http://dx.doi.org/10.3745/KTCCS.2013.2.8.349

Analysis Scheme on Backup Files of Samsung Smartphone available in Forensic

Gyuwon Lee† · Hyunuk Hwang†† · Kibom Kim†† · Taejoo Chang†††

ABSTRACT

As various features of the smartphone have been used, a lot of information have been stored in the smartphone, including the user's personal information. However, a frequent update of the operating system and applications may cause a loss of data and a risk of missing important personal data. Thus, the importance of data backup is significantly increasing. Many users employ the backup feature to store their data securely. However, in the point of forensic view these backup files are considered as important objects for investigation when issued hiding of smartphone or intentional deletion on data of smartphone. Therefore, in this paper we propose a scheme that analyze structure and restore data for Kies backup files of Samsung smartphone which has the highest share of the smartphone in the world. As the experimental results, the suggested scheme shows that the various types of files are analyzed and extracted from those backup files compared to other tools.

Keywords : Samsung Smartphone, Kies Backup File, Electronic Information, Personal Information

포렌식에서 활용 가능한 삼성 스마트폰 백업 파일 분석 기법

이 규 원† · 황 현 욱†† · 김 기 범†† · 장 태 주†††

요 약

스마트폰의 다양한 기능들이 사용되면서 사용자의 개인정보를 비롯한 대용량의 데이터들이 스마트폰에 저장되고 있다. 그러나 운영체제와 어플리케이션의 잦은 업데이트는 데이터의 손실을 야기할 수 있으며, 개인의 소중한 데이터를 분실할 위험성을 갖게 한다. 이로 인하여 데이터의 백업에 대한 중요성이 크게 증가하였으며 많은 사용자들이 자신의 데이터를 안전하게 보관하기 위해 백업 기능을 사용하고 있다. 그러나 포렌식 관점에서 이 백업 파일들은 스마트폰의 은닉 및 데이터의 고의 삭제시 중요한 수사 대상이 된다. 따라서, 이 논문에서는 세계에서 스마트폰 점유율이 가장 높은 삼성 스마트폰의 Kies 백업 파일에 대한 구조를 분석하고, 백업 파일을 복원하는 기법을 제안한다. 실험 결과 제안된 기법은 다양한 유형의 파일들을 분석하여 타 도구들 대비 높은 파일 추출 결과를 보였다.

키워드 : 삼성 스마트폰, Kies 백업 파일, 전자정보, 개인정보

1. 서 론

세계적인 리서치 자문기관인 가트너(Gartner, Inc.)[1]의 발표에 의하면 삼성은 2012년 세계 스마트폰 시장 점유율에서 1위를 차지했으며, 2013년 1분기에서도 점유율 30.8%로 독주 체제를 이어가고 있다. 반면 애플의 경우 점유율 18.2%로 그 뒤를 따르고 있으며, 기타 다른 업체들의 경우 점유율 5% 미만으로 삼성, 애플에 비해 상대적으로 낮은 점유율을 차지하고 있다.

스마트폰 시장은 꾸준한 상승세를 이어가고 있으며, 스마트폰의 성능이 향상되고 용량이 증가하면서 다양한 기능들이 스마트폰에 추가되고 있다. 또한 마켓을 통한 제조사 및 제3(Third-Party)의 다양한 앱들이 사용자들에 의해 다용도로 사용되면서 연락처, 메시지, 통화 이력, 메모, 일정, 계정 정보 등 개인정보와 음악, 사진, 동영상 등 대용량의 데이터들이 스마트폰에 저장되고 있다. 그러나 운영체제 및 어플리케이션의 잦은 업데이트는 데이터의 손실을 야기할 수 있으며, 스마트폰의 분실은 개인의 소중한 데이터를 잃어버리게 할 위험성을 갖게 한다. 그래서 많은 사용자들이 자신의 데이터를 안전하게 보관하기 위해 벤더(Vendor)에서 제공하는 백업 기능을 사용하고 있으며, 문제 발생시 백업으로부

† 정 회 원 : 한국전자통신연구원 부설연구소 연구원
†† 정 회 원 : 한국전자통신연구원 부설연구소 선임연구원
††† 정 회 원 : 한국전자통신연구원 부설연구소 책임연구원
논문접수 : 2013년 4월 23일
수 정 일 : 1차 2013년 6월 7일
심사완료 : 2013년 6월 27일
* Corresponding Author : Gyuwon Lee(gwlee79@gmail.com)

터 데이터를 복원할 수 있게 되었다. 백업 방법은 크게 세 가지로 분류되며 앱(App)을 이용한 방법[2-5]과 클라우드 서비스를 이용한 방법[6-10] 그리고 PC 동기화 프로그램을 이용한 방법[11-12]이 사용되고 있다. 이 중 PC 동기화 프로그램을 이용한 방법은 손쉬운 사용법과 USB 연결만으로 스마트폰에 존재하는 대부분의 데이터를 백업할 수 있는 장점 때문에 많은 사용자들이 이 방법을 사용하고 있다. 그러므로, 이 논문에서는 PC 동기화 프로그램을 이용한 백업 방법을 분석 대상으로 하였다.

