 안드로이드의 경우 국내 제조사 삼성, LG와 중국 제조사 샤오미, 화웨이 등이 있다. 본 논문에서는 각 제조사의 백업 방법과 관련된 연구 자료를 살펴보고, 국내 점유율이 가장 높은 삼성과 더불어 국내 제조사 LG 스마트폰 백업에 대한 분석 결과를 서술한다.

본 논문의 2장에서는 관련 연구에 대해 살펴본다. 3장과 4장에서는 삼성, LG의 스마트폰 백업 방법과 원본 데이터 복원 방법에 대해 살펴본다. 마지막으로 5장에서는 결론을 맺는다.

II. 관련 연구

과거 삼성은 "kies" 라는 프로그램 하나를 이용하여 스마트폰의 백업 및 복원 기능을 지원하였고, 백업 파일 포맷 및 원본 데이터 복원과 관련된 연구가 진행되었다[1][2]. 현재 삼성은 스마트폰 OS 및 기종에 따라 "kies2", "kies3", "smart switch" 세 가지 프로그램을 이용하며, 과거와는 다른 방법으로 데이터를 백업한다.

삼성의 경우 백업 파일 내 원본 데이터를 추출하는 SBU-Extractor라는 도구가 존재한다[6]. 이는 확장자 *.sbu 파일에서 원본을 추출하는데 *.sbu 파일의 경우 과거 kies에서 생성하던 백업 파일로 현재는 지원하지 않는 형식이다.

애플의 경우 "iTunes" 프로그램 하나로 백업 및 복원을 수행하며 관련 연구가 기존에 많이 진행되었다. 또한 ibackupBot 등과 같이 백업파일로부터 원본 데이터를 복원하여 사용자에게 보여주는 프로그램이 이미 여러 개 존재한다.

국내에서 사용되는 중국 스마트폰은 샤오미와 화웨이로 두 가지 제조사에서 생산한다. 샤오미의 경우 "Mi PC Suite" 프로그램을 이용하여 /data 하위 파일들을 git으로 관리한다. 화웨이는 "Hi Suite" 프로그램과 스마트폰 내 설치된 백업 앱을 함께 이용하며, PC에서 사용할 암호 키를 전달하여 암호화된 백업 파일을 받아온다.

백업파일에 관한 연구로는 암호화 기능에 대해서는 옵션으로만 제공하거나 제외하여 효율적으로 스마트폰 백업을 하는 것에 대한 논문[3], 기존의 백업 방법들을 분석하고, AES 암호를 이용한 안전한 백업 기술을 연구한 논문[4] 등이 발표되었다. 하지만 실제 기업들에서 제공하고 있는 백업 프로그램은 AES 암호와 동일하거나 그 이상 수준의 암호 기술을 적용하고 있으며, 그럼에도 불구하고 백업파일로부터 중요한 정보가 유출될 수 있는 가능성이 존재하는 상황이다.

스마트폰에서 이용되는 앱들의 데이터를 백업 및 복원에 대해 연구하는 내용도 있으나, 이러한 기술은 연락처, 메시지, 통화기록과 같은 정보가 아닌 써드파티(Third-party) 앱인 메신저 등에서 사용되는 데이터들을 안전하게 보관 및 관리하는 것으로 PC에 해당 데이터가 보관되는 경우는 거의 없다[5].

III. 삼성 스마트폰 백업

삼성은 스마트폰 OS 버전에 따라 kies2(안드로이드 4.3 미만), kies3(4.3 이상), smart switch(4.3 이상 & 갤럭시 s6 이후 모델) 프로그램을 이용하여 사용자가 선택한 데이터를 백업하며 각 프로그램은 하위 스마트폰 백업을 지원한다[7][8].

각 프로그램은 데이터 백업 및 복원과 디바이스 펌웨어 업그레이드 기능을 제공하며, kies2는 개인정보와 미디어 컨텐츠 관리, kies3은 미디어 컨텐츠 관리 기능을 추가로 제공한다.

3.1 백업 파일 특징

삼성 백업 프로그램은 스마트폰 내 데이터를 PC의 임시 폴더에 복사한 뒤, 백업 폴더 "C:\Users\[사용자명]\Documents\Samsung\[프로그램명]\Backup\[기기명]\[기기명_전화번호]\[기기명_백업날짜시간]" 에 암호화하여 저장하고 임시 폴더를 삭제한다. 백업 폴더 경로는 백업 프로그램을 통해 사용자가 설정할 수 있다.

