

논문 2026-3-2 <http://dx.doi.org/10.29056/jsf.2026.09.02>

삼성 Smart Switch를 통한 데이터 백업 시 모바일포렌식 복원율에 관한 연구

김영준*†

A Study on the Mobile Forensics Restoration Rate for Data Backup with Samsung Smart Switch

Youngjune Kim*†

요 약

삼성 Smart Switch는 기존 스마트폰의 연락처, 사진, 메시지, 앱 설정 등 데이터를 새로운 갤럭시 기기로 무선 또는 USB 케이블을 통해 간편하게 전송하거나 백업하는 기능을 제공하는 애플리케이션이다. 특히 최근에는 범죄자들이 범죄를 은폐할 목적으로 기존에 사용하고 있던 스마트폰을 폐기하고 삼성 Smart Switch와 같은 백업 기능을 사용하여 이전부터 사용하고 있던 스마트폰인 것처럼 데이터를 조작, 악용하는 사례가 발생하고 있다. 따라서 본 논문에서는 삼성 Smart Switch를 통한 데이터 백업 시 모바일포렌식 복원율에 대하여 다루고자 하며, 데이터 획득은 스마트폰 내 모든 데이터에 접근할 수 있는 권한을 부여하기 위해 루팅된 상태에서 데이터를 추출하고 삼성 Smart Switch를 이용하여 다른 루팅된 스마트폰 기기로 데이터를 전송하는 방법을 수행하였다. 이후 기존 스마트폰과 백업된 스마트폰의 데이터 복원율을 비교하였고, 도출된 결과에 따른 수사활용 방안에 대해 제시한다.

Abstract

Samsung Smart Switch is an application that provides features to easily transfer or back up data—such as contacts, photos, messages, and app settings—from an existing smartphone to a new Galaxy device via wireless connection or a USB cable. Recently, however, instances have emerged where criminals dispose of their current smartphones to conceal crimes and misuse backup features like Samsung Smart Switch to manipulate data, making a device appear as if it had been used all along. Therefore, this paper examines the mobile forensic recovery rate during data backup via Samsung Smart Switch. For data acquisition, data was accumulated on a rooted smartphone to grant full access permissions to all internal data, and Samsung Smart Switch was then used to transfer the data to another rooted device. Subsequently, the data recovery rates between the original and the backed-up smartphones were compared, and practical investigative applications based on the findings are presented.

한글키워드 : 모바일포렌식, 데이터 백업, 스마트폰, 안드로이드, 삼성 스마트 스위치

keywords : Mobile Forensics, Data Backup, Smartphone, Android, Samsung Smart Switch

* 서울경찰청 사이버수사과 사이버수사관, 공학박사

† 교신저자: 김영준(email: storesomeday@gmail.com)

접수일자: 2026.08.01. 심사완료: 2026.08.25.

게재확정: 2026.09.20.

1. 서론

국가통계포털에서 공개한 2022년 ~ 2024년까지 국내 스마트폰 제조사별 점유율에 따르면 <표 1>와 같이 국내 스마트폰 보유자 중 80%를 상회하는 제조사는 삼성전자인 것을 알 수 있다.

표 1. 스마트폰 제조사별 점유율
Table 1. Market Share by Smartphone Manufacturer

Year	Samsung	LG	Apple	etc
2024	82.7%	1.9%	15.2%	0.2%
2023	84.4%	3.0%	12.5%	0.1%
2022	83.2%	5.0%	11.7%	0.1%

삼성 스마트폰은 구글 안드로이드 운영체제를 기본 커널 및 플랫폼 구조로 채택하고 있어 안드로이드 파일 시스템 및 데이터 관리 체계를 기반으로 동작한다. 그리고 삼성전자는 자사의 갤럭시 기기 간 데이터 이전 및 백업 편의성을 도모하기 위해 삼성 Smart Switch 애플리케이션을 기본적으로 제공한다. 이용자는 이 애플리케이션을 통해 무선 네트워크 또는 USB 케이블 연결만으로 기존 스마트폰에 저장된 연락처, 사진, 메시지, 통화 기록, 앱 설정 등 다양한 사용자 데이터를 새로운 갤럭시 기기로 간편하게 이전하거나 백업할 수 있다.

그러나 이러한 데이터 백업 및 전송 기능의 편리성은 최근 범죄 현장에서 증거 인멸 및 조작의 수단으로 악용되는 부작용을 야기하고 있다. 특히 피의자가 범죄 행위에 사용하던 기존 스마트폰을 의도적으로 폐기·파손한 후, 삼성 Smart Switch 백업 기능을 활용해 데이터를 새 기기로 전송함으로써 마치 해당 기기를 이전부터 지속해서 사용해 온 것처럼 데이터 현황을 연출하거나

조작하는 사례가 발생하고 있다. 이와 같은 데이터 은폐 시도는 원본 기기 여부를 불확실하게 만들 수 있을 뿐만 아니라 데이터 완전성을 입증하는데 제한요소로 작용할 가능성이 높다.

이에 따라 백업 기기에 잔재하는 데이터의 포렌식적 가치를 정밀하게 평가하고 수사 가이드라인을 수립하기 위해서는 삼성 Smart Switch를 거친 데이터 백업 시 전·후의 포렌식 복원율을 종합적으로 검증할 필요가 있다.

