정 보 보 호 학 회 지
제26권 제5호, 2016. 10

모바일 포렌식 동향

김 도 현*, 이 상 진**

요 약

모바일기기에는 우리 일상생활과 밀접한 데이터가 가장 많이 저장되어 있기 때문에 디지털 포렌식 수사 시 모바일 포렌식의 필요성이 크게 증가하고 있다. 스마트폰 등장 초기부터 현재까지 다양한 모바일 기기의 운영체제와 제품들이 출시되었지만 현재는 안드로이드와 iOS가 전 세계적으로 가장 많이 사용되고 있다. 따라서 본고에서는 모바일 포렌식의 절차, 데이터 수집 기술, 분석 대상 데이터 등의 모바일 포렌식의 동향을 안드로이드와 iOS를 위주로 살펴본다.

Ⅰ. 서 론

모바일 포렌식은 스마트폰, 태블릿PC, 웨어러블기기 등에 대한 디지털 포렌식을 수행하는 것으로 2000년대 후반 전 세계적으로 스마트폰의 사용이 급격하게 증가하면서부터 현재까지 많은 연구가 진행되고 있다. 초기의 스마트폰 시장은 애플의 iOS, 블랙베리 등이 주도하였지만 오픈소스를 기반으로 하는 구글의 안드로이드가 등장하고 삼성, LG, 모토로라, HTC 등이 안드로이드를 기반으로 하는 스마트폰을 개발하면서 스마트폰 시장은 점차 안드로이드와 iOS가 주도하게 되었다.

구글과 애플은 자사의 운영체제를 더욱 발전시켜 스마트폰뿐만 아니라 다양한 모바일기기들을 출시하였고 그 결과 스마트폰, 태블릿PC 등의 다양한 모바일기기들은 현대인의 생활을 편리하게 해줌과 동시에 일상생활과 가장 밀접한 데이터들이 저장된 정보저장매체가 되었다.

본고에서는 현 시점의 모바일기기 중 가장 점유율이 높은 안드로이드와 iOS에 대한 모바일 포렌식 절차, 데이터 수집 기술, 분석 대상 데이터 종류, 이슈 및 향후 연구 방향에 대해 살펴본다.

Ⅱ. 모바일 포렌식 절차

모바일 포렌식 절차와 관련된 다양한 국제, 국내 표준문서와 논문들이 존재한다. 모바일 포렌식 절차는 기본적으로는 컴퓨터 포렌식에서 수립된 절차에서 확장된 것이며 지속적으로 새로운 모바일 기기가 출시되고 있기 때문에 이에 대응하기 위한 절차도 지속적으로 제안 및 수립되고 있다.

2.1. 국제 절차

모바일 포렌식 절차와 관련된 대표적인 국제 표준문서는 미국 NIST의 SP 800-101 Revision1, “Guidelines on Mobile Device Forensics”[1]가 있다. 이 문서는 최초 2006년에 발표되어 새로운 모바일 기기의 특성에 따라 보안 및 수정되어 2014년 5월 가장 마지막으로 개정되었다. 해당 문서에서는 모바일 포렌식의 수행 절차를 크게 Preservation, Acquisition, Examination and Analysis, Reporting 4단계로 나눈다.

- Preservation 단계는 현장에서 모바일기기를 발견했을 때 전파 및 네트워크 차단 등의 대응 방법에 대한 내용이다.
- Acquisition 단계는 모바일 기기의 모델명 등을 통해 해당 기기를 식별 및 확보하고 모바일 포렌식 도구를 사용하여 내부 데이터를 수집하는 방법에 대한 내용이다.

본 연구는 2016년도 정부(미래창조과학부)의 재원으로 한국연구재단-공공복지안전사업(2012M3A2A1051106)의 지원을 받아 수행되었습니다.
* 고려대학교 정보보호대학원 박사과정 (exdus84@gmail.com)
** 고려대학교 정보보호대학원 정교수 (sangjin@korea.ac.kr)

- Examination and Analysis 단계는 수집된 모바일 기기 데이터에서 분석 대상 데이터들의 종류를 나열하고, 모바일 포렌식 분석 도구를 사용하여 데이터를 분석하는 것에 대한 내용이다.
- Reporting 단계는 모바일 포렌식 전체적인 수행 결과에 대한 보고서 작성과 관련된 내용이다.

ISO/IEC 27043, “Information technology - Security techniques - Incident investigation principles and process”[2]에서도 모바일 포렌식과 관련된 절차를 다룬다. 이 절차를 바탕으로 Emilio Raymond Mumba는 실제 케이스 스터디를 통해 해당 절차의 효율성을 확인했다[3]. 해당 절차명은 Harmonized Digital Forensic Investigation Process이며, 크게 Readiness processes, Initialization processes, Acquisitive processes, Investigative processes, Concurrent processes 5단계로 나눈다.