백업되는 데이터 중 연락처, 메시지, 통화기록, 알람, 일정 등의 개인정보는 암호화되어 저장되고, 사진, 동영상 등의 멀티미디어 파일과 이메일, 스마트폰 환경설정 정보는 원본으로 저장된다.

Fig.1.은 동일한 컨텐츠를 각 프로그램을 통해 생성한 백업파일의 구조를 비교한 그림으로 붉은색으로 칠해진 부분은 서로 다른 부분을 나타낸 것이다. 우선 kies2와 kies3의 백업파일을 비교한 결과 두 파

Fig. 1. Backup file compare result

일의 공통점이 나타나지 않았으며 kies3으로 백업한 파일의 크기가 더 작은것을 알 수 있다. 그러나 kies3와 smart switch의 백업 파일은 크기와 구조가 동일하며 일부 공통된 부분이 나타나는것을 볼 수 있다. 이를 통해 kies3 이후로 암호화 방법 또는 암호화 시 필요한 정보와 파일 포맷이 달라졌으며, kies3과 smart switch는 동일한 방식을 사용하고 프로그램에 따라 차이점이 존재함을 유추할 수 있다.

또한 데이터 백업 시 "BackupHistory.xml" 파일이 함께 저장되는데, 이 파일에는 Fig.2.와 같이 스마트폰 모델명, 전화번호, 시리얼넘버, IMEI 등의 스마트기기 정보와 백업 폴더 경로, 백업 파일 종류, 개수, 크기 등의 백업 파일의 정보가 저장된다.

```
<UserInputName>SHV-E210K</UserInputName>
<ModelName>SHV-E210K</ModelName>
<SavedTime>2016-07-27T23:21:01.5219127+09:00</SavedTime>
<LoadedTime>0001-01-01T00:00:00</LoadedTime>
<PhoneNumber>010[redacted]</PhoneNumber>
...
<FileName>Contacts.spb</FileName>
<Type>Contacts</Type>
<ItemsCount>6</ItemsCount>
<AccountCount>0</AccountCount>
<FileSize>18224</FileSize>
```

Fig. 2. Contents of BackupHistory.xml

3.2 백업 파일 분석

Kies2에는 스마트폰 내 연락처 및 PC에 암호화되어 저장된 연락처 백업 파일을 수정하는 기능을 제공하는데, 이때 Kies3과 smart switch의 백업 파일 또한 수정 가능하다. 즉, kies2 분석을 통해 kies3과 smart switch에서 사용하는 암호화 관련 정보를 확인할 수 있음을 알 수 있다.

kies2 프로그램 분석을 통해 확인한 결과 삼성 백업프로그램들은 파일 암호화에 Fig.3.과 같이 고정된 키와 IV(Inivial Vector), 알고리즘(AES-256)을 사용하며, 백업 프로그램에 따라 패딩과 블록 크기를 다르게 설정한다.

위 정보를 이용하여 백업 파일을 복호화하면

```
public StreamCrypto(string filePath)
{
    this._filePath = filePath;
    this._key = Encoding.ASCII.GetBytes("ep[redacted]");
    this._iv = Encoding.ASCII.GetBytes("af[redacted]");
    this._byteArray = new byte[272];
}
```

Fig. 3. Samsung Encryption key & IV

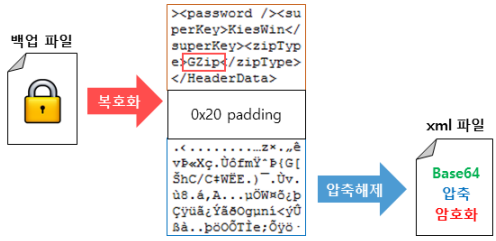

Fig. 4. Decrypt result

Fig.4.와 같이 zip 또는 gzip으로 압축된 파일과 관련 정보가 저장된 xml파일을 추출해 낼 수 있다.

압축 파일 내부에는 또 다른 xml 파일이 저장되어 있으며, Table 1.의 데이터 종류에 따라 Base64, 압축, 암호화가 추가 적용되어 있다.

추가 암호화는 AES-128이 사용되며 암호키는 Fig.5.와 같이 1차 복원으로 추출한 xml 파일 내 저장된 세션키의 SHA256 해시값이고, IV는 2차 복원 대상 암호 파일의 첫 16바이트에 해당한다.