반면, 포렌식 관점에서 PC에 저장된 백업 파일들은 특정 사건에 대한 용의자의 스마트폰 은닉 및 스마트폰 데이터에 대한 고의 삭제 등 안티 포렌식(Anti-forensic)[1]에 대한 대응을 가능하게 하며, 백업 파일로부터 복원된 원본 파일들은 사건 해결에 필요한 중요한 단서가 될 수 있다. 그러므로, 백업 파일을 복원하는 연구는 매우 중요하다고 볼 수 있다.

초기 애플의 혁신적인 스마트폰 출시로 인하여 아이폰 백업 파일에 대한 분석은 많은 연구가 진행되었으나 현재 가장 많이 사용되고 있는 삼성 스마트폰 백업 파일에 대한 분석은 상대적으로 부족한 실정이다. 따라서, 이 논문에서는 백업 파일 분석 관련 기존 연구를 살펴보고, 세계 스마트폰 시장에서 점유율이 가장 높은 삼성 Kies 백업 파일에 대한 분석 기법을 제안한다.

논문의 구성은 다음과 같다. 2장에서 관련 연구를 살펴보고, 3장에서 Kies 백업 파일 구조를 분석한다. 그리고 4장에서 Kies 백업 파일 복원 기법을 제안하고 5장에서 실험 및 평가를 한다. 마지막으로 6장에서 결론을 맺는다.

2. 관련 연구

애플의 iTunes[11] 백업 파일에 대한 분석 기법은 여러 연구들이 진행되었다. 반면, 삼성 Kies[12] 백업 파일에 대한 분석 기법은 아직 공개되지 않고 있으며, 데이터를 추출하는 프로젝트[13-14]가 일부 진행 중에 있다.

Bader[15] 등은 애플의 iPhone 3GS 환경에서 iTunes 백업 유틸리티를 이용한 논리적인 분석을 수행하였다. 그들은 iTunes 백업 폴더에 위치한 mdinfo와 mddata 파일들로부터 SQLite 데이터베이스 파일들과 Plist 파일들을 복원하여 해당 파일들을 분석하였으며, 스마트폰 백업 파일 분석에 대한 초기 포렌식 연구로써 의미 있는 연구를 하였다.

Clinton[16] 등은 iOS 4.x에서 백업 파일을 저장하는 방식에 변화가 있음을 밝혀냈다. iOS 3.x 버전에서 사용되던 "mddata" 확장자가 모두 제거되었으며, mdinfo 파일에서 제공되던 백업 파일의 정보는 mbdx와 mbdb에서 제공하도록 변경되었다. mbdx는 백업된 파일의 이름과 해당 파일의 mbdb 데이터 파일의 오프셋 정보를 가지고 있으며, mbdb는 원본 파일의 경로 및 데이터 해시, 도메인 등의 파일 정보를 포함하고 있다. 그들은 mbdx와 mbdb 정보를 이용하여 원본 파일을 복원 및 분석하였다.

B. Satish[17]는 iOS 5.0.1(iPhone 4 GSM 모델)에서 iTunes 백업으로부터 데이터 추출에 대한 연구를 하였다. iOS 5.x에서는 기존에 사용되었던 mbdx 파일이 더 이상 사용되지 않으며, 그가 소개한 유틸리티들[18-20]은 mbdb에 저장된 정보를 파싱(parsing)하여 원본 파일을 복원 및 분석하였다. Mbdb 파일은 iOS 6.x에서도 동일한 구조를 가지고 있으므로 B. Satish의 방법은 iOS 6.x에서 동일하게 동작된다.

Armomurha[13]는 삼성의 Kies 백업 파일로부터 연락처(VCard) 정보를 추출하는 자바 프로그램을 개발 및 제공하였다. 그러나 이 프로그램은 연락처 정보를 제외한 개인정보, 콘텐츠, 설정 및 계정 정보에 대해서 추출하도록 설계되지 않았다.

Andreas[14]에 의해서 제공된 프로그램은 개인정보의 연락처, S 플래너, 콘텐츠의 음악, 사진, 동영상, 그 외 콘텐츠 파일을 추출할 수 있다. 그러나 개인정보의 S 메모, 미니 다이어리, 통화이력 설정 및 계정 정보의 환경설정 및 벨소리, 네트워크 설정 및 북마크 그리고 이메일 계정 정보를 추출하지 못한다.

3. Kies 백업 파일 구조 분석

저자는 Kies 백업 파일에 대한 구조를 분석하려면 먼저 백업 파일을 수집해야 한다. 삼성 스마트폰과 PC간 동기화 프로그램인 Kies 프로그램을 이용하면 스마트폰에 존재하는 개인정보, 콘텐츠, 계정 정보 및 설정 정보들이 PC에 백업된다. 백업 파일은 "백업 날짜T시간.sbu(20130301T190606.sbu)" 형태로 저장되며, 운영체제 별로 저장되는 경로가 다르다. 사용자가 경로를 변경 할 수 있지만 기본적인 백업 경로는 Table 1과 같다.