- Readiness processes는 일반적인 디지털 포렌식에서의 사전 준비에 해당하는 단계다. 발생 가능사고에 대한 시나리오를 구성하고 이에 대응하기 위한 절차 수립, 도구 및 시스템 준비 등을 통해 최소의 비용과 시간으로 효과적인 디지털 포렌식을 수행하기 위한 내용들을 포함한다.
- Initialization processes는 사건 발생 시 초기 대응, 조사 계획 수립 및 준비를 하는 단계다.
- Acquisitive processes는 현장에서 수집 대상 기기를 식별 및 확보하고 데이터 수집, 운반, 보관 등을 수행하는 단계다.
- Investigative processes는 수집된 디지털 데이터를 조사 및 분석하고 조사를 마무리하는 단계다.
- Investigative processes는 앞의 4가지 단계 모두에서 동시에 수행하는 단계로 조사 권한 확보, 문서화, 조사 절차 관리 수행 및 보관연속성(Chain of Custody)을 유지함으로써 디지털 증거물의 증거 능력을 유지하도록 하는 단계다.

이 외에도 Cynthia A. Murphy[4], Archit Goel이 제시한 절차 등이 존재한다[5]. 이러한 표준 문서 및 논문들이 제안하는 절차의 단계는 세분화 정도에 따라 다양하지만 핵심적인 내용들은 유사하다.

2.2. 국내 절차

모바일 포렌식 절차와 관련된 국내 표준문서로는 2007년 발표된 한국 TTA표준인 “이동 전화 포렌식 가이드라인”이 있다[6]. 해당 문서는 이동 전화 포렌식 절차를 크게 사전 준비, 초기 대응, 증거 수집, 이동 전화 포장 운송 및 보관, 조사 및 분석, 보고서 작성 5단계로 나눈다. 하지만 이 문서는 발표 당시 스마트폰이 대중화되지 않았었기 때문에, 피쳐폰에 대한 디지털 포렌식 수행에 대한 내용을 설명하고 있다. 따라서 해당 문서에서의 절차를 현 상황의 모바일 포렌식에 적용하기에는 많은 한계점이 있다.

이 외 국내 대검찰청, 경찰청 등의 수사기관은 내부적으로 각 기관의 특성에 맞는 모바일 포렌식 절차를 예규 또는 가이드라인 등으로 규정하여 사용하고 있다.

국내 논문들은 국제 문서들과 비교하여 절차와 관련된 내용 보다는 모바일기기 데이터의 증거 능력 확보와 관련된 내용이 대부분이다[7,8].

Ⅲ. 모바일기기 데이터 수집

모바일기기의 데이터는 기기 내부의 메인보드에 부착되어 있는 플래시메모리, 물리메모리와 사용자가 추가적으로 기기에 삽입하여 사용하는 microSD 카드, USIM 카드 등에 저장된다. 이러한 모바일기기 데이터를 수집하는 기술은 지속적으로 연구 개발되고 있으며 Konstantia Barmpatsalou는 2007년부터 2013년까지 안드로이드와 iOS 뿐만 아니라 블랙베리 등의 모바일 기기에 대해 연구 개발된 디지털 포렌식 기술들을 정리하였다[9].

모바일 포렌식 수행과정 중 수집 대상 저장매체는 [표 1]과 같고, 그 수집 방법에 대해 안드로이드와 iOS를 위주로 다음 소절에서 설명한다.

〔표 1〕 모바일기기 내부 수집 대상 저장매체 종류

항 목	비 고
모바일기기 내부의 플래시메모리	필수 수집
모바일기기 내부의 물리메모리	선택 수집 (안드로이드)
microSD 카드	존재 시 수집
USIM 카드	존재 시 수집

3.1. 모바일기기 내부의 플래시메모리

모바일기기 내부의 플래시메모리를 수집하는 방법은 크게 Chip-off, JTAG, 안드로이드 모바일기기의 데이터 수집 방법, iOS 모바일기기의 데이터 수집 방법 4가지로 나눌 수 있다.

3.1.1. Chip-off

Chip-off는 모바일기기의 메인보드에 부착되어 있는 플래시메모리를 물리적으로 분리한 후 하드웨어 리더기 장비를 사용하여 내부 데이터를 이미징하는 방법이다[10]. 플래시메모리를 분리하는 과정에서 핀이 손상될 수 있기 때문에 필요시 리볼링(rebolling)과정을 통해 손상된 핀을 복원한 뒤 리더기를 사용해야 한다.

Chip-off를 통해 메인보드에서 분리된 플래시메모리는 다시 복원을 하는 것이 어렵게 때문에 주로 수집 대상 모바일기기가 파손 등으로 사용할 수 없는 경우에 주로 사용한다.

3.1.2. JTAG(Joint Test Action Group)

JTAG은 모바일기기 메인보드에 있는 PCB(Printed Circuit Board)의 JTAG 포트를 하드웨어 디버깅장비와 연결하여 플래시메모리 데이터를 이미징하는 방법이다[11,12]. 이 방법은 안드로이드와 iOS 모바일기기에 대해 모두 사용할 수 있지만, 삼성 갤럭시S3와 애플 아이폰4부터는 기기 출하 시 메인보드의 JTAG 포트를 없애기 때문에 현재 시점에서는 이 방법을 사용할 수 있는 모바일기기가 제한적이다.