본 논문에서는 삼성 Smart Switch를 통한 데이터 백업 시 모바일포렌식 데이터 복원율을 분석하고자 한다. 이를 위해 스마트폰 내 모든 시스템 및 데이터 영역에 접근할 수 있는 권한을 확보한 루팅 상태에서 실생활 환경 수준의 데이터를 축적한 후, 삼성 Smart Switch를 이용하여 다른 루팅된 스마트폰으로 데이터를 이전하는 실험을 수행하였다. 이후 기존 원본 스마트폰과 백업 대상 스마트폰 간의 아티팩트 복원율을 비교·분석함으로써, 백업 솔루션이 악용된 디지털 범죄 수사 현장에서 적용할 수 있는 실질적인 수사 활용 방안을 제시한다.

2. 선행 연구

2.1 안드로이드 모바일포렌식

안드로이드 모바일포렌식은 물리적, 논리적 기법으로 나눌 수 있고, 물리적 기법에는 chip-off, JTAG 방식이 있다[1]. 그러나 이러한 방법의 경우 메인보드에서 플래시메모리를 분리하거나 JTAG 포트를 없애는 방법으로 스마트폰이 출하되고 있어 적용이 매우 제한적이다[2].

최근 안드로이드 스마트폰 기종에 물리적 기법을 적용할 수 없기에 논리적 기법을 적용하여야 하는데, 논리적 기법에는 펌웨어 업데이트 프로토콜, 루팅, 데이터 공유 프로토콜 등을 이용하

는 방식이 존재한다[3]. 그중 범용성이 넓고 전체 데이터를 확보할 수 있는 방법인 루팅에 대한 연구를 중점적으로 살펴보고자 한다.

2.2 루팅

루팅은 안드로이드 스마트폰의 펌웨어 내부의 커널 이미지를 관리자 권한을 갖도록 수정하고 스마트폰의 커널 영역에 덮어씌운 뒤 해당 커널 이미지로 부팅하여 관리자 권한을 획득하는 방법이다[4]. 스마트폰이 루팅된 상태라면 USB 디버깅 모드가 활성화된 상태에서 대상 파티션에 해당하는 블록 장치명인 “ADB Shell” 명령으로 접속한 다음 이미지를 위한 “dd”와 데이터 전송을 위한 “netcat”를 조합하여 전체 메모리를 덤프하는 방식으로 이미지를 생성할 수 있다.

Stefan Maus의 연구[5]에서는 포렌식 추출 과정에서는 안드로이드 스마트폰의 모든 앱으로부터 데이터를 확보하기 위해 적절한 접근 권한이 필요하고 이러한 포괄적인 접근 권한은 스마트폰을 루팅함으로써 얻을 수 있으며, 루팅된 안드로이드 스마트폰을 기준으로 지리 데이터를 획득하여 분석하였다.

또한 박은후의 연구[6]에서는 당시 최신 버전(안드로이드 9)의 삼성 스마트폰의 루팅과 비루팅 방식에서 수집할 수 있는 로그 데이터를 비교하였는데 총 60개 타입 중 루팅시 기기의 편차는 존재하였지만 루팅 상태에서는 대부분 획득이 가능하였고 비루팅 상태에서는 34개 타입만 획득이 가능하였다. 이는 루팅 과정을 거쳐야만 비로소 전체 데이터에 접근할 수 있음을 의미한다.

그러나 루팅 과정에서 메모리에 저장된 증거물의 무결성이 손상된다면 실제 수사 과정에서는 증거로서의 능력을 상실하게 된다. 루팅 과정에서 메모리에 저장된 증거물의 무결성이 손상될 위험성을 우려하는 목소리가 존재하는 가운데 손남현의 연구[7]에서는 리커버리 이미지 획득 방

식을 이용하여 루팅하는 경우 데이터 영역의 무결성이 보존된다는 연구를 도출하기도 하였다.

2.3 삼성 Smart Switch

삼성에서는 삼성 스마트폰에 저장되어 있는 개인정보, 계정 정보 등을 PC에 동기화할 수 있도록 삼성 스마트폰 백업 프로그램을 지원하고 있다. 현재는 삼성 Smart Switch 프로그램을 지원하고 있지만 이전에는 Kies 프로그램을 지원해 왔다. 이에 이규원의 연구[8]에서는 Kies 백업 파일의 구조를 분석하고 복원하는 기법을 제안하기도 하였다.

Kies 프로그램 이후 삼성 Smart Switch가 새롭게 출시되었고 박명서의 연구[9]에서는 삼성 Smart Switch 4.1.16. 버전에 대해 분석하고 리버스 엔지니어링하여 삼성 Smart Switch로 생성되는 PIN 기반 백업 암호화 프로세스를 도출하기도 하였다. 이후 박명서의 다른 연구[10]에서는 삼성 Smart Switch의 암호 방식에 대해서 정리하였는데 스마트폰 상에서 PIN을 입력하면 백업 데이터가 암호화되고 키 생성은 일방향 암호인 SHA256, SHA1 등을 사용하며, 암호 알고리즘 및 운영모드는 AES-ECB과 AES-CBC를 사용한다. 키 생성 알고리즘과 암호화는 암호화 대상 백업 파일의 확장자에 따라 달리 적용된다는 점을 확인하였다.