Kies 백업 파일에 대한 구조는 아직까지 공개되지 않고 있다. 그러므로 이 장에서는 여러 백업 파일(*.sbu)들을 비교 분석하여 Kies 백업 파일의 구조를 분석한다. Kies 백업 파일 구조(Structure of Kies backup file)는 Fig. 1과 같다.

파일 헤더(File header)는 시그니처(Signature), 디바이스 정보(Device information), 언어(Language)로 구성되어 있으며, 디바이스 정보는 운영체제, IMEI, 모델 번호를 포함하고 있다. 메타데이터 정보 영역(Area of metadata information)에는 백업 항목에 대한 메타데이터 정보(Metadata

Table 1. Path of backup file

OS	Path
Windows XP	C:\Documents and Settings\{UserName}\My Documents\samsung\Kies\Backup\ModelName
Windows Vista/7	C:\Users\{UserName}\Documents\samsung\Kies\Backup\ModelName

1) 안티 포렌식(Anti-forensic): 포렌식을 방해하는 행위

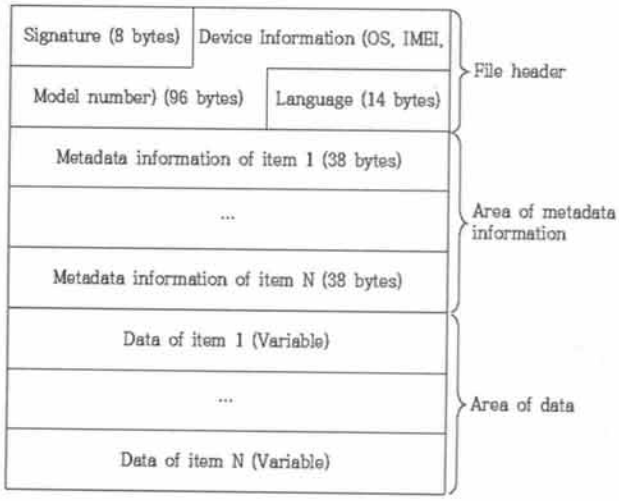

Fig. 1. Structure of Kies backup file

Signature (16 bytes)	
Starting offset of data area (8 bytes)	
Size of data area (8 bytes)	
Number of content files (4 bytes)	Type of data (2 bytes)

Fig. 2. Structure of metadata information

information of item)가 38 바이트 레코드 단위로 존재하고, 데이터 영역(Area of data)에는 각 백업 항목에 대한 데이터(Data of item)들이 존재한다.

백업 항목에 대한 메타데이터 정보 구조(Structure of metadata information)는 Fig. 2와 같다. Signature는 백업 항목별 시그니처 정보이고, Starting offset of data area는 데이터 영역의 시작 오프셋이며, Size of data area는 데이터 영역의 크기를 나타낸다. Number of content files는 데이터 영역에 존재하는 콘텐츠 파일의 수를 의미하고, Type of data는 데이터 종류로써 데이터가 콘텐츠(0x00)인지 아닌지(0x02)를 나타낸다.

백업 항목(Item)에는 연락처(Contacts), S 플래너(S Planner), 메시지(Messages), S 메모(S Memo), 미니 다이어리(Mini diary), 통화 이력(Call log), 음악(Music), 사진(Photos), 동영상(Videos), 그 외 콘텐츠(Miscellaneous content files), 환경 설정 및 벨소리(Preferences and ringtones), 네트워크 설정 및 북마크(Network settings and bookmarks), 이메일 계정 정보(Email account information)가 존재하며, 각 백업 항목별 시그니처 정보가 존재한다. Table 2는 백업 항목의 시그니처 정보를 나타낸다. 각 항목별로 시그니처 정보가 고정되어 있으며, 16바이트 각각의 시그니처 정보는 연락처의 휴대폰과 계정, S 플래너의 일정과 할 일, 메시지 등 각각의 항목을 대표한다. 데이터 영역의 시작 오프셋에 각 백업 항목별 시그니처 정보가 존재하므로 각 항목에 대한 비교 검증 시 이 정보를 활용한다.

백업 항목에 대한 데이터 구조(Data structure of item)는 Fig. 3과 같다. Signature는 백업 항목별 시그니처 정보이고, Type of data는 데이터의 종류를 나타내며, Size of data는 데이터의 크기를 나타낸다. Length of standard string은 "Standard 2.0"과 같은 표준 문자열의 길이를 나타내고, Data는 백업 항목에 대한 데이터를 나타낸다.

Signature (16 bytes)	
Type of data(6 bytes)	Size of data(8 bytes)
Length of standard string(8 bytes)	Size of data(8 bytes)
Length of standard string(8 bytes)	Data(Variable)