3.1.3. 안드로이드 모바일기기의 데이터 수집 방법

안드로이드 운영체제가 탑재된 모바일기기에서 데이터를 수집하는 방법은 펌웨어 업데이트 프로토콜을 이용하는 방법[13], 루팅 커널을 이용하는 방법[14], 안드로이드 백업 프로토콜을 사용하는 방법[15], 안드로이드 데이터 공유 프로토콜을 사용하는 방법 등이 있다[16].

• 펌웨어 업데이트 프로토콜

안드로이드 모바일기기의 AP(Application Processor)에는 펌웨어(firmware) 업데이트를 위해 부트로더(Bootloader)를 로딩한 시점에서 플래시메모리 영역에 대한 읽기·쓰기를 할 수 있는 명령어가 존재한다. 이러한 펌웨어 업데이트 프로토콜을 사용하여 안드로이드 모바일기기를 펌웨어 업데이트 모드로 부팅한 후 플래시메모리의 데이터를 이미징할 수 있다.

이 방법은 안드로이드 모바일기기 데이터 수집 방법 중 가장 최근에 발견된 것으로, 기존의 JTAG보다 빠른 속도로 데이터를 수집할 수 있다. 하지만, 모바일기기 제조사별로 AP의 종류가 다르고 그에 따라 프로토콜이 상이하기 때문에 이 방법을 적용할 수 있는 모바일기기가 제한적이고 전체수집만 가능하다는 단점이 있다.

• 루팅 커널

안드로이드 모바일기기의 펌웨어 내부의 커널이미지를 관리자 권한을 갖도록 수정하고 이것을 모바일기기의 커널영역에 덮어씌운 뒤(flashing) 해당 커널이미지로 부팅하여 관리자 권한을 획득함으로써 내부 데이터를 수집하는 방법이다. 루팅 커널 제작은 일반적으로 모바일기기의 훼손을 최소화하기 위해 리커버리 커널 이미지를 사용한다. 이 방법도 JTAG보다 빠른 속도로 데이터를 수집할 수 있다.

전체수집은 수집 대상 파티션에 해당하는 블록장치명을 선택한 뒤 이미징을 위한 dd와 데이터 전송을 위한 netcat, ADB(Android Debug Bridge) 명령어를 조합하여 사용한다. 안드로이드 모바일기기 내부 블록장치명은 기기 마다 상이하기 때문에 [표 2]와 같은 명령어를 통해 확인해야 한다.

블록장치명은 플래시메모리의 종류에 따라서도 형태가 상이하다. [표 3]은 eMMC, UFS 플래시메모리 종류에 따른 내부 블록장치명의 형태다.

eMMC 플래시메모리의 경우 “mmcblk0” 블록장치명을 이미징하면 플래시메모리 전체 데이터를 수집할

〔표 2〕 안드로이드 모바일기기 블록장치명 확인 명령어

항 목	내 용
mount	마운트된 블록장치명
cat /proc/partitions	모든 블록장치명 확인
cat /etc/recovery.fstab	모든 블록장치명 확인

〔표 3〕 플래시메모리 종류에 따른 블록장치명

플래시메모리	블록장치명	내 용
eMMC	mmcblk0	플래시메모리 전체
	mmcblk0p#	특정 파티션
UFS	sda	플래시메모리 전체
	sda#	특정 파티션

수 있고, 특정 파티션만 선택적으로 수집하려면 “mmcblk0p#”를 이미징하면 된다. UFS 플래시메모리도 동일한 방법으로 수집할 수 있으며, 최신 안드로이드 폰의 경우 대부분 UFS 플래시메모리를 사용한다.

안드로이드 모바일기기 내부에는 상당히 많은 블록장치가 존재하며, 그 중 사용자 데이터가 존재하는 /data 파티션, 시스템 데이터가 존재하는 /system 파티션에 해당하는 블록장치가 주요 수집 대상이다. eMMC, UFS 플래시메모리에서 /sdcard 파티션은 일반적으로 /data 파티션의 블록장치에 함께 포함되어 있다.

선별수집은 [표 2], [표 3]을 통해 수집대상 파티션에 대한 블록장치명, 마운트포인트, 파일시스템의 종류를 확인한 후 “mount”명령어를 통해 해당 파티션을 마운트한 후 수행한다. 이때, 데이터의 훼손을 최소화하기 위해 아래와 같은 읽기전용 속성으로 마운트해야 한다.

mount -o ro -t [파일시스템종류] [블록장치명] [마운트 포인트]

수집대상 파티션을 마운트한 후 선별된 수집 대상 디렉터리 또는 파일들을 아래와 같은 adb 명령어를 사용하여 수집할 수 있다.

adb pull [수집대상경로] [추출경로]

• 안드로이드 백업 프로토콜

안드로이드 백업 프로토콜은 안드로이드 운영체제 버전 4.0 이후 ADB에서 지원하는 데이터 백업 기능으로 관리자 권한이 없이도 사용자 데이터를 수집할 수 있다는 장점이 있다. 안드로이드 모바일기기를 정상 부팅한 후 분석 시스템에 연결하여 사용하며 아래와 같은 명령어를 사용하여 데이터를 수집할 수 있다. 명령어의 옵션에 대한 설명은 [표 4]와 같다.