3. 실험환경 구성

본 연구에서는 삼성 Smart Switch를 통한 데이터 백업 시 모바일포렌식 복원율에 관한 연구를 위해 루팅을 통해 관리자 권한을 확보함으로써 시스템 영역 접근이 가능하도록 환경을 구성하고자 한다. 이를 위해 동일 기종의 삼성 스마트폰 2대를 모두 루팅 과정을 진행하였다.

3.1 루팅 과정

모바일 스마트폰 기종은 삼성 보급형 스마트폰으로 갤럭시 Wide 6, 안드로이드 14가 탑재된 최신 버전의 스마트폰을 선정하였다. 루팅을 위해 개발자 옵션을 활성화하고, 부트로더 잠금 해제와 USB 디버깅 활성화하였다.

이후 부트스트랩 로더를 잠그고 스마트폰 전체 초기화를 진행하였으며, 다시 개발자 옵션 생성 작업하여 부트로더 잠금 해제 활성화 및 음영 처리여부 확인 후 USB 디버깅을 활성화하였다.

안드로이드를 루팅하고 루팅 상태를 관리하기 위해 Magisk 애플리케이션을 이용하였으며, 스마트폰에 Magisk 애플리케이션을 활성화시킨 다음 작업 PC에 Odin(ROM 플래싱 도구) 설치, 갤럭시 Wide 6 순정 펌웨어 다운로드를 진행하고 그중 AP 파일을 스마트폰 다운로드 폴더로 복사 이동한 뒤 스마트폰 내에서 Magisk 실행 후 설치를 진행하였다.

파일에서 magisk_patched 파일이 생성된 것이 확인되었다면 컴퓨터의 펌웨어 폴더로 복사 이동 시킨 뒤 스마트폰 전원을 종료하고 다운로드 모드 진입 및 작업 PC에서 Odin을 실행, AP에는 magisk_patched 파일을 그리고 순정 펌웨어를 통해 다운로드한 파일을 BL, CP, CSC에 삽입하였다. 이 과정을 반복하여 <그림 1>와 같이 삼성 스마트폰의 루팅을 완료하였다.

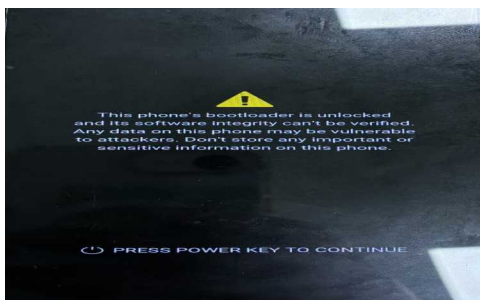


그림 1. 삼성 스마트폰 루팅
Fig. 1. Samsung smartphone rooting

3.2 도구 선정

모바일포렌식 복원율에 관한 연구를 위해 모바일포렌식 도구로 범죄자들이 가장 많이 사용하고 있는 텔레그램, 카카오톡, 인스타그램, 라인, 슬랙 등 모바일 아티팩트 분석을 지원하는 MAGNET AXIOM forensics 도구를 모바일포렌식 도구로 선정하였다. 그리고 MAGNET AXIOM forensics 도구는 운영시스템 Windows 10 이상, CPU 8-16 Logical Cores, GPU Compute capability 5.0 등의 사양을 요구하고 있으므로 해당 사양을 충족하는 삼성 노트북(NT550XDA)을 이용하여 분석을 진행하였다.

3.3 삼성 Smart Switch 활용 데이터 동기화

스마트폰 내 모든 시스템 및 데이터 영역에 접근할 수 있는 권한을 확보한 루팅 상태에서 실생활 환경 수준의 데이터를 축적하였다. 이후 <그림 2>와 같이 삼성 Smart Switch 버전 3.7.71.16를 이용하여 다른 루팅된 스마트폰으로 데이터를 이전하는 실험을 수행하였다. 데이터 이전 시 추가 데이터가 발생하지 않도록 기존 스마트폰에는 비행기 모드를 설정하였고, 이전되는 스마트폰에는 별도의 유심을 넣지 않음으로써 데이터 통신이 되지 않도록 구성하였다.



그림 2. 삼성 Smart Switch 활용 데이터 동기화

Fig. 2. Data synchronization using Samsung Smart Switch

그 결과, 이전되는 스마트폰에 439개 항목, 9.69GB의 데이터가 전송 완료된 것으로 표시되었다.



그림 3. 데이터 전송 결과
Fig. 3. Data Transmission Result

4. 모바일포렌식 복원을

범죄 행위를 규명함에 있어 포렌식을 통해 복원된 증거는 매우 중요한 요소이다. 포렌식 증거는 수사관들이 범죄를 재구성하는 데 도움을 줄 수 있으며, 범죄자의 행동 및 동기를 파악할 수 있게 한다[11]. 권홍균 연구[12]에서는 디지털 장치에 남아 있는 애플리케이션 사용 패턴을 분석하는 사용자 프로파일링 모델을 제시하기도 하였다.

이에 4장에서는 아티팩트별로 구분하여 모바일포렌식 복원율을 산정하고자 한다.