Fig. 3. Data structure of item

Table 2. Signature information of Item

Item		Signature	Etc
Personal information	Contacts	B8 17 5A 8C 86 4C 45 06 9B 50 0C C8 88 28 EE 2E	Phone
		DC DD F4 76 76 31 41 EF 85 B0 D8 A1 56 AB ED FF	Account
	S Planner	ED 25 8D DE FF 89 4C 43 86 FA BC AE 90 93 19 5E	Schedule
		31 DC 09 40 8E 01 4C B4 91 C4 16 68 01 F8 3F 17	To do
	Messages	04 9B A2 D7 EA 67 4A 23 BA E4 FD 93 10 1F D9 E0	
	S Memo	10 95 F4 ED CE E0 45 A0 A9 CC F6 D4 8F CF 60 35	
	Mini diary	1A 1E E8 34 EF CE 42 5F 9C 57 E7 32 3E 0B DC AB	
	Call log	66 3C 6E 54 E2 A3 4A 8D BE 56 B4 CC E1 A9 93 03	
Content	Music	88 6C 05 F1 C0 CC 40 06 B2 84 10 B7 79 2D 18 39	
	Photos	48 05 6F 23 10 86 4F 53 BB 46 46 8D 64 79 A8 10	
	Videos	CC 19 6A 6A 7D F3 40 33 8C 59 15 33 61 98 76 E3	
	Miscellaneous content files	69 67 FD 04 11 27 4D 24 91 24 6A C4 8C 5D DE 1A	
Account information and settings	Preferences and ringtones	0B FF FE B4 6D 4B 46 8D 83 32 50 87 7A BE 56 75	
	Network settings and bookmarks	42 F4 12 B8 AC A4 49 F1 8E 92 88 23 E3 18 03 4D	
	Email account information	C7 7C 44 B8 7F AD 4A 74 87 31 DC A0 C3 27 B6 FF	

Table 3. Signature information of file type on item

Item	File Type	Signature	Etc
Contacts	VCF	42 45 47 49 4E 3A 56 43 41 52 44	vCard 2.1
S Planner	VCS	42 45 47 49 4E 3A 56 43 41 4C 45 4E 44 41 52	vCalendar 1.0
Messages	PK	50 4B 03 04	
S Memo	PK	50 4B 03 04	
Mini diary	PK	50 4B 03 04	
Call log	PK	50 4B 03 04	
Music	MP3, etc	49 44 33, etc	etc(M4A,...)
Photos	JPG, etc	FF D8 FF E1 4B D6 45 78 69 66 00	etc(PNG,...)
Videos	MP4	00 00 00 18 66 74 79 70 69 73 6F 6D	
Miscellaneous content files	PK, etc	50 4B 03 04, etc	etc(MP3,...)
Preferences and ringtones	PK	50 4B 03 04	
Network settings and bookmarks	PK	50 4B 03 04	
Email account information	PK	50 4B 03 04	

백업 파일이 존재하는 데이터 영역(Area of data)에는 각 항목별 여러 가지 파일 타입(File Type)이 존재한다. 연락처는 VCF(vCard 2.1), S 플래너는 VCS(vCalendar 1.0), 음악은 MP3, M4A, 사진은 JPG, PNG, 동영상은 MP4, 그 외 PK 타입 등 다양한 파일 타입이 존재한다. Table 3은 데이터 영역의 백업 항목별 파일 타입 시그니처 정보를 나타낸다. 데이터 영역에서 백업 항목별 파일 타입에 해당하는 시그니처 정보를 비교하여 각 항목에 해당하는 파일들을 추출할 수 있다.

4. Kies 백업 파일 복원 기법

4.1 Kies 백업 파일 복원 절차

Kies 백업 파일(*.sbu)에 대한 복원 절차는 Fig. 4와 같다. 먼저 Kies 백업 파일을 읽어 들인 후 파일 헤더(File header)에서 디바이스 정보(OS, IMEI, 모델번호)를 확인한다. 그리고 메타데이터 정보 영역(Area of Metadata information)의 백업 항목에 대한 메타데이터 정보(Metadata information of item) 구조를 확인하여 데이터 영역의 시작 오프셋과 데이터 영역의 크기, 콘텐츠 파일의 수를 확인한 후 데이터 영역(Area of data)의 시작 오프셋으로 이동한다. 데이터 영역에는 백업 항목별 시그니처 정보가 존재하므로 백업 항목에 대한 데이터(Data of item) 구조를 확인하여 시그니처를 비교하고 데이터의 타입과 데이터의 크기, 표준 문자열의 크기를 각각 확인한 후 데이터로부터 백업 항목별 파일 타입 시그니처 정보를 확인하여 각각의 파일을 추출한다. 콘텐츠 파일의 경우 백업 항목 메타데이터 정보 구조의 콘텐츠 파일의 수만큼 반복하여 파일을 추출한다. 파일 추출 과정이 완료되면 정보 유형별로 파일을 분류하는 과정이 필요하게 된다.