Table 1. Backup and Restore step

1st step	2nd step	File type
-	-	Multimedia Email.bk Configuration.bk
AES 256	-	Contacts.spb
	Base64	Message.sme Splanner.ssc Smemo.ssm
	Base64 UNZIP	Wallpaper.swp WIFI.swl LockScreen.ssm
	Base64 UNZIP AES128	Alarm.sal Calllog.scl

```
<SessionKey>0b1e96db05d64ea4</SessionKey>
```

Fig. 5. SessionKey for 2nd step

3.3 원본 파일 복원

• **1차 복원 - 복호화**

우선 코드 내 저장된 암호키와 IV를 이용하여 백업 파일을 복호화 한다. 그 결과 xml 파일과 압축 파일이 추출되며, xml 내 저장된 압축방식을 이용하여 압축을 해제한다. 이렇게 하여 Fig.6.과 같이 실제 데이터가 저장된 xml 파일을 복원할 수 있다.

Fig. 6. "Contacts.spb" decrypt result

• **2차 복원 - Base64 디코딩**

복원된 xml 파일에는 Fig.7.과 같이 일부 데이터가 Base64로 인코딩 되어있다. 이 부분은 디코딩을 통해 간단히 복원할 수 있다.

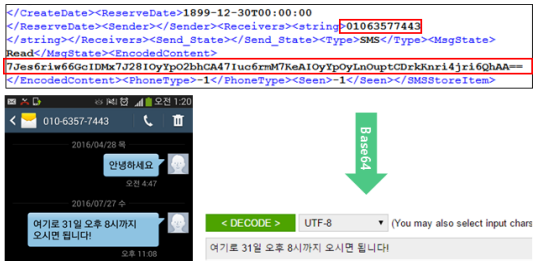

Fig. 7. "Message.sme" decrypt result

• **2차 복원 - 압축 해제**

xml 파일 내용 중 Fig.8.과 같이 〈FileContent〉 태그에 저장되는 값을 Base64 디코딩을 하면 zip 파일을 얻을 수 있다. 해당 zip 파일을 압축해제 하면 xml 파일 또는 암호화된 exml 파일을 추출할 수 있다. 만약 압축된 파일이 exml 인 경우 해당 파일 복호화에 필요한 세션키가 xml 파일 하단에 저장되어 있다.

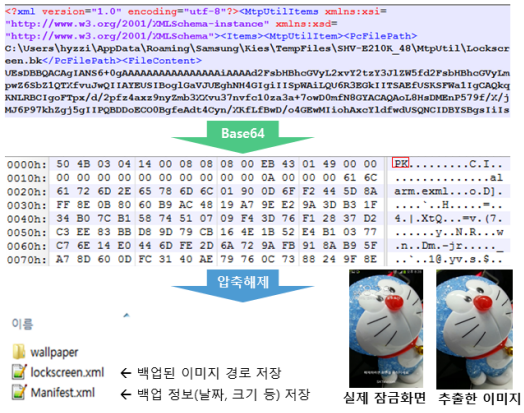

Fig. 8. "LockScreen.sme" decrypt result

• **2차 복원 - 복호화**

압축 해제로 추출된 파일이 exml인 경우 복호화가 필요하다. 이때 암/복호키는 앞서 xml 파일 내 저장된 세션키의 SHA256 해시값이며, IV는 exml 파일의 첫 16바이트이다. 이렇게 exml 파일을 복호화하면 Fig.9.처럼 원본 데이터를 추출할 수 있다.

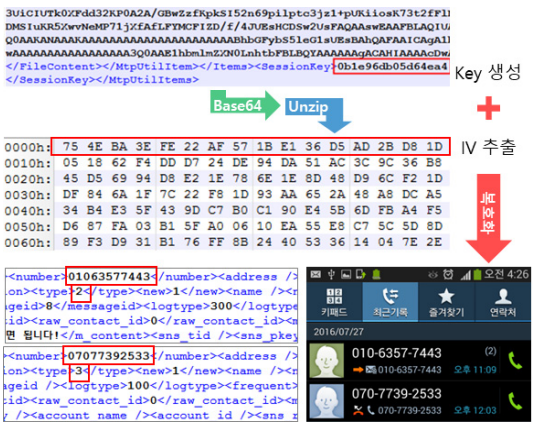

Fig. 9. "Calllog.scl" decrypt result

IV. LG 스마트폰 백업

LG는 스마트폰의 OS 버전에 따라 LG Mobile Sync(4.0 미만, 피쳐폰 데이터 동기화), LG PC Suite(5.0 미만), LG Bridge(G Stylo 이후 모델) 프로그램을 이용한다[9][10]. 특히 LG Mobile Sync 프로그램의 경우 피쳐폰의 데이터를 동기화하는데 특화되어 있으므로 분석대상에서 제외

하였다.