데이터의 비교 및 구분하기 위해 기존 스마트폰에 대한 모바일포렌식 과정을 통해 확보한 데이터를 <CASE 1>, 삼성 Smart Switch를 통해 데이터를 이전한 스마트폰을 모바일포렌식 하여 확보한 데이터를 <CASE 2>로 한다.

또한 데이터 삭제 환경에서의 복원 가능 여부를 검증하기 위해 웹 브라우저, 커뮤니케이션, 소셜 네트워킹 서비스, 미디어, 이메일, 캘린더 및 문서 항목의 데이터 중 일부를 인위적으로 삭제하였다. 모바일포렌식 절차를 통해 복원한 아티

팩트별 데이터 수와 복원율은 <표 2>와 같다.

특히 <CASE 1> 대비 <CASE 2>의 복원율은 미삭제 데이터와 삭제 데이터로 구별하여 산출하였다. 이중 삭제 데이터의 복원율이 0%로 산출된 항목은 백업 및 데이터 전송 과정에서 기존 스마트폰의 삭제된 아티팩트 데이터가 대상 기기로 이전되지 않았음을 의미한다.

4.1 웹 아티팩트

<CASE 1> 웹 아티팩트에는 캐시 레코드, 쿠키, 파비콘, 탭 기록, 웹 기록, 웹 방문 활동 데이터가 복원되었으며, DB 내 미할당 영역(Unallocated Block) 및 WAL(Write-Ahead Log) 파싱을 통해 삭제된 웹 방문 기록 및 검색 쿼리의 복원이 가능하였다.

그러나 <CASE 2>에서는 웹 브라우저의 캐시, 쿠키, 파비콘 및 세션 탭 기록 등 주요 웹 아티팩트 정보가 마이그레이션 대상에서 제외되어 복원되지 않았다.

4.2 커뮤니케이션 아티팩트

커뮤니케이션 아티팩트는 범행에 많이 사용되는 애플리케이션인 카카오톡, 라인, 슬랙, 텔레그램, 스냅챗, 삼성 메시지에 대한 데이터를 축적하였다. 안드로이드 연락처의 경우 시그널 애플리케이션과의 연동을 통해 연락처가 자동 설정되도록 조치하여 동기화 데이터의 복원 여부를 확인하고자 하였다.

분석 결과, <CASE 1>에서는 삼성 메시지 및 안드로이드 연락처의 경우 SQLite DB 내 Free List 및 Journal/WAL 영역 파싱을 통해 삭제된 메시지 및 연락처 데이터의 복원율이 높게 나타났다. 카카오톡을 예시로 들자면 'data/data/com.kakao.talk/files/datastore/LocalUser_DataStore.pref.preferences_pb' 파일 파싱을 통해 추출한 사용자 고유 식별자(User ID)로 압

호화된 DB(KakaoTalk.db)의 복호화 키를 산출한 후, DB 내부 미할당 영역(Unallocated Block) 및 WAL 영역을 분석함으로써 삭제된 메시지 및 대화방 흔적을 복원할 수 있었다. 또한 안드로이드 연락처 및 삼성 메시지 역시 높은 복원율을 보였다.

반면 <CASE 2>에서는 삼성 Smart Switch의 데이터 백업 정책에 따라 기본 문자(삼성 메시지) 및 연락처는 이전·복원되었으나, 카카오톡을 제외한 메신저 앱의 웹 아티팩트 정보가 마이그레이션 대상에서 제외되어 복원되지 않았을 뿐만 아니라 계정 재인증 과정에서 로컬 DB가 초기화되어 삭제된 메시지가 복원되지 않은 한계를 보였다.

4.3 소셜 네트워킹 아티팩트

소셜 네트워킹 아티팩트는 인스타그램, 트위터 데이터를 대상으로 포렌식을 수행하였다. <CASE 1>에서 인스타그램은 앱 내부 캐시 데이터 및 로컬 DB 파싱(BootstrapService.xml, direct.db)을 통해 팔로잉, 팔로워, 사용자 데이터, Direct Message 캐시 및 미디어 등 아티팩트를 복원하였고 트위터도 앱 내부 캐시 데이터 및 로컬 DB 파싱(twitter.db, direct_messages.db)을 통해 팔로잉, 팔로워, 사용자 데이터, message, 트윗 정보 등 아티팩트를 복원할 수 있었다.

그러나 <CASE 2>에서는 앱 마이그레이션 시 로컬 보안 캐시가 이전되지 않아 세션 정보 및 기존 로컬 DB가 제거되었으며, 재로그인 시 서버로부터 활성 데이터만 새로 동기화됨에 따라 삭제된 메시지 데이터 및 활동 로그의 복원은 불가능하였다.

4.4 미디어 아티팩트

미디어 아티팩트는 오디오, 사진, 동영상 파일 데이터를 대상으로 분석을 진행하였다.

<CASE 1>에서는 파일 시스템 레벨의 deletion flag 설정 이후 플래시 메모리의 TRIM 기능 작동 여부에 따라 원본 미디어 파일의 카빙 복원율이 결정되었다. 원본 파일이 삭제·초기화된 경우에도 썸네일 DB(thumbnails.db) 및 캐시 폴더 내 축소판 이미지 파싱을 통해 삭제된 미디어의 시각적 흔적을 상당수 복원할 수 있었다.