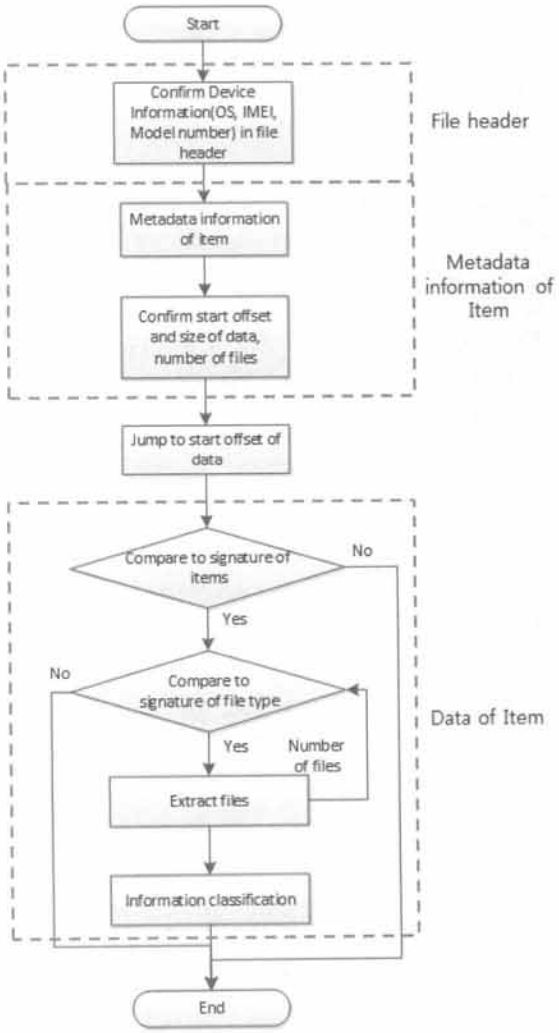

Fig. 4. Restoration procedure on Kies backup file

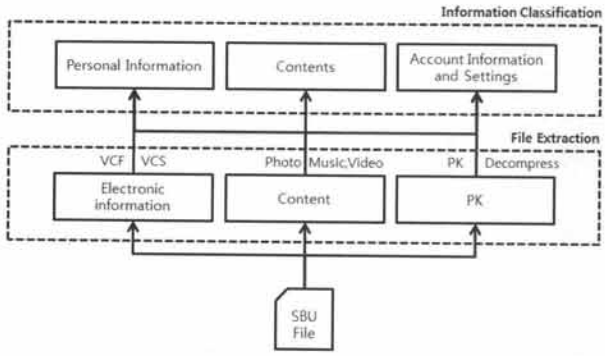

Fig. 5. Information classification

4.2 정보 분류

정보 분류 과정은 Fig. 5와 같다. 전자정보는 VCF 파일 포맷(vCard)과 VCS 파일 포맷(vCalendar)을 가진 파일을 의미하고, 콘텐츠 파일은 음악, 사진, 동영상 파일을 의미한다. 그리고 압축파일은 PK 파일을 의미한다. PK 파일은 압축되어 있으므로 ZIP 라이브러리[21-22] 등을 활용하여 압축 해제가 가능하다. 개인정보(Personal Information)는 연락처, S 플래너, 메시지, S 메모, 미니 다이어리, 통화이력을 포함하고, 콘텐츠(Contents) 파일은 음악, 사진, 동영상 파일을 포함한다. 그리고 계정 및 설정 정보(Account Information and Settings)는 이메일 계정 및 환경설정, 벨소리, 네트워크 설정, 북마크 정보를 포함한다.

파일은 크게 전자정보, 콘텐츠, 압축파일 형태로 추출되므로 각각을 대표하는 연락처, 사진, 이메일 계정 정보에 대해서 메타데이터 정보와 데이터 정보의 의미를 분석하였다. Fig. 6은 백업 항목 중 연락처에 대한 메타데이터 정보를 나타낸다. 시그니처(Signature) '0xB8 17 5A 8C 86 4C 45 06 9B 50 0C C8 88 28 EE 2E'는 연락처를 의미하고, 데이터 영역의 시작 오프셋(Starting offset of data)은 '0x04 EA'이다. 데이터 영역의 크기(Size of data area)는 '0x02 3C E8'로 10진수로 환산하면 146,664 바이트이다. 콘텐츠 파일의 수(Number of content files)는 0이고, 데이터의 타입(Type of data)은 '0x00 02'로 콘텐츠 이외의 정보를 의미한다.

Fig. 7은 연락처에 대한 데이터 정보를 나타낸다. 시그니처(Signature) '0xB8 17 5A 8C 86 4C 45 06 9B 50 0C C8 88 28 EE 2E'는 연락처를 의미하고, 데이터의 타입(Type of