4.1 LG PC Suite

LG PC Suite 프로그램은 미디어 파일 전송, 데이터 백업 및 복원 기능을 지원하며, 데이터 백업의 경우 일부 데이터만 백업하는 카테고리 백업과 전체 백업을 지원한다. 백업 데이터는 C:\Users\{사용자}\Documents\LG PC Suite\backup\{모델명}\{백업날짜T백업시간} 폴더 내 저장되며 백업 프로그램을 통해 사용자가 백업 파일 저장 경로를 변경할 수 있다.

- **카테고리 백업**

카테고리 백업의 경우 연락처, 일정, 북마크, 메시지 중 선택한 데이터를 백업하며 백업 요청 시 원본 파일을 PC에 저장한 후 이를 암호화하여 확장자 ".ecbk"로 저장한다. 또한 PCSuite_ backup_{백업날짜시간}.idx 파일이 함께 저장되어 Fig.10.과 같이 스마트폰 모델명, 백업 데이터 종류 등을 알 수 있다.

카테고리 백업 시 dll 파일이 로드되는데 해당 파일에는 백업 파일 암/복호화에 사용되는 루틴이 저장되어 있다. 백업 파일은 AES-128-CBC 암호화 되어 있으며 Fig.11.과 같이 코드 내 저장된 고정 키와 16개의 null 바이트로 이루어진 IV를 이용한다.

따라서 위 정보를 이용하여 백업 파일을 복호화하면 Fig.12.와 같이 원본 데이터를 손쉽게 추출할 수 있다.

```
<Backup Version="2.1">
    <General>
        <Date>42669.7804282407</Date>
        <Model>LG-F350K</Model>
    </General>
    <Contact>
        <Path>\PCSuite_backup_20161026T184349\Contact
    </Contact>
```

Fig. 10. Contents of ".idx" file

```
sub_10087A20(&v6);
v10 = 0;
sub_10087A40((int)"aK[redacted]", off_1010943C, 16, 0x10u);
memcpy(&v7, &v8, v7);
sub_10088C80((int)v2, v4, a2, 1);
v10 = -1;
sub_10087A30();
return v4;
```

Fig. 11. LG Encryption key & IV

Contact.ecbk

B0	FC	AD	3A	D7	98	45	FF	3F	0B	23	53	0D	15	DC	86
9A	A5	FE	90	83	44	57	5F	2B	D1	33	60	36	40	0A	35
68	C8	7F	48	DE	C7	3C	38	24	13	41	A1	50	86	9C	9D
CB	8D	43	60	EB	48	C2	E3	AC	0D	AD	08	7F	7B	1C	01

Contact 원본

```
BEGIN:VCARD
PRODID:X-MLVERSION-2.0
VERSION:2.1
N;ENCODING=QUOTED-PRINTABLE;CHARSET=utf-8:;=EC=98
TEL;WORK;VOICE;CHARSET=utf-8:100
```

Fig. 12. Contact.ecbk decrypt result

- **전체 백업**

전체 백업의 경우 Fig.13.과 같이 스마트폰 리커버리 모드에 진입하여 /data 경로 내 모든 파일을 암호화 하여 결과를 PC로 전송한다.

암호화된 백업파일의 확장자는 ".tar.enc", "tar.gz.enc"이며, 전체 백업 시 스마트폰 모델명과 버전, 백업 날짜 및 시간, 구글 계정이 포함된 Fig.14.의 PCSuite_FB_{백업날짜시간}.brinfo 파일과 백업된 원본 파일명이 포함된 filenames 파일이 암호화되어 함께 저장된다.

리커버리 모드 진입 후 백업 시 사용되는 파일 "brd"에는 파일 암호에 사용되는 루틴이 존재한다. LG PC Suite를 이용하여 전체 백업을 할 때에는 AES-128-ECB가 사용되며 암호키는 Fig.15.와 같이 구글 계정으로부터 생성되고 IV는 16바이트의 null 값이다. 연산에는 여러 번의 shift 연산이 사용된다.