〔표 4〕 안드로이드 백업 프로토콜의 옵션

옵 션	내 용
-f 〈file〉	• 수집 결과 파일명 • 미선택 시 “backup.ab”로생성
-apk|-noapk	• apk(앱 설치파일)백업 여부
-shared|-noshared	• SD카드 영역 백업 여부
-all	• 전체 데이터 백업 여부
-system|-nosystem	• 시스템앱 설치파일 백업여부
〈packages…〉	• 특정 앱만 백업

adb backup [-f <file>] [-apk|noapk] [-shared|-noshared] [-all] [-system|-nosystem] [<packages…>]

특정 앱만 백업하기 위해서는 아래와 같은 명령어를 통해 안드로이드 모바일기기에 설치되어 있는 모든 앱 목록을 확인하고 진행한다.

adb shell pm list package

옵션 상으로는 전체 데이터를 백업할 수 있지만, 현재는 보안상 전체 데이터, SD카드 영역, 문자, 통화내역과 같은 개인정보가 있는 데이터는 백업되지 않도록 변경되었다. 또한, 카카오톡 등의 몇몇의 3rd 애플리케이션도 백업되지 않는다는 단점이 있다.

• 안드로이드 데이터 공유 프로토콜

안드로이드 데이터 공유 프로토콜은 안드로이드 모바일기기에 설치된 서로 다른 애플리케이션들 간의 데이터 공유를 위해 제공하는 것으로 일반적으로 Content Provider라고 불린다. 이것은 사용자 애플리케이션을 개발하는 경우 기본 애플리케이션의 데이터를 사용하기 위해 주로 사용되며 카카오톡 등의 메신저 애플리케이션이 주소록에 저장된 데이터와 동기화 하는 것이 그 예이다.

이 기능을 사용하여 데이터를 수집하기 위해서는 데이터 수집을 할 수 있는 애플리케이션을 개발하여 수집대상 안드로이드 모바일기기에 설치해야 한다. 따라서 해당 방법은 현재 국내에서는 거의 사용되고 있지 않다. 하지만 Cellebrite UFED[17], Micro Systemation XRY[18]와 같은 해외 모바일 포렌식 도구의 경우

Logical 수집 기능을 사용하면 이 기능을 사용한다.

이러한 안드로이드 데이터 공유 프로토콜은 악성앱에서 악용되기도 한다. 스미싱, 스파이앱 등은 사회공학적 기법 등을 통해 공격 대상 안드로이드 모바일기기에 설치된 후 Content Provider를 사용하여 주소록, 문자, 통화내역, SD카드 내부파일 등을 탈취한 뒤 외부 서버로 전송한다.

이와 같이 모바일기기 데이터에 대한 선별수집이 가능한 수집 방법은 루팅 커널을 통해 관리자 권한을 획득한 후 특정 파일만 수집하는 방법, 안드로이드 백업 프로토콜에서 특정 애플리케이션 데이터만 백업하는 방법, 안드로이드 데이터 공유 프로토콜을 사용하는 방법 등이 있다. 하지만 이러한 방법을 통해 사건과 관련된 데이터만 선별하기에는 기술적으로 많은 한계가 존재하며 모바일 기기를 활성 상태에서 수집하는 방법은 데이터의 무결성이 훼손될 우려가 있다. 따라서 현재 국내에서는 모바일기기는 대부분 원본압수 또는 내부 데이터를 전체수집 하고 있다[19].

3.1.4. iOS 모바일기기의 데이터 수집 방법

iOS 운영체제가 탑재된 모바일기기에서 데이터를 수집하는 방법은 탈옥을 이용하는 방법, iOS 백업 프로토콜을 사용하는 방법이 있다[20]. 최신 iOS 모바일기기는 탈옥을 사용하여 플래시메모리의 파티션을 이미징하면 데이터 복호화에 대한 이슈가 존재하기 때문에 주로 백업 프로토콜을 사용하여 데이터 수집을 수행한다.

• 탈옥

탈옥은 안드로이드의 루팅과 마찬가지로 iOS 모바일기기의 관리자 권한을 획득하는 방법이다. 이를 위해 다양한 해킹그룹에서 개발한 탈옥 도구를 사용할 수 있다[21-23]. 탈옥 방법은 iOS 모바일기기의 종류와 iOS 버전에 따라 상이하기 때문에 두 가지 조건이 맞는 탈옥 도구를 사용해야 한다.

이 방법을 사용하기 위해서는 패스코드, 지문인식 등의 접근제어를 해제한 뒤 iOS 모바일기기에 탈옥에 필요한 Cydia 애플리케이션과 OpenSSH 등을 설치해야 하고 순정 상태로 복원하기 위해서는 운영체제가 가장 최신버전으로 업데이트된다는 단점이 있다.

또한, iOS 운영체제 버전 4부터는 내부 데이터가 모두 암호화되어 있기 때문에 탈옥을 사용하여 데이터를 수집한 후에 추가적으로 데이터 복호화 과정을 수행해야 한다.