<CASE 2>의 경우 삼성 Smart Switch 이전 과정에서 삭제된 미디어 파일 및 썸네일 캐시는 이전 대상에서 제외되어, 활성 미디어 파일만 이전되고 삭제된 미디어 데이터는 복원되지 않았다. 이는 휴지통 기능을 통해 보관되고 있는 데이터도 이전되지 않기에 복원되지 않았다.

4.5 이메일 및 캘린더 아티팩트

이메일 및 캘린더 아티팩트는 Gmail (com.google.android.gm) 및 안드로이드 캘린더 프로바이더(com.android.providers.calendar) 데이터를 대상으로 분석을 진행하였다.

<CASE 1>에서는 추출된 로컬 동기화 DB인 bigTopDataDB 및 calendar.db 파싱을 수행하였으며, DB 내 Free List 및 WAL 영역 조회를 통해 삭제 처리된 일정 및 이메일 헤더/본문 정보의 일부 복원이 가능하였다.

반면 <CASE 2>에서는 삼성 Smart Switch 마이그레이션 및 계정 재동기화 과정을 통해 활성 상태의 캘린더 이벤트 및 이메일 데이터는 정상 수신되었으나, 마이그레이션 과정에서 기존 로컬 DB의 삭제 레코드 및 Rollback Journal/WAL 흔적이 이전 대상에서 제외되어 삭제 데이터의 복원율은 0%로 나타났다.

4.6 문서 아티팩트

문서 아티팩트는 엑셀(xls, csv), 한글(hwp, hwp), PDF, 텍스트(txt) 파일 형태의 데이터를 분석하였다.

<CASE 1>에서는 파일 자체 삭제 시 NAND Flash의 TRIM 특성으로 인해 원본 카빙 복원율은 낮았으나, 문서 편집 과정에서 생성된 임시 파일(.tmp), 자동 저장 파일, 최근 문서 목록(MRU) 파싱을 통해 문서의 일부 내용 및 열람 흔적을 복원할 수 있었다.

<CASE 2>에서는 마이그레이션 시 최종 저장된 정상 문서 파일만 이전되었으며, 임시 파일 및 삭제된 문서 흔적은 이전되지 않아 복원되지 않았다. 미디어 아티팩트와 동일하게 휴지통 기능을 통해 보관되고 있는 데이터도 이전되지 않기에 복원되지 않았다.

표 2. 아티팩트별 복원율
Table 2. Recovery Rate by Artifact
※ Number of Recovered Items (Non-deleted Data / Deleted Data)

Artifacts		<CASE 1>	<CASE 2>	Recovery Rate (CASE 2 compared to CASE 1)
Web	Chrome Cache Records	42(29/13)	0	0%(0%/0%)
	Chrome Cookies	72(57/15)	0	0%(0%/0%)
	Chrome Favicons	16(10/6)	0	0%(0%/0%)
	Chrome Tab History	35(20/15)	0	0%(0%/0%)
	Chrome Web History	18(10/8)	0	0%(0%/0%)
	Chrome Web Visits	55(38/17)	0	0%(0%/0%)
Communication	Android Contacts	1,510(1,310/200)	1,210(1,210/0)	80%(80%/0%)
	KakaoTalk (Chat Rooms, Friends, Messages)	2,930(2,307/623)	2,930(2,307/623)	100%(100%/100%)
	LINE (Chats, Contacts, Messages, Photos)	896(793/103)	0	0%(0%/0%)
	Slack (Accounts, Channels, Direct Messages, Users)	76(44/32)	0	0%(0%/0%)
	Snapchat	108(62/46)	0	0%(0%/0%)
	Telegram (Chats, Messages, Users)	1,028(728/300)	0	0%(0%/0%)
	Samsung Messages	824(746/78)	746(746/0)	90.5(90.5/0)
Social Networking	Instagram	1,348(1,125/223)	0	0%(0%/0%)
	Twitter	832(706/126)	0	0%(0%/0%)
Media	Audio	345(297/48)	297(297/0)	86.1%(86.1%/0%)
	Photos	40,629(32,432/8,197)	32,432(32,432/0)	79.8%(79.8%/0%)
	Videos	177(90/87)	87(87/0)	49.2%(49.2%/0%)
Email & Calendar	Calendar Events	192(177/15)	177(177/0)	92.2%(92.2%/0%)
	Gmail Email	444(413/31)	413(413/0)	93%(93%/0%)
Documents	Excel (xls, csv, etc.)	87(64/23)	64(64/0)	73.5%(73.5%/0%)
	HWP (hwp, hwp, etc.)	109(75/34)	75(75/0)	68.8%(68.8%/0%)
	PDF	68(46/22)	46(46/0)	67.6%(67.6%/0%)
	Text(txt etc)	458(342/116)	342(342/0)	74.7%(74.7%/0%)
Location & Travel	Wi-Fi Profiles	15	15	100%
	Google Maps	42(31/11)	31(31/0)	73.8%(73.8%/0%)

4.7 위치 및 여행 아티팩트

위치 및 여행 아티팩트는 Wi-Fi 프로파일 저장소 (data/misc/apexdata/com.android.wifi/WifiConfigStore.xml) 및 Google Maps 데이터를 대상으로 분석을 수행하였다.