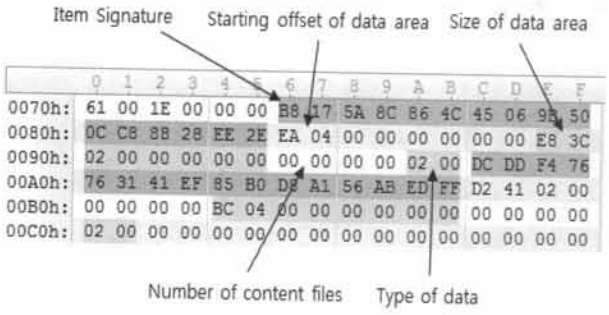

Fig. 6. Metadata information of contact

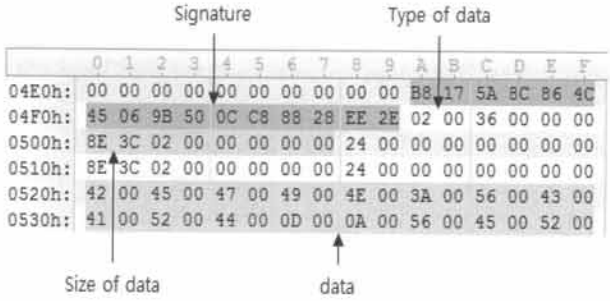

Fig. 7. Data of contact

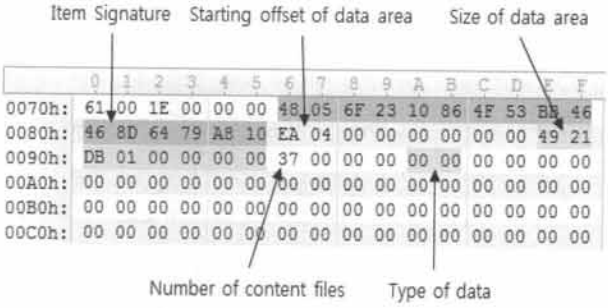

Fig. 8. Metadata information of photo

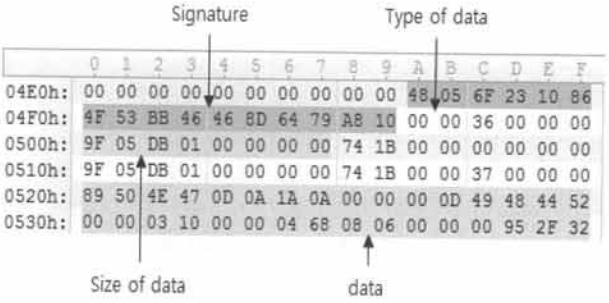

Fig. 9. Data of photo

data)은 '0x00 02'로 콘텐츠 이외의 정보를 의미하며, 데이터의 크기(Size of data)는 '0x02 3C 8E'로 10진수로 환산하면 146,574 바이트이다. 데이터(Data)는 VCF(vCard) 파일을 나타낸다.

Fig. 8은 백업 항목 중 사진에 대한 메타데이터 정보를 나타낸다. 시그니처(Signature) '0x48 05 6F 23 10 86 4F 53 BB 46 46 8D 64 79 A8 10'는 사진을 의미하고, 데이터 영역의 시작 오프셋(Starting offset of data)은 '0x04 EA'이다. 데이터 영역의 크기(Size of data area)는 '0x01 DB 21 49'로 10진수로 환산하면 31,138,121 바이트이다. 콘텐츠 파일의 수(Number of content files)는 '0x37'으로 10진수로 환산하면 55이고, 데이터의 타입(Type of data)은 '0x00 00'로 콘텐츠 정보를 의미한다.

Fig. 9는 사진에 대한 데이터 정보를 나타낸다. 시그니처(Signature) '0x48 05 6F 23 10 86 4F 53 BB 46 46 8D 64 79 A8 10'는 사진을 의미하고, 데이터의 타입(Type of

data)은 '0x00 00'으로 콘텐츠 정보를 의미하며, 데이터의 크기(Size of data)는 '0x01 DB 05 9F로 10진수로 환산하면 31,131,039 바이트이다. 데이터(Data)는 PNG 파일을 나타낸다.

Fig. 10은 백업 항목 중 이메일 계정에 대한 메타데이터 정보를 나타낸다. 시그니처(Signature) '0xC7 7C 44 B8 7F AD 4A 74 87 31 DC A0 C3 27 B6 FF'는 이메일 계정을 의미하고, 데이터 영역의 시작 오프셋(Starting offset of data)은 '0x04 EA'이다. 데이터 영역의 크기(Size of data area)는 '0x05 1E'로 10진수로 환산하면 1,310 바이트이다. 콘텐츠 파일의 수(Number of content files)는 0이고, 데이터의 타입(Type of data)은 '0x00 02'로 콘텐츠 이외의 정보를 의미한다.

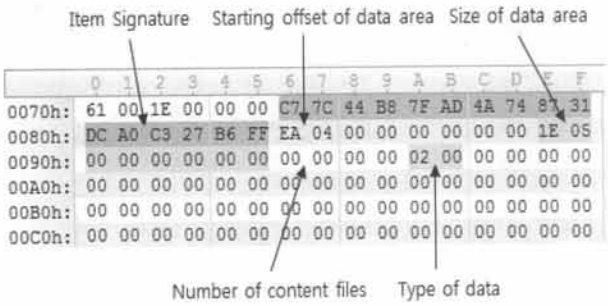

Fig. 10. Metadata information of email account

Fig. 11은 이메일 계정에 대한 데이터 정보를 나타낸다. 시그니처(Signature) '0xC7 7C 44 B8 7F AD 4A 74 87 31 DC A0 C3 27 B6 FF'는 이메일 계정을 의미하고, 데이터의 타입(Type of data)은 '0x00 02'으로 콘텐츠 이외의 정보를 의미하며, 데이터의 크기(Size of data)는 '0x04 C8'로 10진수로 환산하면 1,224 바이트이다. 데이터(Data)는 PK 파일을 나타낸다.