전체 백업 파일을 복호화하기에 앞서 filenames 파일을 복호화 한 결과 아래 Fig.16.과 같이 /data

```
root      198   1     648   256   ffffffff 00000000 S /sbin/ueventd
root      200   1     1432  4     ffffffff 00000000 S /sbin/healthd
root      201   1     29744 18160 ffffffff 00000000 S /sbin/recovery
shell     202   1     5680  180   ffffffff 00000000 S /sbin/adbd
root      203   1     1612  272   ffffffff 00000000 S /sbin/brd
root      207   2     0     0     ffffffff 00000000 S jbd2/mmcblk0p38
root      208   2     0     0     ffffffff 00000000 S ext4-dio-unwrit
root      211   2     0     0     ffffffff 00000000 D mdss_fb0
root      214   2     0     0     ffffffff 00000000 S flush-179:0
root      215   2     0     0     ffffffff 00000000 S jbd2/mmcblk0p34
root      216   2     0     0     ffffffff 00000000 S ext4-dio-unwrit
shell     280   202   932   472   c010a270 b6f0f354 S /system/bin/sh
shell     286   280   1244  236   00000000 b6f3650c R ps
shell@bi:/ $
```

Fig. 13. Backup in android recovery

```
<BRDataInfo>
    <ModelName>LG-F350K</ModelName>
    <DN>44829,46587,43071,46587,42192,50103,42192
    <BDate>2016-10-27T00:08:48</BDate>
    <BRType>Full_ADB_RECOVER</BRType>
    <AndVer>4.4.2</AndVer>
    <RDate></RDate>
    <Account>rk[redacted]</Account>
```

Fig. 14. Contents of ".brinfo" file

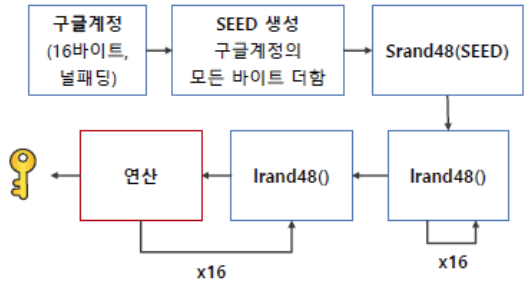

Fig. 15. Encrypt key generation

```
1 /data/app
2 /data/app/LGCounselingbin.apk
3 /data/app/LGHome3_Theme_Marshmallow.apk
4 /data/app/LGMeChatEngine.apk
5 /data/app/sensor_ctl_socket
```

Fig. 16. "filenames" file decrypt result

하위 경로의 파일명들을 볼 수 있다.

Fig.17.은 전체 백업 파일 중 일부를 복호화 한 결과로 /data/app과 /data/data 하위 경로의 파일들을 tar 파일로 백업한 것을 확인할 수 있다.

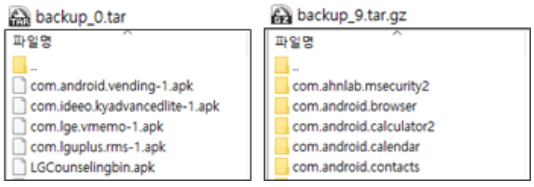

Fig. 17. LG Backup file decrypt result

4.2 LG Bridge

LG Bridge는 데이터 백업, 소프트웨어 업데이트 기능을 지원하며 데이터 백업 시 스마트폰 내 설치된 LG 백업 앱을 통해 백업 파일(.lbf)을 생성하며 결과 파일을 PC로 전송한다.

화면, 설정, 개인 데이터, 어플리케이션, 미디어 데이터를 선택해서 백업할 수 있으며, C:\Users\〔사용자〕\Documents\LG Bridge\BackupDataFile\〔LGBackup_날짜_시간^01.lbf〕에 저장된다. 해당 경로 역시 사용자가 백업 프로그램을 이용하여 변경 할 수 있다.

LG Bridge로 백업 시 데이터들이 ".lbf" 파일 하나에 저장되는데, 이 파일의 경우 백업을 선택한 데이터 원본이 이어 붙어있는 형태로 각각을 잘라내어 따로 저장하면 Fig.18.과 같이 SQLite 브라우저를

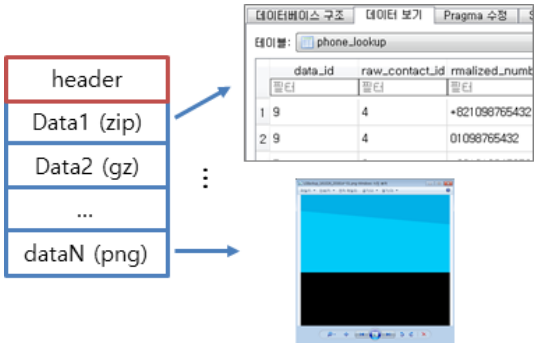

Fig. 18. Data from LG backup file

통해 DB의 내용을 추출 및 확인할 수 있다〔11〕.