<CASE 1>에서는 WifiConfigStore.xml 파일 파싱을 통해 기기에 접속 및 저장되었던 Wi-Fi 네트워크의 SSID, 보안 모드(Security Mode), 네트워크 암호(Pre-Shared Key), 네트워크 유형, 항목 ID(Network ID) 등의 세부 식별 정보가 식별 및 복원되었다. 또한 Google Maps의 로컬 캐시 DB(gmm_storage.db 등) 파싱을 통해 삭제된 검색 장소 및 방문 좌표값의 복원이 가능하였다.

<CASE 2>의 경우 저장된 Wi-Fi 프로파일 정보(SSID, 보안 모드, 암호 등)는 삼성 Smart Switch의 시스템 설정 이전 정책에 따라 정상적으로 마이그레이션되어 높은 복원율을 유지하였으나, Google Maps의 로컬 위치 캐시 및 삭제된 검색 좌표 정보는 마이그레이션 대상에서 제외되어 복원되지 않았다.

5. 수사활용 방안

디지털 포렌식 수사 과정에서 대상 기기가 삼성 Smart Switch를 통한 데이터 마이그레이션을 거친 경우, 수사관은 분석 결과에 대한 증거능력 확보 및 범죄 사실의 입증에 위해 단순 데이터 확보를 넘어 데이터가 이전된 사실 자체와 그 정확한 수행 시기를 과학적으로 증명해야 한다.

이를 위해 수사관은 다음과 같은 아티팩트 및 로그 분석 기법을 종합적으로 활용하여 마이그레이션 행위를 특정할 수 있다. 우선 삼성 Smart Switch 전용 시스템 로그 및 백업 관련 아티팩트 파싱을 통한 직접적인 타임스탬프 확보가 가능하다. 수사관은 data/data/com.sec.android.easyMover/

또는 com.samsung.android.smartswitchbz 경로 내부에 존재하는 데이터베이스 및 XML, 로그 파일을 확인한다. 해당 경로의 smartswitch.log 및 transfer_history.db 등의 파일 내부에는 데이터 동기화의 성공 여부뿐만 아니라 마이그레이션이 시작되고 종료된 정확한 시각이 직접 기록되어 있어 동기화 시점을 명확히 입증할 수 있다.

이와 함께 시스템 이벤트 로그를 파싱함으로써 삼성 Smart Switch 패키지가 실행된 최초 시각과 대량의 백업 및 복원 I/O 작업이 집중적으로 일어난 시간대를 교차 검증하여 특정한다.

다음으로 파일 시스템의 생성 시각과 내부 데이터베이스 레코드 타임스탬프 간의 불일치성을 분석하는 기법을 적용한다. 스마트폰 내 사진, 동영상, 문서 등 미디어 파일과 DB 파일들의 메타데이터를 확인하면 실제 파일이 최초 촬영되거나 작성된 날짜와는 무관하게 삼성 Smart Switch 동기화가 이루어진 특정 일시에 수천 개 파일의 생성 및 수정 시각이 동일하게 군집화되는 현상이 관찰된다.

또한 앱 내부 레코드의 작성 시각은 수년 전 과거로 기록되어 있는 반면, 정작 해당 DB 파일 자체의 파일 시스템 생성 시각(FileSystem Birth/Creation Time)은 특정 단일 시점에 고정되어 나타나며, 수사관은 이러한 타임스탬프 불일치 분석을 통해 데이터가 외부로부터 일괄 복원된 시점을 산출해낼 수 있다.

마지막으로 데이터 이전 과정에서 필연적으로 발생하는 네트워크 및 하드웨어 연결 흔적 파싱을 수행한다. 삼성 Smart Switch가 무선 방식으로 실행된 경우, Wi-Fi Direct 및 블루투스 연결 로그가 기록되는 WifiConfigStore.xml, bt_config.conf의 수정 시기를 확인함으로써 데이터 마이그레이션 행위의 물리적 실행 시점을 재구성할 수 있다.

삼성 Smart Switch가 실행한 시점이 특정되었

다면 웹 브라우저, 제3자 메신저(LINE, Slack, Snapchat, Telegram), SNS(Instagram, Twitter) 아티팩트의 경우 이전 후 복원율이 0%로 나타나기에 활성화 데이터와 카카오톡 복원으로만 범행을 증명할 수 있는 경우와 아닌 경우로 구분하여 수사의 방향을 설정할 필요가 있다.

파일 이름 **bt_config.conf**
 파일 확장명 **.conf**
 논리적 크기 **630 bytes**
 수정됨 **2026-02-09 PM 12:51:23.000**
 MD5 해시 **01f247397c0fce7bbf133012a39789a7**
 증거 정보
 소스 **samsung SM-A1365 논리적 이미지 Image - Data.tar\data**
 \misc\bluedroid\bt_config.conf

그림 4. bt_config.conf
 Fig. 4. bt_config.conf

파일 이름 **WifiConfigStore.xml**
 파일 확장명 **.xml**
 논리적 크기 **5,958 bytes**
 수정됨 **2026-02-09 PM 12:51:12.000**
 MD5 해시 **cfe2dd69dcd0139b01fa6bc30ca45652**
 증거 정보
 소스 **samsung SM-A1365 논리적 이미지 Image - Data.tar\data**
 \misc\apexdata\com.android.wifi\WifiConfigStore.xml