• iOS 백업 프로토콜

iOS 모바일기기도 안드로이드와 마찬가지로 백업프로토콜을 통해 내부 데이터를 수집할 수 있다. 프로토콜의 종류는 Apple의 iTunse 프로그램에서 사용하는 Mobile Backup2와 AFC, File Relay, Installation Proxy, House Arrest 총 5가지가 있으며 각 프로토콜마다 백업되는 데이터의 종류와 범위가 상이하고 iOS 운영체제의 버전마다 지원하는 프로토콜의 종류도 다르다.

Mobile Backup2는 기본 및 사용자 애플리케이션 데이터와 안드로이드의 SD카드 영역으로 볼 수 있는 Media 데이터를 백업한다. [그림 1]은 iOS 버전 10인 아이폰에서 내부의 모든 데이터를 iTunes 프로그램으로 백업한 데이터를 캡쳐한 것이다. iOS 버전 9까지는 백업된 모든 파일의 파일명이 자신의 전체 경로를 SHA1 해시한 결과 값으로 되어있었다. 또한, 모든 파일의 정보는 특정 포맷의 Manifest.mbdb라는 파일에 저장되어 있었다. 하지만 iOS 버전 10부터는 [그림 1]과 같이 모든 파일들은 자신의 애플리케이션의 데이터들과 함께 각각의 폴더에 백업되며 모든 파일의 정보가 저장된 Manifest.mbdb 파일은 SQLiteDB 포맷으로 변경되어 Manifest.db로 변경되었다. [그림 2]는 백업된

〔그림 1〕 iOS 10버전 아이폰을 iTunse로 백업한 결과

〔그림 2〕 백업 결과의 특정 폴더 내부 데이터

fileID	domain	relativePath
(empty)	(empty)	(empty)
b1529201502c902a0ccbc961de80c6da9b61c67e	AppDomainPlugin-com.apple.news.diagnosticextension	
5b54f06a6837c79d9b6ab332d7eb82c71db1e006	AppDomainPlugin-com.apple.news.diagnosticextension	Library
ec2e41ededb1350351e53fc73ea1f2fc345ad1f2	AppDomainPlugin-com.apple.news.diagnosticextension	Library/Preferences
d52891ebb2374366c0e9638408Bb30dfe20b3f6c	AppDomainPlugin-com.apple.news.diagnosticextension	Documents
26821d31f90ceb078fb65c401d1f32d3db814074	AppDomainPlugin-com.apple.DiagnosticsService.Diagnostic-3744	
8cc61a8fb42817fbc622d0a5817a3de6ec4f73ff	AppDomainPlugin-com.apple.DiagnosticsService.Diagnostic-3744	Library
163244a68d256442c5fb80d46750e6ec44378360	AppDomainPlugin-com.apple.DiagnosticsService.Diagnostic-3744	Library/Preferences
09c69852ad9f64aa9e190425894c04c30dd81d1a	AppDomainPlugin-com.apple.DiagnosticsService.Diagnostic-3744	Documents
d2597db0f23bd128299b59a3c11b76984fe74dfc	AppDomainPlugin-com.apple.Maps.TransitWidget	
a4b3ff7049e5cb614981b122f32aed53033e2f3	AppDomainPlugin-com.apple.Maps.TransitWidget	Library
0163dbf9b2051edca153790870bf25a64030faa4	AppDomainPlugin-com.apple.Maps.TransitWidget	Library/Preferences

〔그림 3〕 Manifest.db 파일의 Files 테이블 데이터

특정 폴더 내부에 존재하는 파일을 캡쳐한 것이다.

AFC는 Media 데이터만 백업하고 File Relay는 시스템 로그와 설정 정보만 백업하며 이것은 iOS 버전 7.1.2까지만 지원한다. Installation Proxy는 설치된 애플리케이션 목록만 백업하고 House Arrest는 애플리케이션 설치파일만 백업하는데 이를 위해서는 Installation Proxy와 병행하여 사용해야 한다. Houses Arrest는 iOS 버전 8.3까지만 지원한다. 각 프로토콜의 특성은 [표 5]와 같다[24].

3.2. 모바일기기 내부의 물리메모리

모바일기기 내부의 물리메모리 수집은 활성 포렌식(Live Forensics)에서 수행하며 현재 기술적인 한계로 인해 안드로이드만 가능하다. 이것은 루팅 커널을 사용한 데이터 수집 방법에서만 사용 가능하며, 루팅 커널 제작 시 물리 메모리 수집을 위한 LiME 커널 모듈을 추가해야 한다[25,26].

하지만 모바일기기에 대한 활성포렌식은 데이터 훼손에 대한 위험이 존재하기 때문에 국내에서는 수행하고 있지 않다.

3.3. microSD 카드

모바일기기에 삽입되어 있던 microSD 카드는 모바일기기에서 분리한 후 전용 커넥터를 사용하여 일반적인 하드웨어 데이터 수집 도구에 연결한 후 내부 데이터를 수집한다.

3.4. USIM 카드

USIM 카드에는 통신사 정보 등이 존재하고 사용자가 데이터를 백업해 놓을 가능성이 있기 때문에 모바일기기에서 분리한 후 전용 도구를 사용하여 내부 데이터를 수집한다[27].