V. 결 론

본 논문에서는 국내 스마트폰 제조사 별 백업 방법에 대해 분석하고, 그 중 PC 백업 방법을 통해 생성된 파일들로부터 원본 데이터의 추출 가능성을 분석해보았다. 먼저 삼성의 경우 스마트폰 OS 및 기종에 따라 세 가지 프로그램을 이용하며, 각각은 동일한 알고리즘을 이용하나 블록 사이즈 및 패딩 종류가 다르며, 사용되는 키와 IV는 백업 프로그램 또는 백업 파일 내에서 찾을 수 있는 것을 확인하였다. LG 또한 세 가지 프로그램을 이용하며 삼성과 달리 각각 다른 방법을 이용하여 백업을 수행하는 것을 확인할 수 있었다. 하지만 LG 역시 백업 파일 암호화에 사용되는 키와 IV 정보를 백업 프로그램 또는 백업 정보 파일 내에서 찾을 수 있었으며, 한 프로그램의 경우 암호화를 수행하지 않는 것을 확인하였다. 즉, 국내 스마트폰 제조사의 PC 백업 방법에 사용되는 백업 프로그램 분석을 통해 백업파일 생성 과정, 파일 암호화에 사용되는 키, 알고리즘 정보를 파악할 수 있었으며, 이를 통해 PC에 남아있는 임의의 백업 파일로부터 복호화 과정을 통해 연락처 같은 중요 정보의 추출이 가능한 것을 확인하였다.

References

〔1〕 Gyuwon Lee, Hyunuk Hwang, Kibom Kim and Taejoo Chang . "Analysis Scheme on Backup Files of Samsung Smartphone available in Forensic." KIPS Transactions on Computer and

Communication Systems, 2(8), pp. 349-356, Aug. 2013
〔2〕 Woo-Sung Chun and Dea-Woo Park, "A Study of Vulnerability Analysis and Mobile Forensic Technology about Android/Windows Mobile Smart Phone" Proceedings of the Korean Society of Computer Information Conference, 19(2), pp. 192-195, June. 2011
〔3〕 Medhavi S.Shriwas, Neetesh Gupta and Amit Sinhal, "Efficient Method for Backup and Restore Data in Android" International Conference on Communication Systems and Network Technologies, pp. 693-697, April. 2013
〔4〕 Pratap P. Nayadkar, "Automatic and secured backup and restore technique in android" IEEE Sponsored 2nd International Conference on Innovations in Information Embedded and Communication Systems, pp. 1-4, March. 2015
〔5〕 Anupam Shukla, Prashant Shrivastava, Prateek Yadav and Alok Kumar, "Backup manager-An Android application for storing messages and apps information online", Proceedings of 2015 Global Conference on Communication Technologies, pp. 45-48, April. 2015.
〔6〕 SBU-Extractor, https://github.com/Luncher91/SBU-Extractor/
〔7〕 Samsung Kies, http://local.sec.samsung.com/comLocal/support/down/kies_main.do?kind=kies
〔8〕 Samsung Smart Switch, http://www.samsung.com/sec/support/smartswitch/smartswitch.html
〔9〕 LG PC Suite, http://www.lge.co.kr/lgekor/download-center/softwareMenualPopup.do?swCatRegNo=193&mdlNo=425&winSwRegNo=252&macSwRegNo=259&pgmName=LG%20PC%20Suite
〔10〕 LG Bridge, http://www.lge.co.kr/lgekor/download-center/softwareMenualPopup.do?swCatRegNo=195&mdlNo=1044&winSwRegNo=262&macSwRegNo=263&pgmName=LG%20Bridge
〔11〕 DB Browser for SQLite, http://sqlitebrowser.org/

〈저자소개〉

김 상 후 (Sangwho Kim) 정회원
2014년 2월: 충남대학교 컴퓨터공학과 졸업
2016년 2월: 충남대학교 컴퓨터공학과 석사
2016년 3월~현재: 충남대학교 컴퓨터공학과 박사과정
〈관심분야〉 시스템보안, 모바일보안, 취약점분석

류 재 철 (Jae-Cheol Ryou) 종신회원
1985년 2월: 한양대학교 산업공학과 졸업
1988년 5월: Iowa State University 전산학 석사
1990년 12월: Northwestern University 전산학 박사
1991년 2월~현재: 충남대학교 컴퓨터공학과 교수
〈관심분야〉 정보보호, 인터넷보안, 암호학, 보안프로토콜