**안드로이드 기기 내 파일 공유 어플리케이션에 관한 디지털 포렌식 연구**

삼성 안드로이드 기기에서 별도 설치가 필요 없는 세 가지 파일 공유 어플리케이션 분석

<관련 연구>

모바일 기기 분석 방법: 1) 앱의 패키지 구조를 분석하여 저장된 데이터를 통한 사용자 행위 분석 2) 앱 APK에 대한 정적, 동적 분석

BLE(Bluetooth Low Energy): 저전력 근거리 무선 통신으로, 통신하고자 하는 기기를 탐색하여 기기 간 채널을 형성하여 통신 -> Google의 Nearby, 삼성의 파일 공유 어플리케이션이 사용

<Nearby Share>

Google 에코 시스템에서 사용

근거리 안드로이드 사용자 간 파일 공유 가능 (안드로이드 버전 6 이상, 와이파이, 블루투스 필요)

모든 파일 포맷에 대한 파일 공유 가능

<Quick Share>

삼성 에코시스템에서 사용

BLE를 통해 주변 기기의 거리, 방향 등 탐지하고 와이파이, 데이터 통신으로 공유 데이터 전송 (안드로이드 버전 10 이상, OneUI2.1 이상의 삼성 기기 필요)

<Private Share>

Quick Share 기반으로 블록체인 기반 암호화 기법을 통해 보안성을 강화한 파일 공유 앱

공유 시 전화번호 혹은 개인 고유번호 필요, 공유된 파일은 수신자만 열람 가능

발신자는 공유 파일에 대한 유효기간 설정 가능

공유된 파일 상태를 발, 수신자 모두 실시간 확인 가능

공유된 파일은 기기에 다운로드 불가, 어플리케이션 상에만 열람 가능

파일 형식 제한적

**안드로이드 플랫폼 내 파일 공유 추적에 대한 포렌식 분석**

언제 어떤 파일을 공유했는지가 중요

1. Nearby Share

공유된 파일의 메타데이터인 생성, 수정, 접근 시간은 변경되고 데이터 변조 없음. 해시값 또한 변경 없음 -> 파일 원본성 유지 입증 가능

다운로드 받은 파일 및 정보 획득 가능

발신 -> 파일 공유 흔적 x

수신 -> download.db, esternal.db에 저장. 저장 경로, 밈 타입, 받은 시간, 파일 크기 및 이름 저장

1. Quick Share

와이파이, 블루투스 가능한 Windows에서도 사용 가능

Nearby보다 다양한 아티팩트 수집 가능 (상대방 정보, 상대방 기기 이름 등)

발신 -> share\_live.db 파일 내 세 테이블에 파일 크기, 전송 상태, 시간 정보 등저장

수신 -> inbound\_transfer.db의 두 테이블 내에 저장경로, 발신자 이름, 공유 상태 등 저장. UrisDB6 파일에는 보다 정확한 전송 상태 저장

Windows에서는 Download/QuickShare에 파일 이름, 발신자 정보 등 저장됨

1. Private Share

SIM 카드 없을 시엔 열 자리 무작위 숫자를 통해 사용자 식별 가능

파일 공유를 위해 먼저 초대가 필요하고 수락 시 상호 동의 하에 파일 공유 가능

Transaction\_database.db에 파일 이름, 공유 시간, 사용된 공개 키 등 저장

* 사용자 간 구성 행위 재구성 가능

위의 세 가지 앱에 대한 분석 방법을 도구로 구현한 내용 깃허브에 있음

한계점: 루팅을 안하면 데이터 수집 제한적, private share는 어떤 파일인지 확인하기 위해 복호화가 필요함

향후 복호화 연구 or 새로운 앱에 대한 연구