그림 5. WifiConfigStore.xml
 Fig. 5. WifiConfigStore.xml

활성 데이터 및 카카오톡 복원 데이터만으로 범행 입증이 가능한 경우는 삼성 Smart Switch 이전 후에도 정상 유지되는 활성 데이터(사진·동영상, 삼성 메시지, 연락처, Wi-Fi 프로필 등)와 카카오톡 복원 데이터 내에 핵심 범죄 혐의점이 직접적으로 포함되어 있는 경우이다. 카카오톡의 경우 LocalUser_DataStore.pref.preferences_pb 파일을 통해 추출한 User ID로 DB 복호화 키를 산출하여 대화내역 및 WAL 영역의 삭제 흔적을 완벽히 재구성하고, 이를 핵심 직접증거로 채택한다. 마이그레이션 시 100% 이전된 Wi-Fi 프로필(WifiConfigStore.xml)의 SSID/BSSID 정보, 마이그레이션 시점 이전에 작성된 미디어 파일의 EXIF GPS 메타데이터, Google Maps 및 캘린더의 활성 일정을 결합하여 피의자의 범행 당시 물리적 동선과 알리바이를 입증하는데 적용할 수 있다.

활성 데이터 및 카카오톡 복원 데이터만으로 범행 입증이 불가능한 경우에는 범행의 주요 수단이 LINE, Telegram, Slack, Snapchat 등 제3자 메신저나 Instagram, Twitter 등 SNS DM, 또는 Chrome 웹 브라우저의 비밀 모드/검색 쿼리였거나, 피의자가 마이그레이션 직전 이전 기기에서 미디어·문서 파일 등을 의도적으로 삭제하여 단말기에 데이터가 이전되지 않은 경우이다. 이때는 원본 단말기 및 백업 매체 확보 및 외장 SD 카드, PC 백업 데이터에 대한 정보 획득이 필요하다. 또한 Google 계정 백업, 카카오톡 독서랍, 인스타그램 계정 데이터 다운로드 등 클라우드 서버에 동기화되어 있는 백업 아티팩트를 확보하여 로컬 단말기에서 소실된 삭제 흔적을 보완한다.

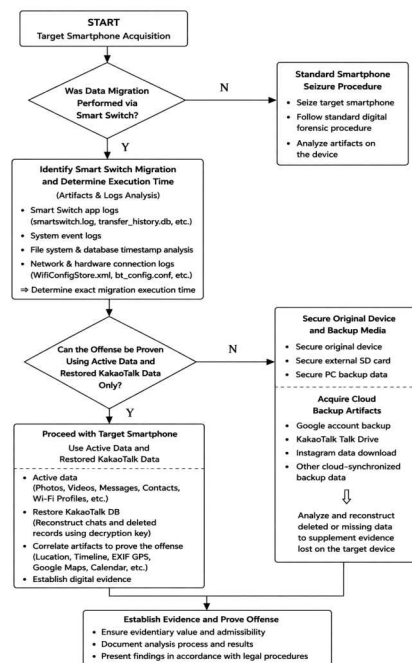


그림 6. 삼성 Smart Switch를 통한 데이터
 백업 여부에 관한 증거 확보 절차
 Fig. 6. Evidence Acquisition Procedure for
 Verifying Samsung Smart Switch Data
 Backup

이를 <그림 6>와 같이 삼성 Smart Switch를 통한 데이터 백업 여부에 관한 증거 확보 절차로 정립하였다.

6. 결론

본 연구에서는 국내 모바일 시장의 과반을 차지하는 삼성 스마트폰 환경에서 데이터 백업 및 마이그레이션 솔루션인 삼성 Smart Switch가 악용된 디지털 범죄 수사 현장에 적용할 수 있는 실질적인 포렌식 수사 가이드라인을 제시하고자 하였다. 이를 위해 안드로이드 14 기반의 동일 기종 스마트폰 2대를 루팅하여 실생활 수준의 데이터를 축적한 후, 마이그레이션 전과 후의 7개 영역 아티팩트 복원율을 종합적으로 비교·분석하였다.

실험 분석 결과, 삼성 Smart Switch를 통한 데이터 이전 시 기본 애플리케이션의 활성 데이터(카카오톡 100%, Gmail 93%, 삼성 메시지 90.5%, Wi-Fi 프로파일 100% 등)는 높은 복원율을 보였으나, DB 내 미할당 영역, Free List, Journal/WAL 영역에 존재하던 삭제 데이터의 복원율은 카카오톡을 제외한 사실상 0%에 수렴하는 한계를 보였다. 특히 웹 브라우저(Chrome), 제3자 메신저(LINE, Slack, Telegram, Snapchat), SNS(Instagram, Twitter) 아티팩트의 경우 로컬 보안 캐시 및 계정 세션이 승계되지 않거나 계정 재인증 과정에서 로컬 DB가 초기화되어 마이그레이션 이후 단말기 자체 포렌식만으로는 소실된 삭제 흔적을 확보할 수 없음을 규명되었다.