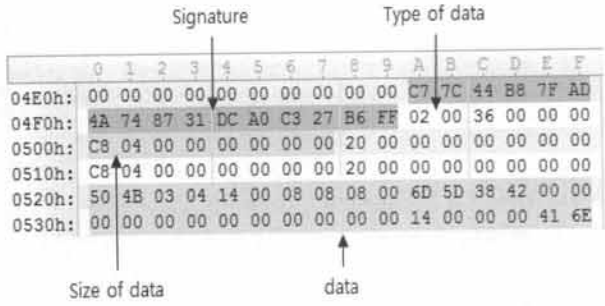

Fig. 11. Data of email account

5. 실험 및 평가

이 장에서는 Kies 백업 파일에 대해서 원본 파일을 추출하는 실험 및 평가를 한다. 실험을 위해 윈도우 7 환경에서 삼성 Kies 프로그램(버전 2.5)을 설치하였으며, 갤럭시 노트(SHV-E160S)와 갤럭시 S III LTE(SHV-E210K)를 실험폰으로 사용했다.

Fig. 12는 Kies 백업 파일 복원 절차를 통해 획득된 연락처 정보를 나타낸다. 데이터는 vCard 2.1 포맷을 가지고 있으며, 이름(N)은 "Quoted Printable"로 인코딩(Encoding) 되어 있다. 그러므로 이름의 경우 디코딩(Decoding) 과정이 필요하다. 인코딩 값 '=ED=99=8D=EA=B8=B8=EB=8F=99'은 디코딩하면 '홍길동'이란 의미를 갖는다.

```
BEGIN:VCARD
VERSION:2.1
N;CHARSET=UTF-8;ENCODING=QUOTED-PRINTABLE:;=E
D=99=8D=EA=B8=B8=EB=8F=99;;;;;;
TEL;HOME;CELL:01042092013
X-DIRTY:0
X-ACCOUNT:vnd.sec.contact.phone;vnd.sec.contact.phone
END:VCARD
```

Fig. 12. Contacts

Fig. 13은 Kies 백업 파일 복원 절차를 통해 획득한 사진 파일들을 나타낸다. 사진 파일들은 Table 3의 'FF D8 FF E1 4B D6 45 78 69 66 00' 시그니처 정보를 가지고 있는 JPG 파일들을 나타낸다.

Fig. 13. Photos

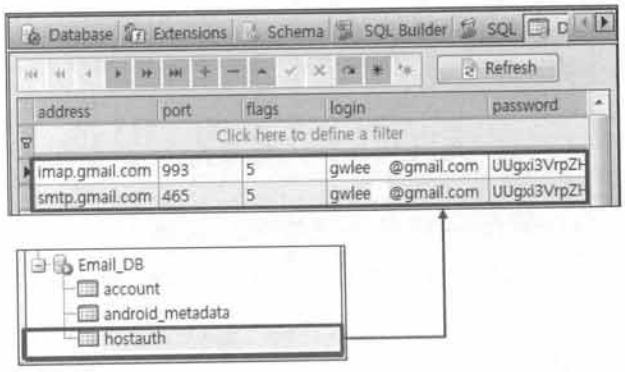

Fig. 14. Email account

Fig. 14는 PKZIP 툴로 압축 파일을 해제한 후 SQLite 뷰어로 이메일 계정 정보를 확인한 화면이다. PK 파일은 압축 파일이므로 압축 해제가 필요하다. 그림에서와 같이 로그인(login) 정보와 암호화된 비밀번호(password) 등 이메일 계정 정보를 확인할 수 있다.

Kies 백업 파일의 경우 파일 추출에 대해서 제안된 방법과 비교하기 위해 Armomurha의 SSVCard Extractor[13]와 Andreas의 SBU-Extractor[14]를 사용하였다. 기존의 도구들과 제안된 기법을 비교하면 Table 4와 같다.

Table 4. The comparison of Kies backup file extraction

Item	Armomurha	Andreas	Suggest
Contacts	O	O	`O
S Planner	-	O	O
Messages	-	-	O
S Memo	-	-	O
Mini diary	-	-	O
Call log	-	-	O
Music	-	O	O
Photos	-	O	O
Videos	-	O	O
Miscellaneous content files	-	O	O
Preferences and ringtones	-	-	O
Network settings and bookmarks	-	-	O
Email account information	-	-	O

실험 결과 Armomurha 도구는 연락처 정보만을 추출하였으며, Andreas 도구는 연락처, S 플래너, 음악, 사진, 동영상, 그 외 콘텐츠 파일을 추출하였다. 반면 이 논문에서 제안한 기법은 기존 도구들에 비해서 높은 파일 추출 결과를 보였다. 그 이유는 기존의 도구들이 일부 파일 포맷만을 비교하여 추출한 반면 제안된 기법은 백업 파일 구조를 분석한 후 복원 절차 및 정보 분류를 통해 백업 항목을 추출하였기 때문이다.

6. 결 론

이 논문에서는 삼성 Kies 백업 파일에 대한 구조를 분석하였으며, 백업 파일로부터 데이터를 복원하는 기법을 제안하였다. 제안된 기법은 백업 파일의 메타데이터 정보와 데이터 정보의 구조를 분석하여 전자정보, 콘텐츠 파일, 압축 파일들을 추출하였으며, 추출한 파일들을 개인정보, 콘텐츠 파일, 계정 및 설정 정보로 구분하여 정보 유형별로 분류하였다. 실험 결과 제안된 기법은 타 도구들에 비해 다양한 유형의 파일을 분석하여 원본 파일을 추출하는데 성공하였다.

