ExT2 파일시스템 복호화 관련

1. 관련 도구
   - ➔ MOBILedit Forensic 9.4: WearOS 분석 제공. 보안 우회에 탁월한 UFED와 결합함. 모든 유형의 Android 암호 해독 지원 (근데개비싸네요 기각)
     MOBILedit Forensic 9.4 출시: WearOS 추출, UFED 전체 파일 시스템 추출 등! — 모빌편집
   - ➔ Debugfs: Ext2 구조 분석 (메타데이터 확인)
   - ➔ EncFS: EXT2 같은 파일시스템 위에 암호화된 디렉토리를 평문처럼 접근
   - ➔ Bulk_extractor: 디스크 이미지, 메모리 덤프, 파티션 등에서 유의미한 문자열, 패턴, 암호화 키 후보를 뽑아내는 자동 분석 툴
   - ➔ Lime: 메모리 덤프 추출

참고논문

Ext 4 파일시스템이 Fscrypt로 암호화된 안드로이드 환경에서 실행중인 메모리 덤프를 통해 복호화 키 추출 시도 가능.. 너무 길어서 요약해서 봤어요..

🛠️ 사용 기술 및 방법

1. **fscrypt 기반 EXT4 분석**
   - Android에서 널리 사용하는 파일 기반 암호화 구조
   - `inode` 메타데이터는 열 수 있으나, 파일 내용은 복호화 없이는 볼 수 없음
2. **메모리 덤프 활용**
   - 시스템 실행 중 메모리를 덤프하여 **fscrypt 키 존재 여부 확인**
   - 키가 메모리에 평문 형태로 남아있는 경우를 포착
3. **도구 사용**
   - `LiME` : 메모리 덤프 수집
   - `Volatility` : 메모리 분석
   - 자체 제작 도구 `fbekeyfind` : FBE 키 패턴 탐지
4. **암호화 키 복구**
   - `fscrypt_master_key` 의 구조를 역공학으로 분석하여 메모리 내에서 키 검색
   - 키를 확보한 후 암호화된 파일 복호화 시도

2. 방향 제안

암호화 알고리즘 식별 및 복구 시나리오

메모리 덤프 떠서 volatility나 LiME 등으로 키 추출 시도

암호화 키 저장 위치 파악 시도 (AVD 내부 파일 구조에서 키 캐시 위치 리버싱)ㄴ