Ⅳ. 모바일기기 데이터 분석

모바일기기 데이터는 크게 시스템 데이터, 사용자 데이터 2가지로 나눌 수 있으며 모바일기기와 운영체제 종류에 따라 데이터의 경로와 존재 여부가 상이할 수 있다. 다음 소절에서는 시스템, 사용자 데이터를 안드로이드와 iOS 운영체제 별로 소개한다.

4.1. 시스템 데이터

[표 6]은 안드로이드 모바일기기의 시스템 데이터를 정리한 것이며, [표 7]은 iOS 모바일기기의 시스템 데이터를 정리한 것이다. 이러한 데이터들은 일반적으로 텍스트 또는 xml 포맷으로 존재한다.

〔표 5〕 안드로이드 모바일기기 블록장치명 확인 명령어

프로토콜 종류	수집 대상	특 징
Mobile Backup 2	• var/mobile/Media • var/mobile/Library • var/mobile/Applications	• 기본 및 사용자 앱 데이터 수집 • 기기명, 전화번호 정보 등
AFC	• var/mobile/Media'	• Media 관련 데이터 수집
File Relay	• var/logs/AppleSupport • var/mobile/Library/Caches • Library/Logs/CrashReporter • var/mobile/Library/Logs/CrashReport • var/mobile/Library/Logs/MobileWirelessSync	• 설정 정보, 시스템 로그 수집 • 앱 데이터는 수집 불가 • tmp 디렉터리 접근 가능 • iOS 7.1.2 까지만 지원
Installation Proxy	• 설치된 앱 목록 획득	• House Arrest와 병행 사용
House Arrest	• 앱 설치 파일 수집	• iOS 8.3 까지만 지원

〔표 6〕 안드로이드 모바일기기의 시스템 데이터

항 목	파일 경로
커널 정보	/data/log/recovery_kernel_log.txt
리커버리 로그	/data/log/recovery_log.txt
전원 종료 로그	/data/log/poweroff_info.txt
전원 재시작 로그	/data/log/powerreset_info.txt
전원 부팅 로그	/data/log/rtc.log
통화중 단절 로그	/data/log/CallDropInfoLog.txt
앱 에러 로그	/data/log/dumpstate_app_error.txt.gz
공유기 연결 로그	/data/misc/wifi/wpa_supplicant.conf
블루투스 정보	/data/misc/bluetoothd/config
앱 실행 정보	/data/system/dmappmgr.db
설치된 앱 정보	/data/system/packages.xml
등록된 계정 정보	/data/system/users/0/accounts.db
자동 로그인 .계정 정보	/data/system/registered_services /android.accounts.AccountAuthenticator.xm
자동 동기화앱 목록	/data/system/registered_services/ android.content.SyncAdapter.xml

〔표 7〕 iOS 모바일기기의 시스템 데이터

항 목	파일 경로
시스템 플러그인, 설정 정보	/Library 하위
시스템 환경설정, 라이브러리 디렉터리	/System 하위
모바일기기의 통신사업자명	/var/mobile/Library/ConfigurationProfiles/PayloadManifest.plist
모바일기기 번호, 번호 등록 날짜와 시간	/var/wireless/Library/Preferences/com.apple.commcenter.plist
모바일기기, 사용자명	/var/preferences/SystemConfiguration/com.apple.network.identification.plist

4.2. 사용자 데이터

[표 8]은 안드로이드 모바일기기의 사용자 데이터를 정리한 것이며, [표 9]는 iOS 모바일기기의 사용자 데이터를 정리한 것이다. 이러한 데이터들은 일반적으로 SQLite DB또는 xml 포맷으로 존재한다.

〔표 8〕 안드로이드 모바일기기의 사용자 데이터

항 목	파일 경로
통화 내역	/data/com.sec.android.provider.logsprovider/databases/logs.db
문자 내역	/data/com.android.providers.telephony/databases/mmsms.db
주소록	/data/data/com.android.providers.contacts/databases/contacts2.db
캘린더	/data/com.android.providers.calendar/databases/calendar.db
인터넷 사용 내역	/data/com.sec.android.app.sbrowser/Default/History
지메일	/data/com.google.android.gm/databases/mailstore.UserID@gmail.com
이메일	/data/com.android.email/databases/EmailProvider.db
미디어 데이터 기록	/data/com.android.providers.media/databases/external.db
구글 지도	data/com.google.android.apps.map/databases/gmm_myplaces.db
s노트	data/data/com.sec.android.app.snotebook/databases/fmFiles.db data/data/com.samsung.android.snote/databases/Snote.db
카카오톡	/data/data/com.kakao.talk/KakaoTalk.db /data/data/com.kakao.talk/KakaoTalk2.db /data/data/shared_prefs/KakaoTalk.perferences.xml
텔레그램	data/org.telegram.messenger/files/cache4.db
네이트온	/data/data/Uxpp.UC/shared_prefs/nateon_login.xml /data/data/Uxpp.UC/databases/neteon.db /data/data/Uxpp.UC/databases/neteon_wb.db
네이버 라인	/data/data/jp.naver.line.android/naver_line
드롭박스	/data/com.dropbox.android/databases/3180000599-db.db
N드라이브	/data/com.nhn.android.ndrive/databases/ndrive.db
티맵	/data/data/com.skt.tmap/databases/recent.db
올레네비	/data/data/kt.navi/databases/Db_RecentDestination /data/data/kt.navi/databases/Db_RecentSearchListDbControl