이 논문에서 제안한 삼성 백업 파일 구조 분석 및 복원 기법은 애플 백업 파일 분석에 비해 부족한 연구를 수행하였다는 점에서 의미가 있으며, 특정 사건에 대한 용의자의 스마트폰 은닉 및 데이터의 고의 삭제 등에도 효과적으로 대응할 수 있으므로 포렌식 분야에서도 활용 가능하다.

참 고 문 헌

[1] Gartner [Internet], http://www.gartner.com/.

[2] Titanium Backup [Internet], http://www.titaniumtrack.com/.

[3] MyBackup Pro [Internet], http://www.rerware.com/.

[4] Astro File Manager [Internet], http://www.metago.net/astro-file-manager.php.

[5] Dropbox [Internet], https://www.dropbox.com/.

[6] Mobile cloud computing [Internet], http://en.wikipedia.org/wiki/Mobile_cloud_computing.

[7] E. T. Park, K. Kim, and Y. I. Eom, "A Smart Phone Backup Method in Mobile Cloud Environments," *Proceedings of The 39th KIISE Fall Conference*, Vol.39, No.2(D), pp.97-98, 2012.

[8] H. Y. Kim, O. G. Min, and G. H. Nam, "The Technology Trend of Mobile Cloud," *Electronics and Telecommunications Trends*, Vol.25, No.3, pp.40-51, 2010.

[9] K. C. Lee, "A Concept and Technology Trends on Mobile Cloud," *ICT Standard & Certification TTA Journal*, Special Report 2, Vol.139, pp.54-58, 2012.

[10] G. H. Park, and S. Y. No, "Cloud Services for the forensic aspects of the investigative methods," *Korea Industrial Information Systems Society*, Vol.17, No.1, pp.39-46, 2012.

[11] iTunes [Internet], http://www.apple.com/kr/itunes/.

[12] Kies [Internet], http://www.samsungapps.com/mercury/about/onPc.as?COUNTRY_CODE=KOR&_isAppsDep=Y.

[13] Armomurha, SSVCardExtractor [Internet], http://forum.xda-developers.com/attachment.php?attachmentid=644065&d=1309648829.

[14] L. Andreas, SBU-Extractor [Internet], https://www.lord-luncher.de/.

[15] M. Bader and I. Baggili, "iPhone 3GS Forensics: Logical analysis using Apple iTunes Backup Utility," *SMALL SCALE DIGITAL DEVICE FORENSICS JOURNAL*, Vol.4, No.1, September, 2010.

[16] C. Clinton, "Looking to iPhone backup files for evidence extraction," *the Proceedings of the 9th Australian Digital Forensics Conference*, December, 2011.

[17] B. Satish, iPhone Forensics - Analysis of iOS 5 backups : Part 1 [Internet], http://resources.infosecinstitute.com/iOS-5-backups-part-1/.

[18] iPhone Backup Extractor [Internet], http://supercrazyawesome.com/.

[19] iPhone Backup Browser [Internet], http://code.google.com/p/iphonebackupbrowser/.
[20] iBackupBot [Internet], http://www.icopybot.com/itunes-backup-manager.htm.
[21] PKZIP [Internet], http://www.pkware.com.
[22] 7-ZIP [Internet], http://www.7-zip.org.

이 규 원

e-mail : cool2527@ensec.re.kr
2005년 2월 단국대학교 전자.컴퓨터학부(이학사)
2007년 2월 단국대학교 전자계산학과(이학석사)
2007년 1월~2010년 6월 (주)케이사인 책임연구원
2010년 7월~현 재 한국전자통신연구원 부설연구소 연구원
관심분야 : 디지털 포렌식, 정보보호

황 현 욱

e-mail : hhu@ensec.re.kr
2000년 2월 조선대학교 정보통신공학과(공학사)
2002년 2월 조선대학교 전자공학과(공학석사)
2004년 8월 전남대학교 정보보호협동과정학과(이학박사)
2004년 9월~현 재 한국전자통신연구원 부설연구소 선임연구원
관심분야 디지털 포렌식, 파일시스템

김 기 범

e-mail : kibom@ensec.re.kr
1994년 2월 제주대학교 정보공학과(공학사)
1996년 8월 고려대학교 전산과학과(이학석사)
2001년 2월 고려대학교 전산과학과(이학박사)
2001년 1월~2004년 7월 ㈜ECO 개발부장
2004년 8월~현 재 한국전자통신연구원 부설연구소 선임연구원
관심분야 : 디지털 포렌식, 사이버보안

장 태 주

e-mail : tchang@ensec.re.kr
1982년 2월 울산대학교 전기공학과(공학사)
1990년 2월 한국과학기술원 전기및전자공학과(공학석사)
1998년 2월 한국과학기술원 전기및전자공학과(공학박사)
1982년 1월~2000년 1월 국방과학연구소 연구원
2000년 2월~현 재 한국전자통신연구원 부설연구소 책임연구원
관심분야 : 디지털 포렌식, 정보보호