삼성 Smart Switch를 통한 데이터 이전 시 수사한계를 극복할 수 있는 방안으로 수사관은 마이그레이션이 수행된 대상 기기 분석 시 삼성 Smart Switch 전용 로그(smartswitch.log, transfer_history.db) 파싱, 파일 시스템 생성 시

각과 DB 레코드 타임스탬프 간 불일치(군집화 현상) 분석, P2P/USB 연결 흔적(WifiConfigStore.xml, 커널 로그) 파싱을 통해 마이그레이션 행위 및 정확한 실행 시점을 정밀하게 특정하여 삼성 Smart Switch를 활용하여 데이터 백업이 진행되었는지를 확인한다.

삼성 Smart Switch를 활용하여 데이터 백업이 진행된 경우 활성 데이터 및 카카오톡 DB 복호화를 통한 증거 입증이 가능하다면 해당 휴대전화를 모바일포렌식하여 혐의 구증할 수 있다. 그러나 이러한 방법으로 증거 입증이 불가능할 시에는 원본 단말기 및 백업 매체 확보 및 외장 SD카드, PC 백업 데이터에 대한 정보 획득 또는 클라우드 서버에 동기화되어 있는 백업 아티팩트를 확보하여 로컬 단말기에서 소실된 삭제 흔적을 보완할 수 있게 된다.

본 연구는 삼성 Smart Switch를 통한 데이터 백업 시 모바일포렌식 복원율에 관한 연구를 통해 실제 수사 현장에서 적용 가능한 절차를 제시하였다는 점에서 그 의의가 있다. 다만, 본 연구의 한계로 삼성 스마트폰 내 데이터 백업 환경에서 연구가 진행되어 타 제조사 간 교차 마이그레이션 시 발생하는 아티팩트 변동성에 대한 비교 분석까지는 진행되지 않았다.

향후 연구에서는 안드로이드-iOS 이중 OS 간 삼성 Smart Switch 데이터 이전 시 발생하는 아티팩트 잔재 및 보안 데이터 승계 메커니즘에 대한 추가적인 연구를 진행하고자 한다.

참 고 문 헌

- [1] Choi, J., & Kim, S. J., "A Study on Mobile Forensic Data Acquisition Method Based on Manufacturer's Backup Mobile App". Journal of The Korea Institute of Information Security and Cryptology,

- 28(1), pp.95-110, 2018,
DOI : 10.13089/JKIISC.2018.28.1.95
- [2] Lee, Y. H., "A Study on User Data Acquisition of Smart Devices". Master's thesis, Graduate School of Information Security, Korea University, 2014,
URL :<http://www.riss.kr/link?id=T13383988>
- [3] Kim, D., & Lee, S., "Trends in Mobile Forensics". Review of KIISC, 26(5), pp.22-31, 2016, pISSN : 1598-3978
- [4] Lee, H. W., "Android based Mobile Device Rooting Attack Detection and Response Mechanism using Events Extracted from Daemon Processes", Journal of The Korea Institute of Information Security and Cryptology, 23(3), pp.479-490, 2013.,
DOI : 10.13089/JKIISC.2013.23.3.479
- [5] Maus, S., Höfken, H., & Schuba, M., "Forensic Analysis of Geodata in Android Smartphones". Proceedings of the 2011 IEEE 10th International Conference on Cybernetic Intelligent Systems (CIS), pp.104-109, 2011,
<https://www.semanticscholar.org/paper/5cad6c29acc200f2ebbf13efa5c9df4533cc836a>
- [6] Park, E., Kang, S., Kim, S., & Kim, J., "System Log Analysis and Forensic Application Techniques of Latest Samsung Smartphones by Data Acquisition Methods". Journal of Digital Forensics, 14(1), pp.1-19., 2020, ISSN : 2713-931X
- [7] Son, N., Lee, Y., Kim, D., James, J. I., Lee, S., & Lee, K., "A study of user data integrity during acquisition of Android devices", Digital Investigation, 10, pp.3-11, 2013, DOI : 10.1016/j.diin.2013.06.001
- [8] Lee, G. W., Hwang, H., Kim, K. B., & Jang, T. J., "Analysis Scheme on Backup Files of Samsung Smartphone available", KIPS Transactions on Computer and Communication Systems, 2(8), pp.349-356, 2013, DOI : 10.3745/KTCCS.2013.2.8.349
- [9] Park, M., Kim, H., & Kim, J., "How to decrypt PIN-Based encrypted backup data of Samsung smartphones", Digital Investigation, 26, pp.63-71, 2018,
DOI : 10.1016/j.diin.2018.05.006
- [10] Park, M., & Kim, J., "A Study on Research Trends in Smartphone Backup Data Acquisition", Review of KIISC, 28(5), pp.5-8, 2018, pISSN : 1598-3978
- [11] Al Mutawa, N., Bryce, J., Franqueira, V. N. L., & Marrington, A., "Forensic investigation of cyberstalking cases using Behavioural Evidence Analysis", Digital Investigation, 16, pp.96-103, 2016,
DOI : 10.1016/j.diin.2016.01.012
- [12] Kwon, H., Lee, S., & Jeong, D., "User profiling via application usage pattern on digital devices for digital forensics", Expert Systems with Applications, 168, 2021, DOI : 10.1016/j.eswa.2020.114488

저 자 소 개



김영준(Young-June Kim)

2022.8 아주대학교 대학원, 공학박사
2023.3-현재 : 서울경찰청 사이버수사과
사이버수사관
<주관심분야> 디지털포렌식, 데이터 복원,
정보보호