항 목	파일 경로
폴라리스 오피스	/data/data/com.infraware.office.link/databases/InfrawarePoLinkFiles.db
어도비 리더	/data/data/com.adobe.reader/databases/com.adobe.reader.filebrowser.ARRecentsFileManager.ARRecentsFileDatabase /data/data/com.adobe.reader/databases/ARUserBookmarkDB

〔표 9〕 iOS 모바일기기의 사용자 데이터

항 목	파일 경로
통화 내역	/Data/wireless/Library/CallHistory/call_history.db
문자 내역	/Data/mobile/Library/SMS/sms.db
주소록	/Data/mobile/Library/AddressBook/AddressBook.sqlitedb
캘린더	/Var/mobile/Library/Calendar/Calendar.sqlitedb
인터넷 사용 내역	/Data/mobile/Library/Safari/Bookmarks.db
이메일	/Data/mobile/Library/Mail/Envelope Index
미디어 데이터 기록	/var/Mobile/Media/Recordings/Recordings.db
지도	/var/mobile/Library/Maps/Bookmarks.plist
메모	/Data/mobile/Library/Notes/notes.sqlite
카카오톡	/var/mobile/Applications/com.iwilab.KakaoTalk/Library/PrivateDocuments/Message.sqlite
텔레그램	/var/mobile/Applications/ph.telegra.Telegraph/Documents/tgdata.db
네이트온	/com.nate.nateon/home/숫자/ntc.db.21
네이버 라인	/jp.naver.line/Documents/talk.db
드롭박스	/com.getdropbox.Dropbox/Documents/Users/318000599/Uploads.sqlite
N드라이브	/com.nhncorp.ndrive/Library/ndrive.sqlite
티맵	/com.SKTelecom.Tmap/Documents/destination_history.db
폴라리스 오피스	/kr.co.infraware.office.link/Library/PolarisOffice5.db

Ⅴ. 이슈 및 향후 연구 방향

모바일기기가 사용자에게 다양한 편의성을 제공하면서 더욱 많은 개인정보들이 모바일기기 내부에 저장되고 있다. 이에 따라 안드로이드 모바일기기 시장을 주도하고 있는 삼성과 iOS의 애플은 모바일기기에 다양한 보안 기능을 추가하고 있다.

최근 삼성은 자사의 안드로이드 모바일기기의 루팅을 막기 위한 다양한 장치를 마련하고 있고 특히 최신 갤럭시 시리즈는 한번이라도 루팅을 수행하면 데이터 암호화 기능을 제공하는 녹스와 삼성페이 등의 기능을 사용하지 못하게 하였다. iOS도 마찬가지로 탈옥을 막기 위한 많은 노력을 하고 있다. 이러한 이유로 모바일 포렌식 관점에서 데이터를 수집하는데 많은 어려움이 발생하고 있고 새로운 데이터 수집 방법의 연구 개발이 지속적으로 요구된다. 특히 임베디드 기기 특성 및 취약점을 이용한 하드웨어와 소프트웨어 역공학 기술을 사용하여 모바일기기의 데이터를 수집하는 연구가 필요할 것이다.

또한, 모바일기기 내부 데이터를 암호화함으로써 데이터를 수집하더라도 이를 분석하는데 어려움이 있다. iOS의 경우 이미 버전 4이상부터 모든 데이터를 암호화 저장하고 있으며 안드로이드의 경우 버전 6이상부터 모든 데이터를 암호화하는 기능을 추가하였다. 이 외에도 카카오톡, 텔레그램과 같은 메신저들도 데이터를 암호화하고 있다. 따라서 이를 대응하기 위해 안드로이드와 iOS의 운영체제의 데이터 암호화 알고리즘을 역분석하여 이를 복호화할 수 있는 연구가 필요하다. 이 과정에서 하드웨어 및 소프트웨어 역공학 기술과 모바일기기 동적 디버깅 등의 연구가 필요할 것이다. 애플리케이션의 암호화의 경우 애플리케이션의 설치파일을 소프트웨어 역공학 기술을 통해 암호화 알고리즘을 파악하고 이를 복호화하는 기술을 개발해야 한다.

이 외에도 안드로이드의 경우 버전 4.1부터 제공되는 공장초기화 시 데이터를 완전 삭제하는 기능을 대응하기 위해서는 사용자가 완전 삭제를 수행한 흔적과 그 시점을 판단할 수 있는 방안을 연구해야 한다. 또한, 최근 카카오톡 등의 메신저 애플리케이션에서 제공하는 데이터 완전 삭제 기능을 대응하기 위해서는 모바일기기 애플리케이션의 로그를 저장하기 위해 사용되는 SQLite DB 파일에 대한 삭제된 레코드 복구에 대한 더

욱 심화된 연구가 필요할 것이다.

참 고 문 헌

[1] NIST Special Publication 800-101 Revision1, “Guidelines on Mobile Device Forensics”, May 2014.

[2] ISO/IEC 27043, “Information technology – Security techniques – Incident investigation principles and processes”, March 2015.

[3] Mumba, Emilio Raymond and Hein S. Venter, “Mobile forensics using the harmonised digital forensic investigation process”, *2014 Information Security for South Africa IEEE*, 2014.

[4] Murphy, Cynthia A. “Developing process for mobile device forensics”, 2009.

[5] Goel, Archit, Anurag Tyagi and Ankit Agarwal, "Smartphone forensic investigation process model", *International Journal of Computer Science & Security (IJCSS)*, pp. 322-341, 6(5), 2012.

[6] TTAS.KO-12.0059, “이동 전화 포렌식 가이드라인”, *한국정보통신기술협회*, 2007.

[7] 이정훈, 천우성, “디지털 증거 수집과 분석을 위한 스마트폰 포렌식 적용 연구”, *정보보호학회지*, 21(6), pp. 56-65, 2011.

[8] 이무영, “디지털 증거 압수수색에 있어서 관련성 개념에 관한 연구 - 모바일 포렌식을 중심으로 -”, *서울대학교 융합과학기술대학원*, 2015.

[9] Konstantia Barmpatsalou, Dimitrios Damopoulos, Georgios Kambourakis and Vasilios Katos, “A critical review of 7 years of Mobile Device Forensics”, *Digital Investigation*, 10(4), pp. 323-349, December 2013.

[10] Marcel Breeuwsma, Martien de Jongh, Coert Klaver, Ronald van der Knijff and Mark Roeloffs, “Forensic Data Recovery from Flash Memory”, *SMALL SCALE DIGITAL DEVICE FORENSICS JOURNAL*, 1(1), pp. 1-7, June 2007.

[11] 이규안, “JTAG 방식을 이용한 모바일 포렌식 기법 연구”, *숭실대학교*, 2010.

[12] Ing. M.F. Breeuwsma, “Forensic imaging of embedded system using JTAG”, *Digital Investigation*, 3, pp. 32-42, 2006.

[13] Yang, Seung Jei, et al. “New acquisition method based on firmware update protocols for Android smartphones”, *Digital Investigation,* 14, pp. S68-S76, 2015.

[14] Namheun Son, Yunho Lee, Dohyun Kim, Joshua I. James, Sangjin Lee and Kyungho Lee, “A study of user data integrity during acquisition of Android devices”, *Digital Investigation,* 10, pp. S3-S11, 2013.

[15] Android Developer, “https://developer.android.com/”, 2016.

[16] 오정훈, 이상진, “안드로이드 스마트폰 포렌식 분석 방법에 관한 연구”, *고려대학교 정보보호대학원*, 2012.

[17] Cellebrite UFED, “http://www.cellebrite.com/”, 2016.

[18] XRY, https://www.msab.com/, 2016.

[19] 형사소송법 제106조 3항, “http://www.law.go.kr/법령/형사소송법”, 2016.

[20] Jonathan Zdziarski, “Identifying back doors, attack points, and surveillance mechanisms in iOS devices”, *Digital Investigation*, 11, pp. 3-19, 2014.

[21] evasi0n, “http://evasi0n.com/”, 2106

[22] PanGu, “http://en.7.pangu.io/”, 2016.

[23] TaiG, “http://www.taig.com/en/”, 2016.

[24] libimobiledevice, “ http://www.libimobiledevice.org/”, 2016.

[25] Joe Sylve, Andrew Case, Lodovico Marziale and Golden G. Richarda, “Acquisition and analysis of volatile memory from android devices”, *Digital Investigation*, 8(3), pp. 175-184, February 2012.

[26] LiME, “https://github.com/504ensicsLabs/LiME”, 2016.

[27] Fabio Casadei, Antonio Savoldi and Paolo Gubian, “Forensics and SIM cards: an Overview”, *International Journal of Digital Evidence*, 5(1), Fall 2006.

〈저 자 소 개〉

김 도 현 (Dohyun Kim)
학생회원

2011년 2월 : 서울과학기술대학교 컴퓨터공학과 졸업
2013년 8월 : 고려대학교 정보보호대학원 정보보호학과 석사
2013년 9월 ~ 현재 : 고려대학교 정보보호대학원 박사과정
관심분야 : 디지털 포렌식, 모바일 포렌식

이 상 진 (Sangjin Lee)
종신회원

1987년 2월 : 고려대학교 수학과 졸업
1989년 2월 : 고려대학교 수학과 석사
1994년 8월 : 고려대학교 수학과 박사
1989년 10월 ~ 1999년 2월 : ETRI 선임 연구원
1999년 3월 ~ 2001년 8월 : 고려대학교 자연과학대학 조교수
2001년 9월 ~ 현재 : 고려대학교 정보보호대학원 교수
2008년 3월 ~ 현재 : 고려대학교 디지털포렌식연구센터 센터장
2012년 7월~2013년 12월 : 디지털포렌식연구회 회장
2013년 2월~현재 : 고려대학교 정보보호대학원 부원장
2013년 11월~현재 : 한국디지털포렌식학회 회장
관심분야 : 디지털 포렌식, 심층 암호, 해쉬 함수